Analyse Wezenlijke Belangen van de Defensie-basisgebieden (V2450)

ONGERUBRICEERD Releasable to the public › TNO 2025 R11120
Augustus 2025

Defence, Safety & Security
www.tno.nl
+31 88 866 10 00
info@tno.nl

TNO 2025 R11120 – Augustus 2025

Analyse Wezenlijke Belangen van de Defensie-basisgebieden (V2450)

Rubricering rapport	ONGERUBRICEERD Releasable to the public
Vastgesteld d.d.	21 augustus 2025 (deze rubricering wijzigt niet)
Titel	ONGERUBRICEERD Releasable to the public
Managementuittreksel	ONGERUBRICEERD Releasable to the public
Samenvatting	ONGERUBRICEERD Releasable to the public
Rapporttekst	ONGERUBRICEERD Releasable to the public
Oplage	-
Aantal pagina's	73 (excl. voor- en achterblad en distributielijst)
Aantal bijlagen	0
Opdrachtgever	Ministerie van Defensie, Directie Strategie & Kennis
Programmanaam	Technologie- en Innovatie-analyses voor Beleidsondersteuning
Programmanummer	V2450
Projectnaam	Analyse Wezenlijke Belangen van de Defensie-basisgebieden
Projectnummer	060.57047/01.06

Managementuittreksel

Analyse Wezenlijke Belangen van de Defensie-basisgebieden

Programma

Programmanaam:
Technologie- en Innovatie-analyses voor Beleidsondersteuning

Programmanummer: V2450

Programmaplanning: Startdatum 1 januari 2023
Einddatum 31 december 2026

Project

Projectnaam:
Analyse Wezenlijke Belangen van de Defensie-basisgebieden

Projectnummer: 060.57047/01.06

Projectplanning: Startdatum 1 april 2025
Einddatum 31 augustus 2025

Het Ministerie van Defensie heeft in samenwerking met het Ministerie van Economische Zaken in april 2025 de Defensie Strategie voor Industrie en Innovatie (DSII) gepubliceerd. Daarin zijn tien Defensie-basisgebieden gedefinieerd die samen de kennis- en innovatiebehoefte van Defensie vormen. Dit rapport dient als aanvulling op de DSII: hier worden de wezenlijke veiligheidsbelangen van de tien Defensie-basisgebieden beschreven, alsmede welke rol de overheid per (sub-)gebied zou kunnen overwegen.

Doelstelling

Het doel van dit rapport is het duiden en preciseren van de wezenlijke veiligheidsbelangen van de tien Defensie-basisgebieden.

Beschrijving van de werkzaamheden

In het kader van de Defensie Industrie Strategie (DIS) 2018 is destijds door HCSS een toetsingskader ontwikkeld waarmee een kwalitatief inzicht is te geven in nationale veiligheidsbelangen, bedreigingen, en daaruit voortvloeiende voor Defensie benodigde (industriële) capaciteiten en kennis- en technologiegebieden. In het toetsingskader vormt het begrip 'wezenlijke belangen' het centrale ankerpunt dat wordt beredeneerd vanuit (1) veiligheidsrisico's en dreigingen; (2) doelen van het Nederlands buitenlands-, veiligheids- en defensiebeleid; en (3) fundamentele karakteristieken van de krijgsmacht. In dit rapport is het toetsingskader van HCSS geactualiseerd en is er een vierde factor geïdentificeerd: (4) de Nederlandse industriële capaciteiten. Met deze factor kan bijvoorbeeld een economisch of strategisch belang worden toegevoegd aan de afweging die wordt gemaakt. Ten opzichte van de DIS 2018 zijn in de DSII 2025 bovendien tien nieuwe Defensie-basisgebieden gedefinieerd. Omdat deze als basis dienen voor de operationalisering van de wezenlijke belangen, zijn de in de DIS 2018 gehanteerde kennisgebieden, technologiegebieden en industriële capaciteiten in dit rapport herleid naar de nieuwe Defensie-basisgebieden. Vervolgens is het geactualiseerde toetsingskader toegepast op de tien Defensie-basisgebieden.

Resultaten en conclusies

Voor alle tien Defensie-basisgebieden, uitgesplitst in 53 subgebieden, is aan de hand van het geactualiseerde en uitgebreide toetsingskader geanalyseerd welke wezenlijke belangen deze technologiegebieden kunnen hebben voor Nederland. Het resultaat is een gedetailleerd

overzicht van alle basisgebieden en subgebieden waarin de verschillende soorten belangen zijn geduid, alsmede de technologische en industriële capaciteiten in Nederland. Ook is per (sub-)gebied aangeduid wat de meest voor de hand liggende rollen zijn die de Nederlandse overheid op dat gebied zou kunnen overwegen.

Toepasbaarheid

Het overzicht van wezenlijke belangen van Defensie-basisgebieden is te gebruiken als hulpmiddel bij het prioriteren van investeringen en bij het selecteren van de meest passende aanbestedingsmethode bij investeringen. Sommige (verkorte) aanbestedingsprocedures zijn alleen mogelijk als er wezenlijke belangen in het geding zijn, waarvoor dit rapport onderbouwing kan leveren.

Summary

In April 2025, the Netherlands Ministry of Defence, in collaboration with the Ministry of Economic Affairs, published the Defence Strategy for Industry and Innovation (DSII). The DSII defines ten Defence technology areas that together form the knowledge and innovation needs of the Ministry of Defence. This report serves as a supplement to the DSII: it describes the essential security interests of the ten Defence technology areas, as well as the role(s) the Dutch government could consider for each (sub)area.

This overview of essential security interests of Defence technology areas can be used as a tool for prioritising investments and for selecting the most suitable procurement method for investments. Some (quicker) procurement procedures are only possible if essential interests are at stake, and this report can assist in providing validation for such procedures.

Inhoudsopgave

1 Inleiding

1.1 Achtergrond

Het Ministerie van Defensie heeft in samenwerking met het Ministerie van Economische Zaken in april 2025 de Defensie Strategie voor Industrie en Innovatie (DSII) gepubliceerd. Daarin zijn 10 Defensie-basisgebieden gedefinieerd die tezamen de kennis- en innovatiebehoefte van Defensie vormen. TNO heeft bijgedragen aan de totstandkoming van de DSII door technologische ontwikkelingen die relevant zijn voor Defensie in kaart te brengen en de taxonomie van de tien Defensie-basisgebieden te definiëren.

Figuur 1.1: De 10 Defensie-basisgebieden.

Bij het uitbrengen van de DSII hebben Defensie en Economische Zaken aangegeven om later in 2025 een publicatie met de Tweede Kamer te delen waarin de wezenlijke veiligheidsbelangen van de tien Defensie-basisgebieden worden beschreven alsmede welke rol de overheid per (sub-)gebied ambieert. Dit rapport komt uit deze behoefte voort: het analyseert de wezenlijke veiligheidsbelangen van de tien Defensie-basisgebieden en beschrijft overwegingen betreffende de mogelijke rollen die de Nederlandse overheid per (sub-)gebied zou kunnen ambiëren. In de DSII zijn negen verschillende rollen gedefinieerd, zie Figuur 1.2. Deze rollen worden aangeduid als de ‘SMART rollen’.

Artikel 346 van het VWEU kan alleen van toepassing worden verklaard indien er sprake is van wezenlijke veiligheidsbelangen. Deze wezenlijke belangen zijn echter niet verder gespecificeerd door de Europese Unie (EU). In 2018 is door *The Hague Centre for Strategic Studies* (HCSS), als onderdeel van de totstandkoming van de toenmalige DIS, een analyse uitgevoerd voor de operationalisering van wezenlijke veiligheidsbelangen voor Nederland. Wezenlijke veiligheidsbelangen zijn in de HCSS-analyse gedefinieerd als: *“in functie van de 1) Nederlandse soevereiniteit, 2) veiligheid van zijn onderdanen en schepen onder zijn vlag, en 3) bevoorradingszekerheid (of inzetzekerheid) van de vijf defensiedomeinen (land, lucht, zee, ruimte, cyber)”*. Dit is gebaseerd op eerder onderzoek van de Radboud Universiteit.

In de HCSS-analyse is uiteengezet waarom het beschikken over een eigen technologische en industriële basis van belang is om in de veiligheid van Nederland en haar bondgenoten te kunnen voorzien. De validiteit van die analyse is bevestigd in 2022, toen na het uitbrengen van de Defensienota 2022 de DIS is bezien in de veranderde geopolitieke context.

Figuur 1.2: De 9 'SMART' rollen zoals in de DSII gedefinieerd.

1.2 Uitgangspunten

TNO is gevraagd om ondersteuning te bieden bij het herijken van de wezenlijke veiligheidsbelangen van de tien Defensie-basisgebieden alsmede het duiden welke rol de overheid per (sub)-gebied zou kunnen ambiëren. TNO heeft daarbij met name bestaande materiekennis en methodische kennis aangewend en doet op basis daarvan in dit rapport verslag. De uiteindelijke keuzes die worden gemaakt, zullen door Defensie en Economische Zaken worden genomen. Daarbij zal ook interne juridische expertise door beide ministeries worden meegewogen; juridische overwegingen zijn in dit rapport niet meegenomen.

Bij het uitvoeren van dit project zijn, in overleg tussen TNO en de opdrachtgevers, de volgende uitgangspunten gehanteerd:

1. De wezenlijke veiligheidsbelangen op basis van de HCSS-definitie worden hier beschouwd als een gegeven en staan niet ter discussie. Daarnaast wordt er een extra belang aan toegevoegd: de Nederlandse (NLD) industriële capaciteiten.
2. De 10 Defensie-basisgebieden (inclusief de 53 onderliggende subgebieden) zijn gedefinieerd in de DSII en zijn, als taxonomie, in de plaats gekomen van de Kennisgebieden, Technologiegebieden en Industriële Capaciteiten zoals in de DIS 2018 benoemd.

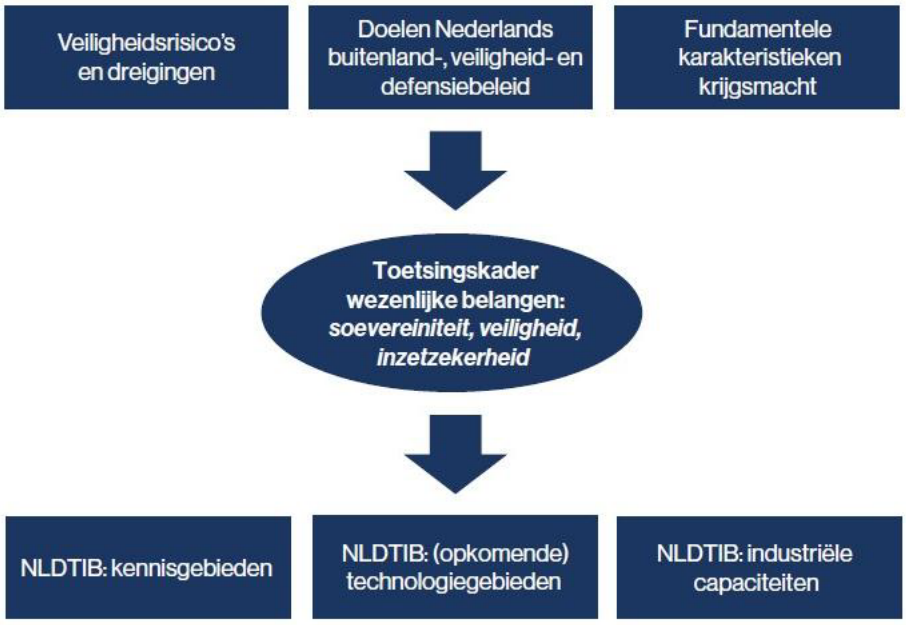
1.3 Doel van het project

Het doel van het project is het duiden en preciseren van de wezenlijke veiligheidsbelangen voor de 10 Defensie-basisgebieden. Als startpunt wordt de HCSS-studie uit 2018 en het daarin ontwikkelde toetsingskader gebruikt en zullen de destijds gemaakte kwalitatieve beoordelingen worden herijkt op basis van de huidige situatie en de nieuwe taxonomie van de 10 Defensie-basisgebieden. Daarbij wordt per Defensie-basisgebied aangeven welke SMART rol de Nederlandse overheid hierin zou kunnen overwegen. TNO geeft, op basis van de beschikbare informatie uit beleidsdocumenten en de uitgevoerde Technologie Verkenningen 2024, uitsluitend een eerste inschatting of overweging voor een of meerdere keuzemogelijkheden. De uiteindelijke keuze van rollen is aan de Nederlandse overheid.

2 Toetsingskader

2.1 Toelichting

In het kader van de DIS 2018 is destijds door HCSS een toetsingskader ontwikkeld waarmee een kwalitatief inzicht is te geven in bedreigingen, nationale veiligheidsbelangen en daaruit voortvloeiende benodigde (industriële) capaciteiten en kennis- en technologiegebieden. Hierin vormt het begrip 'wezenlijke belangen' het centrale ankerpunt, zie Figuur 2.1.



Figuur 2.1: Toetsingskader ontwikkeld door HCSS ten dienste van de DIS 2018.

Het begrip 'wezenlijke belangen' is in de HCSS-studie uit 2018 uitgewerkt op basis van: (1) de structurele ontwikkelingen in de risico's en dreigingen die op Nederland en zijn bondgenoten afkomen, bezien vanuit (2) de accenten die voortvloeien uit de doelen van het Nederlandse defensie- en veiligheidsbeleid en, meer in het bijzonder, (3) vanuit de fundamentele karakteristieken (zoals veelzijdig inzetbaar, technologisch hoogwaardig en adaptief) die ons land van zijn krijgsmacht verwacht.

Deze aanpak heeft geleid tot een samenhangende set van overwegingen – een toetsingskader – die het begrip wezenlijke belangen operationaliseert. Op basis daarvan kunnen uitspraken gedaan worden over de gewenste mate van nationale zekerstelling van de Nederlandse defensie- en veiligheid-gerelateerde technologische industriële basis in generieke zin. Dit laatste geeft een beeld welke onderdelen van de defensie- en veiligheid-gerelateerde technologische industriële basis bij voorkeur nationaal georganiseerd zouden moeten worden en (daarom) wellicht vanuit een nationaal defensie-industriebeleid worden ondersteund. Dit beeld is vanuit een specifieke invalshoek, namelijk een top-down uitwerking van het begrip wezenlijke belangen, opgebouwd. Er zijn ook andere overwegingen van

politieke of economische aard om het defensie-industriebeleid op te baseren. In de DIS 2018 zijn deze andere overwegingen samengevoegd met het top-down perspectief dat in deze bouwsteen is uitgewerkt.

2.2 Wijzigingen

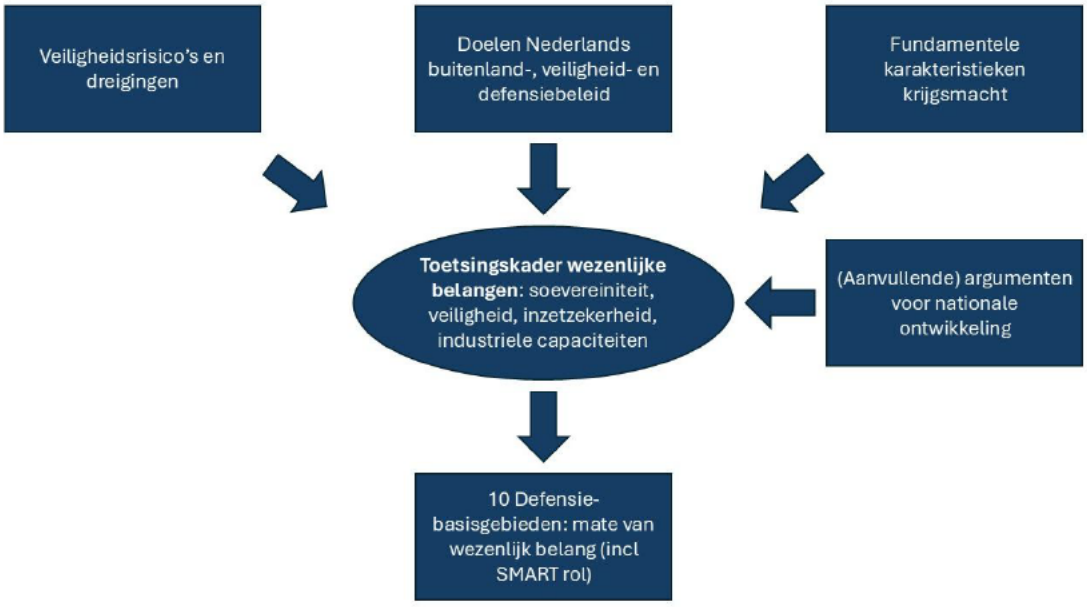
De aanpak zoals in het toetsingskader uit 2018 is uitgewerkt, is in de huidige analyse overgenomen. Wel is daarbij een vierde wezenlijk belang toegevoegd: de Nederlandse industriële capaciteiten. Die laatste is toegevoegd aan de drie wezenlijke belangen, omdat daarmee ook een belang kan worden geduid, bijvoorbeeld een economisch belang of een strategisch belang.

De overwegingen zoals die in de 2018 studie zijn gehanteerd zijn in de voorliggende analyse geactualiseerd op basis van de huidige situatie. Daarbij spelen onder meer de oorlog in Oekraïne en nieuwe beleidsambities, verwoord in onder meer de Defensievisie 2035, Defensienota 2024 en de DSII 2025, een belangrijke rol. Zo zijn in de afgelopen zeven jaar ook bepaalde dreigingen geïntensiveerd en/of ontstaan, denk aan *seabed warfare* en de massale inzet van (deels low-tech) drones. Ook zijn inrichtingsprincipes zoals Informatiegestuurd Optreden (IGO) en Multi Domein Operaties (MDO) voor de Nederlandse krijgsmacht verder geoperationaliseerd.

In hoofdstuk 3 wordt de actuele stand van zaken geanalyseerd als het gaat om de drie uitwerkingen van wezenlijke belangen: (1) veiligheidsrisico's en dreigingen; (2) doelen Nederlands buitenlands-, veiligheids- en defensiebeleid; en (3) fundamentele karakteristieken krijgsmacht. Deze actualisatie geeft dan een beeld of, en zo ja, waar er tussen 2018 en nu veranderingen hebben plaatsgevonden. Eventuele veranderingen zijn vervolgens meegenomen in de daadwerkelijke operationalisering van de wezenlijke belangen (zie hoofdstuk 6). Voor het toegevoegde vierde belang (NLD industriële capaciteiten) is geen actualisatie ten opzichte van 2018 uitgevoerd aangezien deze als dusdanig niet in de 2018 studie is uitgewerkt.

Verder zijn in de HCSS-studie als onderdeel van het toetsingskader 11 relevante argumenten genoemd die een nationale ontwikkeling van defensiecapaciteiten kunnen rechtvaardigen. Deze zijn aangevuld met argumenten die in de huidige tijdsgeest een belangrijke rol spelen. In hoofdstuk 4 worden alle argumenten kort op een rij gezet. Waar relevant zijn deze argumenten meegenomen in de operationalisering van de wezenlijke belangen (zie hoofdstuk 6).

Ten opzichte van 2018 zijn verder in de DSII 2025 tien Defensie-basisgebieden gedefinieerd. Deze dienen als basis voor de operationalisering van de wezenlijke belangen. Om die reden zijn de in de DIS 2018 gehanteerde kennisgebieden, technologiegebieden en industriële capaciteiten herleid naar de Defensie-basisgebieden. Deze herleiding is in hoofdstuk 5 beschreven.



Figuur 2.2: Geactualiseerde toetsingskader.

3 Actualisatie

3.1 Veiligheidsrisico's en dreigingen

Sinds 2018 is het dreigingslandschap niet zozeer veranderd, maar is met name de intensiteit ervan toegenomen. In 2018 had Rusland al wel delen van Oekraïne geannexeerd (onder andere de Krim), maar in 2022 volgde een grootschalige Russische invasie waarmee de strijd tussen Rusland en Oekraïne werd geïntensiveerd, evenals Westerse betrokkenheid. Westerse landen, inclusief Nederland, leveren sinds 2022 grootschalige financiële en materiële steun aan Oekraïne. De strijd in Oekraïne toont dat grootschalige, interstatelijke oorlogvoering op Europees grondgebied reëler is dan in de decennia na het einde van de Koude Oorlog voor mogelijk werd gehouden (Ministerie van Defensie, 2024, 11).

In 2018 was er ook al aandacht voor hybride conflictvoering, dat wil zeggen offensieve activiteiten in het grijze gebied tussen vrede en oorlog in, dus onder de drempel van gewapend conflict. In de jaren erna is het aantal hybride aanvallen op Nederland en bondgenoten echter aanzienlijk toegenomen, met name in de zin van cyberaanvallen, ondermijnende desinformatiecampagnes en sabotageacties in verschillende soorten (zoals brandstichtingen en het beschadigen van onderzeese communicatiekabels). Veel van deze hybride aanvallen worden toegeschreven aan Rusland; dit land is zich assertiever (en agressiever) gaan gedragen richting Westerse landen, mede omdat Rusland op deze manier steun aan (en draagvlak voor) het Oekraïense verzet tegen de Russische invasie probeert te verzwakken. Ook voor andere landen, zoals China en Iran, vormt Nederland in toenemende mate een doel van hybride operaties (Ministerie van Defensie, 2020; Ministerie van Defensie, 2024, 11-12; MIVD, 2025).

Vanuit het oogpunt van veiligheidsrisico's en dreigingen is geen directe aanpassing van het toetsingskader uit 2018 nodig: de risico's en dreigingen zijn weliswaar concreter en urgenter geworden, maar qua aard weinig veranderd. In het gebruik van het toetsingskader voor het beoordelen van specifieke technologieën kan de toegenomen dreiging van zowel interstatelijk als hybride conflict echter wel extra aandacht krijgen.

3.2 Doelen Nederlands buitenlands, veiligheids- en defensiebeleid

Sinds het opstellen van het toetsingskader in 2018 zijn er nieuwe beleidsdocumenten verschenen waarin het Nederlandse buitenlands, veiligheids- en defensiebeleid worden geactualiseerd. Het gaat dan met name om de Veiligheidsstrategie voor het Koninkrijk der Nederlanden (Rijksoverheid, 2023) en de nieuwe Defensienota uit 2024 (Ministerie van Defensie, 2024). Deze bieden geen grote verschuivingen in het Nederlandse beleid vergeleken met de situatie in 2018, al is de intensivering van dreigingen, zoals in de vorige paragraaf beschreven, ook in het beleid zichtbaar. Wel is inmiddels een verschuiving en prioritering te zien naar meer Europese verantwoordelijkheid, die met name sinds 2024 aan belang wint. Ook is de urgentie van geïntegreerd buitenlands, veiligheids- en defensiebeleid, in Nederland maar ook in de EU, alleen maar groter geworden.

De Veiligheidsstrategie voor het Koninkrijk der Nederlanden uit 2023 biedt een goed overzicht van de prioriteiten voor Nederland (Rijksoverheid, 2023). De strategische koers voor de nationale veiligheid wordt in drie hoofddoelstellingen onderverdeeld:
1. Een veilig Koninkrijk in een multipolaire wereld;
2. Een weerbare democratische rechtsorde;
3. Een parate en veerkrachtige samenleving.

Vervolgens worden twaalf actielijnen uiteengezet op basis waarvan Nederland de weerbaarheid wil vergroten:
1. Investeringen in internationale partnerschappen en versterking van de krijgsmacht;
2. Bestrijden van hybride conflictvoering;
3. Vergroten weerbaarheid economie en beschermen van wetenschap;
4. Vergroten van de sociale stabiliteit;
5. Tegengaan van georganiseerde, ondermijnende criminaliteit;
6. Tegengaan van ongewenste buitenlandse inmenging en spionage;
7. Versterken van de digitale weerbaarheid;
8. Voorkomen en bestrijden van terrorisme en extremisme;
9. Intensiveren klimaatmitigatie en -adaptatie;
10. Beter beschermen van de vitale infrastructuur;
11. Vergroten van pandemische paraatheid;
12. Versterken van crisisbeheersing en vergroten paraatheid samenleving.

In deze doelstellingen en actielijnen zitten geen fundamentele verschillen met de Geïntegreerde Buitenland- en Veiligheidsstrategie uit 2018, die is gebruikt bij het opstellen van het toetsingskader door HCSS. Wel zijn er accenten aangescherpt, zoals de versterking van de krijgsmacht, het vergroten van de weerbaarheid van de economie en het beschermen van wetenschap. Aangezien het fundament niet is gewijzigd, is het toetsingskader uit 2018 nog steeds goed bruikbaar in de huidige situatie.

3.3 Fundamentele karakteristieken krijgsmacht

In 2020 verscheen de Defensievisie 2035 met daarin een aantal doelstellingen waar de Nederlandse krijgsmacht de komende jaren naartoe gaat werken. In de Defensievisie zijn drie eigenschappen genoemd waaraan Defensie in 2035 zou moeten voldoen:
1. Technologisch hoogwaardig;
2. Informatiegestuurd in organisatie en optreden;
3. Een betrouwbare partner en beschermer.

Om deze eigenschappen te bevorderen, zijn tien ‘inrichtingsprincipes’ voor de defensieorganisatie geïdentificeerd:
1. Unieke mensen en arbeidsextensieve capaciteiten;
2. Flexibel optreden: snel inzetbaar, schaalbaar en zelfstandig;
3. Sterk innoverend vermogen;
4. Escalatiedominantie, met onze partners;
5. Gezaghebbende informatiepositie;
6. Multidomein en geïntegreerd optreden;
7. Transparant en zichtbaar in een betrokken samenleving;
8. Inzetten op een sterker, zelfredzamer Europa;
9. Inzetten op verdere specialisatie binnen de NAVO en de EU;
10. Strategische capaciteiten voor een weerbare samenleving.

Hoewel de Defensievisie 2035 verscheen vóór de grootschalige Russische invasie in Oekraïne (maar na de eerdere annexatie van delen van het land), zijn deze eigenschappen en inrichtingsprincipes nog geheel actueel. Sterker nog, de oorlog in Oekraïne heeft het belang van de meeste ervan alleen maar vergroot. Andere recente geopolitieke ontwikkelingen, zoals de veranderde rol van de Verenigde Staten op het wereldtoneel, zijn ook al goeddeels afgedekt door bijvoorbeeld inrichtingsprincipe 8: het inzetten op een sterker, zelfredzamer Europa.

Het toetsingskader uit 2018 was nog gebaseerd op de Defensienota uit 2018, waarin enigszins andere terminologie wordt gebruikt, maar die inhoudelijk niet heel verschillend is; het gaat in die Defensienota om termen als ‘veelzijdig inzetbaar', wendbaar', ‘robuust', ‘technologisch hoogwaardig', ‘strategisch anticiperend', ‘informatiegestuurd', en ‘snel tenzij & van de plank tenzij verwervend’ (Ministerie van Defensie, 2018). Deze terminologie is vrij eenvoudig te plotten op de termen die in de Defensievisie uit 2020 worden gebruikt. Ook wat dit betreft is er geen aanleiding om het toetsingskader uit 2018 te herzien, maar voor het beoordelen van specifieke technologieën kan de toegenomen noodzaak van (Europese dan wel Nederlandse) autonomie wel meer nadruk krijgen.

4 Argumenten voor nationale ontwikkeling

Het toetsingskader is gebruikt bij het analyseren van de wezenlijke belangen van de Defensie-basisgebieden, zijnde 1) de veiligheidsrisico's en dreigingen waar Nederland mee te maken heeft of kan krijgen, 2) de doelen van het Nederlandse buitenland-, veiligheid- en defensiebeleid, en 3) de fundamentele karakteristieken van de Nederlandse krijgsmacht. Als onderdeel daarvan of als aanvulling daarop zijn er specifieke argumenten die vanuit een wezenlijk belang een rol kunnen spelen bij de afweging om militaire capaciteiten nationaal te ontwikkelen. In de HCCS-studie 2018 zijn 11 argumenten uitgewerkt. Deze 11 zijn nog steeds van kracht, maar er zijn inmiddels ook twee aanvullende argumenten, ingegeven door de huidige (geopolitieke) tijdsgeest. Hieronder worden alle 13 argumenten kort opgesomd en toegelicht. Waar relevant zullen deze in de daadwerkelijke analyse van de wezenlijke belangen per Defensie-basisgebied benoemd worden.

1. Geheime opdrachten

Geheime opdrachten vallen op grond van een uitzonderingsbepaling van de Aanbestedingswet op defensie- en veiligheidsgebied buiten de aanbestedingsregels. Dit heeft vooral betrekking op de specificaties van taakkritische systemen of subsystemen die onvoldoende kunnen worden beschermd onder aanbestedingsprocedures. Vooral de specificaties van sensor-, wapen- en commandovoeringsystemen, waaronder tevens begrepen informatiesystemen voor het verzamelen en verwerken van inlichtingen, mogen niet bekend zijn.

2. Existentiële dreigingen

Wanneer aannemelijk kan worden gemaakt dat een te ontwikkelen, te verwerven of in stand te houden capaciteit van doorslaggevend belang is in het tegengaan van dreigingen waarbij Nederland er in beginsel en/of in het begin alleen voor staat, dan is er sprake van een wezenlijk belang. Dit geldt tevens voor dreigingen tegen de wezenlijke belangen van het Koninkrijk en/of van zijn NAVO- en EU-partners waarbij Nederland een verdragsrechtelijke verplichting heeft, of dreigingen die de wezenlijke belangen van het Koninkrijk en/of zijn NAVO- en EU-partners zodanig raken dat de Regering zich geen opstelling als *free rider* kan veroorloven.

3. Nederlandse karakteristieken

Een capaciteit is meer dan alleen een systeem of materieel, het behelst een bundeling van DOTMLPFI (Doctrine, Organisatie, Training, Materieel, Leiderschap, Personeel, Faciliteiten, Interoperabiliteit) waarmee uiteindelijk een militair vermogen of effect wordt gerealiseerd. Ook al hebben krijgsmachten bijvoorbeeld hetzelfde materieel, een gezamenlijke opleiding of een gedeelde doctrine, de DOTMLPFI aspecten als geheel reflecteren de specifieke eigenschappen van een krijgsmacht die veelal gebaseerd zijn op de normen en waarden, cultuur, geschiedenis en politiek-maatschappelijke keuzen van een land. De keuze en inzet van een capaciteit zal moeten passen binnen de Nederlandse invulling van DOTMLPFI en is per definitie een nationale verantwoordelijkheid.

4. Operationeel voordeel
Samen met zijn bondgenoten streeft de Nederlandse krijgsmacht naar het behoud van technologisch overwicht ten opzichte van (potentiële) tegenstanders. Dit is lastiger naarmate deze gemakkelijker toegang krijgen tot geavanceerde civiel-gedreven maar militair-relevante technologieën. Technologische hoogwaardigheid vereist dat Defensie ten minste moet kunnen optreden als SMART buyer. Om een asymmetrisch (operationeel) voordeel te behouden of creëren ten opzichte van tegenstanders, is het noodzakelijk om capaciteiten op maat te kunnen (laten) ontwikkelen in plaats van generieke “van de plank” capaciteiten in te kopen. Dat vereist dat Defensie op sommige gebieden zelfs meer dan de SMART buyer rol moet vervullen en bijvoorbeeld als SMART specifier of developer moet optreden (zie Figuur 1.2 voor de set van SMART rollen).

5. Brede kennisbasis
Om ten minste als SMART buyer te kunnen optreden, moet Defensie over een brede kennisbasis met voldoende diepgang kunnen beschikken. Alleen dan kunnen slimme keuzes worden gemaakt voor het verwerven en uiteindelijk inzetten van relevante capaciteiten in alle operationele domeinen (zee, land, lucht, ruimte en cyber). Het gaat hierbij zowel om technologische, operationele als strategische kennis. De kennisbasis in een relatief klein land als Nederland is over het algemeen kwetsbaar, en het bundelen van kennis en ervaring binnen de defensieorganisatie, kennisinstellingen en bedrijven in eigen land kan noodzakelijk zijn om voldoende kritische massa en diepgang in de kennisbasis te verzekeren. Nationale R&D-ecosystemen met daarin de defensiegerelateerde kennisinstellingen zijn hiervoor onmisbaar. Zij vormen bovendien een portaal naar technologie- en kennisgebieden die civiel-gedreven zijn maar wel defensierelevant zijn. Ook hebben zij een internationaal netwerk met partnerinstituten waarin veel informatie-uitwisseling plaatsvindt, veelal op basis van wederkerigheid *(quid pro quo).*

6. Innovatie gedurende levensduur
Militaire systemen kennen een lange gebruiksduur. Het met een zekere regelmaat upgraden van hardware en updaten van software, alsmede *technology insertion* (het introduceren van een nieuwe generatie technologie), maken het mogelijk dat een capaciteit zich kan aanpassen aan veranderende technologische en geopolitieke dynamieken (nieuwe dreigingsactoren). Snelheid van innovatie kan ook vanuit de ‘vraag’-zijde een belangrijke vereiste zijn, namelijk als wezenlijke belangen daadwerkelijk door plots opkomende dreigingen worden aangetast. De eis van snelheid staat haaks op het relatief trage proces van aanbesteding. De nadruk op snelle innovatie vereist voorinvesteringen in vertrouwde *triple helix*-samenwerkingsverbanden (overheid, industrie, kennisinstellingen). Het inrichten van dergelijke structurele samenwerking kan een wezenlijk belang dienen.

7. Integratievermogen
Het integratievermogen op systeem/platform/capaciteitsniveau is essentieel voor de Nederlandse krijgsmacht. In de huidige dynamische veiligheidsomgeving moet Defensie generieke oplossingen bedenken die snel kunnen worden toegespitst op specifieke (nieuwe) toepassingen. Het militaire overwicht wordt in toenemende mate bepaald door het innovatieve vermogen om nieuwe toepassingsmogelijkheden te combineren in functioneel samenhangende systemen. Dit integratievermogen – waarbij het nadrukkelijk niet alleen om technische integratie maar om integratie van alle DOTMLPF-elementen gaat - is in de praktijk verankerd in vertrouwde *triple helix*-samenwerkingsverbanden. Integratie maakt van het totaal aan componenten en deelsystemen een ‘Nederlands’ product, ook al worden de componenten elders ontwikkeld of gefabriceerd. Integratievermogen is daarmee een wezenlijk belang.

8. Beheersing toeleveringsketen

Door de toename aan civiel-gedreven technologie in militaire systemen of capaciteiten, neemt ook het ecosysteem van (toe)leveranciers toe. Niet al deze (toe)leveranciers voelen zich onderdeel van de militaire *supply chain*, waardoor leveringszekerheid niet altijd gegarandeerd is. Beheersbaarheid van de *supply chains* door Defensie, zeker voor kritieke onderdelen, is essentieel tijdens de gehele levensduur van een systeem of capaciteit. Internationale samenwerking binnen de *supply chains* is mogelijk, en is vaak zelfs onoverkomelijk, maar nationale regie hierover is nodig. Daarmee wordt leveringszekerheid verhoogd en kunnen ook tijdig alternatieven gezocht worden, bijvoorbeeld door het onderhoud van een systeem (tijdelijk) onder nationale regie te plaatsen.

9. Informatie(systemen) als middel

In de moderne maatschappij is het belang van informatie als productiefactor immens en nog steeds groeiend. Dit is ook in het militaire domein het geval, onder meer binnen de functies van C4ISR maar ook als enabler voor IGO. Een goede informatiepositie is essentieel om de gewenste militaire effecten vast te stellen en te realiseren. Dit geldt op alle niveaus: strategisch, operationeel en tactisch. Een belangrijk deel van de onderliggende ICT is onderhevig aan de 'snelle innovatie'-dynamiek. C4ISR en IGO kennen een belangrijke doctrinaire en *human factor* component die per land kan verschillen. *Triple helix*-samenwerking met vertrouwde nationale partijen op het gehele terrein van hoogwaardige en defensiespecifieke IGO/C4ISR-systemen ligt dan voor de hand en kan een wezenlijk belang dienen.

10. Informatie(systemen) als doelwit en wapen

Defensieve en offensieve cyberoperaties liggen in elkaars verlengde. Diepe kennis van het een is niet mogelijk zonder diepe kennis van het ander. Cyberoperaties zijn verder bij uitstek gevoelig van aard, zowel voor wat betreft de inhoud van de informatie als voor wat betreft de juridische, morele en conceptueel-strategische implicaties van mogelijke acties.
Op het gebied van defensieve en offensieve informatie- / cyberoperaties is het organiseren vankennis en capaciteiten(-ontwikkeling) in nationale industrie aan de orde en kan een wezenlijk belang dienen.

11. Toegang tot capaciteiten

Een belangrijke notie als gevolg van een aantal samenkomende ontwikkelingen is dat militaire organisaties meer en meer moeten denken in andere vormen van het garanderen van de 'toegang tot' (*access to*) capaciteiten dan door deze capaciteiten in eigendom te verwerven. Allerlei (meng)vormen van *military / civil owned* en *military / civil operated* zijn in beginsel denkbaar. Diverse lease-constructies zijn mogelijk, maar Defensie kan 'het vermogen tot' ook volledig als dienst verwerven. Een volgende optie is dat Defensie capaciteiten wel verwerft, maar met het bedrijfsleven dwingende afspraken maakt voor onderhoud en het technologisch up-to-date houden gedurende de levenscyclus.
Ook personele uitwisseling tussen Defensie en het bedrijfsleven en andere organisaties wordt steeds nadrukkelijker mogelijk gemaakt. Dit zal altijd nationaal worden georganiseerd. Voldoende kwalitatief hoogstaande en voor jongeren aantrekkelijke opleidingen die bijvoorbeeld technisch personeel opleiden voor zowel bedrijfsleven als overheid / Defensie is zo te verbinden met nationale veiligheidsbelangen.

12. Strategische autonomie en continuïteit

Door de vele conflicten die er wereldwijd woeden, neemt ook het gebruik van sancties als geopolitiek wapen toe, ook mogelijk naar landen waarmee Nederland langjarig handel drijft. De afhankelijkheid van niet-EU-leveranciers voor het leveren van militaire systemen wordt daarmee onwenselijker. Nationale productie danwel productie binnen de EU (of via

strategische partnerschappen binnen de EU) voorkomt strategische verlamming. Het opbouwen van nationale industriële capaciteit draagt ook bij aan Europese weerbaarheid en zorgt er tevens voor dat Nederland een positie binnen de EU verkrijgt waarmee het wederkerige strategische afhankelijkheden kan creëren. Dat laatst zorgt voor bepaalde garanties in het nakomen van afspraken. In een niet-militaire crisissituatie, zoals gezien tijdens de COVID-19 pandemie, moeten kritieke productielijnen kunnen doorgaan zonder (te veel) afhankelijk te zijn van buitenlandse toelevering. Dit vereist Europese en/of nationale redundantie en schaalbare capaciteit.

13. Maatwerk voor kleine landen

Voor kleinere landen zoals Nederland is het behouden van een eigen, strategisch relevante defensie-industriële capaciteit essentieel om binnen bondgenootschappen als de NAVO en de EU effectief en zelfstandig te opereren. Door hun beperkte schaal zijn kleinere landen zelden zelfvoorzienend, maar kunnen zij juist door specialisatie een waardevolle bijdrage leveren aan coalities. Maatwerk betekent in dit verband: kiezen voor nichecapaciteiten en technologische competenties die aansluiten bij de eigen krijgsmacht én van meerwaarde zijn voor bondgenoten. Denk aan Nederland als leverancier van hoogwaardige maritieme sensoren, C4ISR-integratie, of geavanceerde software voor informatiegestuurd optreden. Met de keuze van vijf Nederlandse prioritaire gebieden (Slimme materialen, Sensoren, Quantum, Ruimtetechnologie en Intelligente systemen) zet Defensie al een stap in die richting.
Deze specialisatie voorkomt ook het ‘one size fits all’-denken dat kleinere landen overgeleverd raken aan standaardproducten van grote leveranciers, die vaak niet aansluiten bij nationaal operationele en nationaal politieke eisen. Daarnaast kan maatwerk helpen om sneller te innoveren, flexibeler op te schalen en beter aan te sluiten bij nationale wetgeving, ethische normen of cyberbeveiligingseisen. Door selectief te investeren in deze gebieden kan Nederland zijn soevereiniteit versterken, een geloofwaardige partner blijven binnen Europese defensiesamenwerking, en tegelijkertijd bijdragen aan bredere Europese strategische autonomie.

5 Defensie-basisgebieden

In de DIS 2018 zijn drie gebieden/lijsten gebruikt die voor de Nederlandse Defensie de kritische kennis, technologie en industriële basis definiëren. In de DSII 2025 is die driedeling losgelaten en worden tien Defensie-basisgebieden gebruikt om de voor de Nederlandse defensie kritische technologische, industriële en kennisbasis te definiëren. Elk van deze tien Defensie-basisgebieden kent een onderverdeling in subgebieden, hetgeen leidt tot een totaal van 53 subgebieden.

Deze subgebieden zijn in een apart document beschreven. Aan de hand van deze beschrijving is een 'mapping' gemaakt van de 53 subgebieden op de drie lijsten zoals die in de DIS 2018 zijn gehanteerd. De reden voor de mapping is dat het daardoor mogelijk is om de door HCSS in 2018 gedane kwalitatieve beoordeling en operationalisering van de wezenlijke belangen te vertalen naar de Defensie-basisgebieden c.q. subgebieden. Met die basis wordt daarna een actualisatie van de kwalitatieve beoordeling en operationalisering van de wezenlijke belangen gedaan, mede vanwege mogelijke nieuwe inzichten en ontwikkelingen zoals beschreven in hoofdstuk 3, en mede vanwege voortschrijdende inzichten in kennis- en technologische ontwikkelingen.

In onderstaande tabel is de gemaakte mapping weergegeven. Daaruit valt op te maken dat:

- Vijf subgebieden niet te herleiden zijn naar de initiële DIS 2018 gebieden, dat betreft:
  - (Counter)Hybrid: kennis hieromtrent is met name vanaf 2018 ontwikkeld.
  - Effects in the Cognitive Domain: relateert deels ook aan beïnvloeding in hybride conflictvoering, waar vanaf 2018 meer aandacht voor is.
  - Semiconductor technologies: is een civiel-gedreven technologie die met name de laatste jaren in het defensiedomein meer aandacht heeft gekregen door de toenemende vraag naar geavanceerde elektronische systemen, zoals sensoren, communicatiemiddelen en wapensystemen, die hogere prestaties en efficiëntie vereisen. De snelle ontwikkelingen binnen halfgeleidertechnologieën bieden defensietoepassingen nieuwe mogelijkheden op het gebied van precisie, snelheid en dataverwerking.
  - Human resource Management & Organization: hiervoor is inmiddels meer aandacht binnen Defensie vanwege een noodzaak tot cultuurverandering om een adaptievere en innovatievere organisatie te realiseren. Ook de aanhoudende personele schaarste noopt tot meer kennis van defensiespecifiek personeelsbeleid.
  - System Engineering & Innovation: toenemende aandacht voor sneller innoveren is hier een drijvende kracht, evenals de inzichten dat Defensie zelf in haar SMART rollen nog meer differentiatie kan aanbrengen tussen SMART developer en SMART buyer, bijvoorbeeld door zelf bestaande producten te integreren (SMART integrator).
- De overige 48 subgebieden zijn op een of andere wijze wel te koppelen aan een of meerdere initiële DIS 2018 gebieden. Dat betekent nog niet dat daarmee beoordelingen en teksten 1-op-1 kunnen worden overgenomen. Naast de noodzaak om te actualiseren zien we ook dat bepaalde defensie basis-gebieden ofwel ruimer ofwel nauwer zijn gedefinieerd dan de initiële DIS 2018 lijsten, hetgeen een aanvulling of aanpassing van beoordelingen en teksten vereist.

Defensie-basisgebied	Subgebied	Beschrijving	DIS Kennisgebied	DIS Technologiegebied	DIS Industriele capacit.
1. Cyber & Elektronische Oorlogsvoering	1.1 Electronic Warfare	Capaciteiten voor de beheersing van het elektromagnetisch spectrum, in het bijzonder gericht op radar, communicatie en navigatie. Onderdelen zijn opbouw van situation awareness, bescherming van eigen capaciteiten, en het uitvoeren van offensieve acties.		Cyber, **EMA** & QC	
	1.2 Cyber Operations	Offensieve cyberactiviteiten gericht op het binnendringen en/of verstoren van ICT-systemen van opponenten.		**Cyber**, EMA & QC	
	1.3 Cyber and Electro-Magnetic Activities	Gecoördineerd inzetten van offensieve en defensieve activiteiten in het gebied waar elektronische oorlogsvoering en cyber overlappen, met specifieke aandacht voor sensor-, wapen- en communicatiesystemen.		**Cyber, EMA** & QC	
	1.4 Cybersecurity & Cryptography	Defensieve cyberactiviteiten gericht op de bescherming van de eigen ICT-systemen, en toepassing van cryptografische technieken voor het beveiligen van data en communicatie.	Network Infrastructure & **cyber security**	**Cyber**, EMA & QC	
2. Sensorsystemen	2.1 Radar	Systemen voor het waarnemen van objecten middels hoogfrequente (>100 MHz) elektromagnetische golven.	Situational Awareness	Sensoren	Waarnemings- en infovergaringssystemen
	2.2 Sonar	Systemen voor waarneming van objecten of communicatie onder water middels geluidsgolven.	Situational Awareness	Sensoren	Waarnemings- en infovergaringssystemen
	2.3 Electro-Optics & Infra Red	Systemen voor het waarnemen van objecten middels zichtbaar, ultraviolet of infrarood licht.	Situational Awareness	Sensoren	Waarnemings- en infovergaringssystemen
	2.4 Non-traditional Sensors	Overige sensoren, bijvoorbeeld voor positionering, navigatie en timing (PNT), voor het meten van fysische grootheden zoals magnetisme of gravitatie of voor het detecteren en/of identificeren van specifieke organismen of chemicaliën.	Situational Awareness	Sensoren	Waarnemings- en infovergaringssystemen
	2.5 Sensor fusion	Integratie en fusie van input afkomstig uit verschillende sensoren of andere bronnen (zoals inlichtingen) ter verbetering van de situation awareness.	Situational Awareness	Sensoren	Waarnemings- en infovergaringssystemen

Defensie-basisgebied	Subgebied	Beschrijving	DIS Kennisgebied	DIS Technologiegebied	DIS Industriele capacit.
3. Wapensystemen	3.1 Basic Weapon Technology	Technologie voor het afvuren of lanceren van munitie en raketten, voor optimalisatie van de dracht, voor geleiding en voor ontsteking.	Effectors		Wapensystemen
	3.2 High Energy Laser / Directed Energy Weapons	Wapens die hun effect genereren middels laserlicht of microgolf straling.	Effectors	DEW	Wapensystemen
	3.3 Guided and Hypersonic Weapons	Raketten of torpedo's die tijdens hun dracht actief worden bestuurd om een doel gericht te raken. Een belangrijke ontwikkeling betreft hypersone raketten die snelheden > Mach 5 kunnen bereiken en tevens manoeuvreerbaar zijn.	Effectors		Wapensystemen
	3.4 Lethality	De mate waarin munitie in staat is schade of (dodelijke) verwondingen te veroorzaken (wapen-doel interactie).	Effectors		Munitie
	3.5 Smart munition production and safe use	Het veilig en duurzaam ontwikkelen, produceren, gebruiken, vervoeren, opslaan en verwijderen van munitie en raketten. Omvat ook de verhoging van de inherente veiligheid en de levensduurbewaking.	Effectors		Munitie
4. Platformsystemen	4.1 Land Systems	Op land in te zetten bemenste platforms zoals tanks, (pantser)voertuigen, wapensystemen en geniematerieel.	Platforms		Platformen Land
	4.2 Maritime Systems	Bemenste maritieme platforms zoals fregatten, onderzeeboten, patrouilleschepen, mijnenjagers, en logistieke schepen.	Platforms		Platformen Maritiem
	4.3 Air Systems	Bemenste (gevechts- en transport) vliegtuigen en helikopters.	Platforms		Platformen Lucht
	4.4. Space Systems	(Constellaties van) satellieten, grondstations en satellietlanceersystemen.	Platforms	Space / Satellieten	Platformen Space
	4.5 Power & Energy Resilience	Energieopwekking voor en -gebruik van platforms, systemen en faciliteiten, met als belangrijke drijfveer het borgen van energiezekerheid.	Platforms		

Defensie-basisgebied	Subgebied	Beschrijving	DIS Kennisgebied	DIS Technologiegebied	DIS Industriele capacit.
	4.6 Signatures	Het beheersen en indien nodig beïnvloeden van radiofrequente, optische, infrarood, magnetische en akoestische signaturen van platforms, systemen of faciliteiten.	Platforms		
5. C3I en Digitalisering	5.1 Network Infrastructure & Communication	Communicatieapparatuur en -verbindingen en netwerkinfrastructuur om data te versturen en beschikbaar te krijgen.	**Network Infrastructure** & cyber security		Communicatie-systemen
	5.2 Information technology	Computers, dataopslag en software om data te creëren, verwerken en op te slaan.			Informatie-verwerkende systemen
	5.3 Intelligence	Verzamelen en integreren van informatie uit diverse bronnen zoals: mensen (HUMINT), media (OSINT), beeldmateriaal (IMINT), het elektromagnetisch spectrum (SIGINT) en het cyberdomein.	Situational Awareness		Inlichtingen-verwerkende systemen
	5.4 Decision support & Human control	Ondersteuning van menselijk beslissen en handelen binnen Command & Control, gebruikmakend van kennis over menselijk beslisgedrag. Belangrijk daarbij is het mogelijk maken van 'meaningful human control'.			Besluitvormings-ondersteunende systemen
	5.5 Command & Control	Ontwerp en inrichting van C2-concepten, -processen en -omgevingen alsmede de evaluatie van operationele effecten.	Command & Control		C2 systemen
	5.6 Digital transformation	De integratie van geavanceerde digitale technologieën en data-gedreven processen om concepten als genetwerkte besluitvorming en informatiegestuurd optreden mogelijk te maken.			Informatie-verwerkende systemen
6. Bescherming	6.1 CBRN	Bescherming tegen chemische, biologische, nucleaire en radiologische dreigingen. Dit omvat dreigingsanalyse, detectie, identificatie, bescherming, decontaminatie, diagnostiek en medische tegenmaatregelen.	Protection	Biotechnologie	
	6.2 Ballistic Protection	Bescherming van platforms, systemen en gebouwen tegen de uitwerking van projectielen en explosieven.	Protection		Platformbescherming

Defensie-basisgebied	Subgebied	Beschrijving	DIS Kennisgebied	DIS Technologiegebied	DIS Industriele capacit.
	6.3 Soldier Protection	Bescherming van personeel tegen letsel veroorzaakt door wapens of stressoren zoals hitte, koude, lawaai of trillingen.	Protection		
	6.4 Explosive Ordnance Disposal & Mine Counter Meas.	Identificatie, veiligstellen en vernietigen van explosieven en van land- en zeemijnen.	Protection		
	6.5 Counter Terrorism & Security	Bescherming en beveiliging van personen, materieel, informatie, activiteiten of infrastructuur tegen dreigingen zoals terrorisme, spionage, sabotage, ondermijning, criminaliteit alsmede schade zonder opzettelijk handelen.	Protection		
	6.6 (Counter) Hybrid	Strategieën en maatregelen om de gecombineerde inzet van traditionele militaire middelen en andere statelijke machtsmiddelen ten behoeve van hybride conflictvoering te detecteren, weerstaan en neutraliseren.			
7. Menselijk Presteren & Medicijnen	7.1 Human Performance & Resilience	Bepaling en verbetering van menselijk fysiek, cognitief en mentaal prestatievermogen (individueel en in teamverband), uitgezonderd verbetering dmv training. Tevens de bepaling en verbetering van weerbaarheid tegen fysieke, cognitieve of mentale belasting en tegen ongewenste beïnvloeding.	Personel readiness & Human performance	Human enhancement	
	7.2 Training, Education & Simulation	Methoden en systemen voor training, opleiding en gereedstelling, waaronder het gebruik van simulatie/simulatoren, 'serious games' en (digitale) leermiddelen.	Personel readiness & Human performance	Simulatie en Virtualisatie	Training en opleiding
	7.3 Effects in the Cognitive Domain	Psychologische, sociale en fysiologische factoren en methoden die ingezet worden voor beïnvloedingsoperaties.			
	7.4 Military Health	Medische en geestelijke gezondheidszorg voor militairen. Het omvat o.a. diagnose en therapie inclusief benodigde apparatuur en middelen.	Personel readiness & Human performance	Biotechnologie	Combat Service Support

Defensie-basisgebied	Subgebied	Beschrijving	DIS Kennisgebied	DIS Technologiegebied	DIS Industriele capacit.
8. Autonome & Onbemande Systemen	8.1 Unmanned Systems	Onbemande militaire platforms of systemen (land, lucht, zee) die op afstand bestuurd worden en/of autonome functionaliteit hebben.	Platforms	Robotica en autonome systemen	
	8.2 Autonomy	Het vermogen van platforms of systemen om zonder menselijke interventie (deel)taken uit te voeren en zich aan te passen aan veranderende omstandigheden. AI is daarvoor een belangrijke enabler.		Robotica en autonome systemen	
	8.3 Human Machine Teaming	Inrichting van de samenwerking tussen mensen en platforms of systemen met autonome functionaliteit, zodat de gezamenlijke taakuitvoering wordt geoptimaliseerd.		Mens-Systeem Integratie	
9. Logistiek	9.1 Smart and predictive maintenance	Methoden en tools gebaseerd op onder andere data-analyse, AI en IoT-sensoren om onderhoud proactief te plannen en uitval te minimaliseren.	Materiel Readiness & Logistics		Materieel-logistieke ondersteuning
	9.2 Supply chain management	Beheer van de volledige toeleveringsketen inclusief voorraadbeheer, van grondstoffen tot eindgebruiker, met nadruk op efficiëntie en beschikbaarheid.	Materiel Readiness & Logistics		Materieel-logistieke ondersteuning / Combat Service Support
	9.3 Transport	De verplaatsing van goederen, materieel en personeel over land, zee en lucht, inclusief optimalisatie en logistieke vervoersplanning.	Materiel Readiness & Logistics		Transportsystemen en -diensten
	9.4 Life Cycle Support Analysis	Beoordeling en planning van de ondersteuning van systemen gedurende de hele levensduur, inclusief levensduurkosten, vervanging en afstoting.	Materiel Readiness & Logistics		Materieel-logistieke ondersteuning
10. Defensie-toepasbare sleuteltechnologieën en -methodologieën	10.1 AI, Data Science & Machine Learning	Systemen en algoritmes die grote hoeveelheden data kunnen verwerken, die daardoor kunnen leren en zich verbeteren, om inzichten uit complexe data te genereren, of autonoom gedrag mogelijk te maken.		Artificiële Intelligentie	

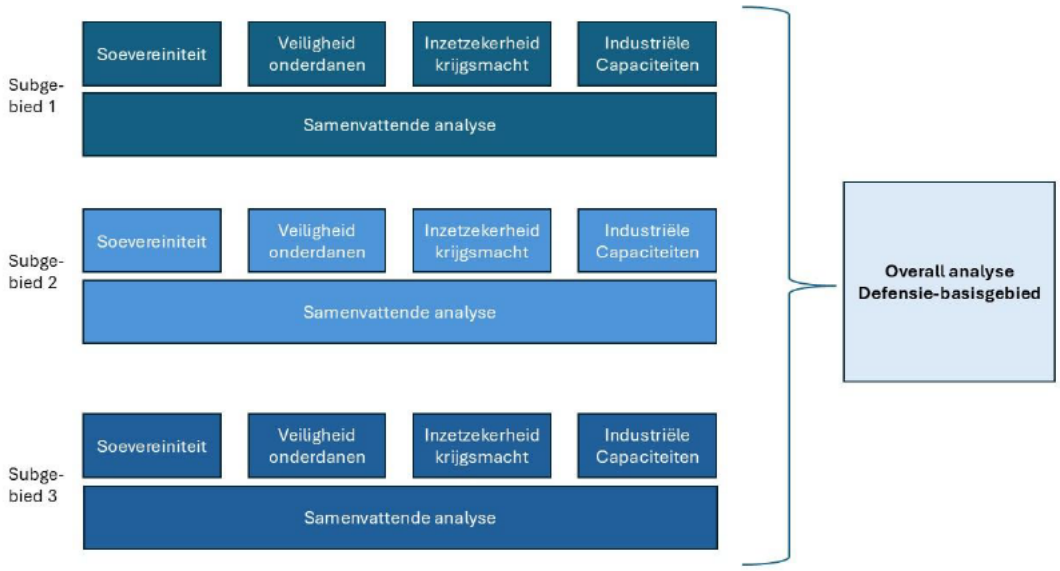
Defensie-basisgebied	Subgebied	Beschrijving	DIS Kennisgebied	DIS Technologiegebied	DIS Industriele capacit.
	10.2 Advanced Materials & Additive Manufacturing	Materialen die zijn ontworpen en vervaardigd om speciale eigenschappen te hebben, zodat ze bijvoorbeeld duurzamer zijn of sterkere structuren, betere bescherming of gereduceerde signaturen mogelijk maken. Omvat ook toepassing van methoden zoals 3D printing voor vervaardiging van materialen en structuren.		3D printing en nieuwe materialen	
	10.3 Modelling & Simulation	Het modelleren van omgevingen, personen, objecten en processen en het gebruik daarvan in simulaties en/of virtuele omgevingen. Toepassingen zijn onder meer verwerving, opleiding, training, missievoorbereiding en 'course of action'-analyse.		Simulatie en Virtualisatie	Training en opleiding
	10.4 Quantum Technologies	Technologieën die gebruik maken van quantum verschijnselen zoals verstrengeling, superpositie en tunneling. Deze worden toegepast in quantumsensoren, -communicatie en -computers.		Cyber, EMA & QC	
	10.5 Semiconductor technologies	Ontwerp, fabricage, verpakking en testen van halfgeleidercomponenten en sterk geminiaturiseerde elektronische subsystemen. Tevens de ontwikkeling en bouw van de machines om deze activiteiten uit te voeren.			
	10.6 Operational Analysis	Het analyseren en modelleren van militaire operaties om nieuwe militaire concepten te ontwikkelen, om besluitvorming (bijv. bij verwerving) te ondersteunen, middelen optimaal in te zetten en de effectiviteit van strategieën en tactieken te verbeteren.	Defence analysis		
	10.7 Strategic Foresight & Analysis	Continue en systematische analyse van trends en ontwikkelingen (o.a. demografische, economische, socioculturele, technologische, ecologische en politieke/juridische) en toekomstscenario's, ter ondersteuning van beleids- en investeringskeuzes.	Defence analysis		

Defensie-basisgebied	Subgebied	Beschrijving	DIS Kennisgebied	DIS Technologiegebied	DIS Industriele capacit.
	10.8 Human Resource Management & Organization	Ontwikkeling en toepassing van kennis over defensiespecifieke aspecten van personeelsmanagement en organisatie-inrichting. Dit omvat onder meer selectie, cultuur, adaptiviteit, leiderschap, diversiteit & inclusiviteit en ondersteuning van de familie.			
	10.9 Ethics & Legal	Ontwikkeling en toepassing van kennis over (oorlogs)recht, 'rules of engagement', ethisch gedrag en ethiek en juridische aspecten van de toepassing van militaire technologie.	Legal, ethical and moral implications		
	10.10 System Engineering & Innovation	Ontwerp, integratie, implementatie en instandhouding van complexe systemen, inclusief innovatiemanagement.			

6 Analyse wezenlijke belangen

In dit hoofdstuk wordt de uitwerking (operationalisering en beoordeling) van de wezenlijke belangen voor de tien Defensie-basisgebieden gedaan. Daarbij is er voor gekozen om dit gestructureerd te doen door steeds een analyse per subgebied te doen (dat zijn er in totaal 53) en niet per basisgebied als geheel. Daarbij is die analyse eerst gedaan voor elk van de drie wezenlijke belangen afzonderlijk, en tevens voor de industriële capaciteiten. Die laatste is toegevoegd aan de drie wezenlijke belangen, omdat daarmee nog explicieter een economisch belang of een strategisch belang kan worden geduid. Hierbij wordt gebruik gemaakt van actuele beleidsdocumenten; met name de DSII en de STRAIK-D bieden daarbij houvast. Waar mogelijk zijn overwegingen voorgesteld, en dus geen keuzes; uiteindelijke keuzes zijn immers aan Defensie en EZ. Verder zijn de vijf defensiedomeinen niet afzonderlijk opgevoerd, maar worden deze waar nodig en relevant wel benoemd in de verschillende uitwerkingen.

Op basis van deze vier analyses (drie wezenlijke belangen + industriële capaciteiten) is vervolgens een 'samenvattende analyse' per subgebied opgesteld. Daarnaast is een 'overall analyse' op elk Defensie-basisgebied toegevoegd. Dit is een beknopte samenvatting van de analyses van de subgebieden en zal steeds aan het begin van de betreffende paragraaf (defensie-basisgebied) worden gepresenteerd. Voor elke analyse is zoveel mogelijk teruggegrepen naar relevante beleidsdocumenten (zie Referenties, waarin ook de gebruikte afkortingen voor deze documenten zijn opgenomen), en zijn deze waar nodig ook genoemd.



Figuur 6.1: Overzicht van de systematische aanpak voor analyse per defensie-basisgebied.

De reden om de analyse zo gestructureerd en uitgebreid te doen, is dat op die wijze alle beoordelingen herleidbaar zijn en de argumenten puntsgewijs inzichtelijk zijn. Daarmee worden Defensie en EZ zoveel mogelijk in staat gesteld om strategische afwegingen te maken.

Verder dient te worden opgemerkt dat alle Defensie-basisgebieden de basis vormen voor de Defensie kennis- en technologiebasis. Zo zijn ze immers ook gekozen. Daarmee vormen ze feitelijk al een wezenlijk belang. Er zijn echter gradaties in wezenlijke belangen. Veel gebieden zijn cruciaal omdat, als ze weg zouden vallen, dit grote consequenties zal hebben voor essentiële capaciteiten van de krijgsmacht en/of de veiligheid van Nederland c.q. de Nederlandse bevolking. Zonder munitie geen slagkracht, zonder logistiek geen operatie, zonder medische zorg geen voortzettingsvermogen etc. Bij een aantal gebieden is het echter zo dat die, zeker op de kortere termijn, minder grote gevolgen hebben voor de soevereiniteit, onderdanen en/of inzetzekerheid, bijvoorbeeld omdat het om nieuwe technologie gaat die huidige capaciteiten op termijn kunnen vervangen en/of veranderen. Met de huidige capaciteiten kan dan nog wel slagkracht of ondersteuning daarvoor worden geleverd. Echter op termijn zouden tegenstanders met nieuwe technologie deze (huidige) slagkracht kunnen inperken of zelfs neutraliseren. Vanwege de complexiteit en de daaraan gerelateerde afhankelijkheden en aannames is ervoor gekozen om in deze analyse gradaties in elk geval niet te kwantificeren. In kwalitatieve zin wordt wel zoveel mogelijk geduid waar het wezenlijk belang op gebaseerd is en welke effecten dat, met name voor Defensie, heeft.

Ook wordt per technologie(sub)gebied een indicatie gegeven welke SMART-rollen het meest voor de hand liggen voor Defensie om hierbij te vervullen (zie Figuur 1.2 voor de set van SMART-rollen). Deze indicaties zijn deels ontleend aan beleidsdocumenten zoals DIS en DSII, en deels beredeneerd op basis van het analyseren en vergelijken van technologie(sub)gebieden. De aangegeven SMART-rollen zijn nadrukkelijk indicatief, want het is uiteindelijk aan Defensie om hier beleidskeuzes over te maken.

Tot slot, waar relevant zijn verwijzingen in de tabellen opgenomen. Deze betreffen:

- Onderlinge verwijzingen: er zijn tal van onderlinge afhankelijkheden tussen de Defensie-basisgebieden (en subgebieden). Waar relevant zijn deze verwijzingen opgenomen in deze vorm: [zie ook par. XX]
- Argumenten: in de diverse kolommen staan argumenten, deze zijn deels afgeleid uit relevante brondocumenten (dit wordt aangeduid via *[ref. YY]*) en deels uit argumenten zoals die in hoofdstuk 4 (argumenten voor nationale ontwikkeling) zijn verwoord. Dit wordt aangeduid in deze vorm: [zie ook naam argument].

6.1 Cyber en Elektronische Oorlogsvoering

Overall analyse: Het basisgebied Cyber en Elektronische Oorlogsvoering is van wezenlijk belang voor de Nederlandse krijgsmacht. De onderliggende subgebieden zijn essentieel voor defensieoptreden in alle domeinen; zonder kennis en technologie in dit basisgebied komt de inzetzekerheid van de krijgsmacht in het geding. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Ondanks een relatief sterke industrieel-technische kennisbasis in Nederland, zijn er momenteel op diverse subgebieden echter (sterke) afhankelijkheden van buitenlandse leveranciers. Gezien de geopolitieke ontwikkelingen is streven naar meer autonomie in dit basisgebied te overwegen. De meest voor de hand liggende SMART-rol voor alle subgebieden is: Developer.

Onderstaand volgt de systematische analyse van elk subgebied, gebaseerd op een analyse van de drie wezenlijke belangen en de industriële capaciteiten voor dat subgebied.

Subgebied	Nederlandse soevereiniteit	Veiligheid van onderdanen	Inzetzekerheid in defensiedomeinen	Industriële Capaciteiten
1.1 Electronic Warfare (EW)	✓ Ondersteunt autonomie in het elektromagnetisch spectrum; voorkomt afhankelijkheid van buitenlandse systemen en interventies. *[ref. DN2024; DSII; HCSS WB]*	✓ Bescherming tegen vijandige signalen die navigatie, communicatie en/of medische systemen kunnen verstoren. *[ref. DN2024; DB MH]*	✓ EW is cruciaal voor commandovoering, bescherming en operatiecapaciteit in alle domeinen. *[ref. DN2024; DSII; HCSS WB]*	✓ Nederland heeft veel expertise op het gebied van digitale signaalverwerking bij zowel kennisinstellingen als enkele bedrijven. Dit is belangrijk voor het detecteren en verstoren van vijandelijke communicatie en radar. Daarnaast werkt Nederland vaak binnen NAVO-programma's aan gezamenlijke EW-capaciteiten, maar is daarbij ook nog sterk afhankelijk van NAVO-bondgenoten. *[ref. DIS]*
Samenvattend: Kennis en technologie inzake EW zijn van een wezenlijk belang. EW is cruciaal voor bescherming, commandovoering en operatiecapaciteit in alle domeinen. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Op dit moment is inzet in het defensiedomein echter nog sterk afhankelijk van NAVO-bondgenoten; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. [zie ook 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rol voor Defensie is: Developer.				

1.2 Cyber Operations	✓ Offensieve cybercapaciteit is vanwege afschrikking een belangrijk middel om soevereiniteit in het informatiedomein te borgen. *[Ref. DN2024; MIVD; HCSS WB]*	✓ Door het preventief inzetten van offensieve cyber kunnen potentiële cyberdreigingen worden weggenomen, waarmee de samenleving wordt beschermd tegen cyberaanvallen op vitale infrastructuur, financiën, communicatie, etc. Daar zitten overigens wel juridische aspecten aan vast. *[Ref. DB MH; MIVD; DN2024]*	✓ Binnen het concept van Multi Domein Operaties is offensieve cyber een belangrijke capaciteit waarmee opponenten het gebruik van het cyberdomein kan worden ontzegd danwel worden bemoeilijkt. Daarmee is het een belangrijke capaciteit om het eigen optreden zo effectief mogelijk te kunnen uitvoeren zonder (teveel) verstoringen. *[Ref. DN2024; HCSS WB]*	✓ Nederland heeft een sterke basis in de technologieën die nodig zijn voor cyberweerbaarheid, zoals chipdesign, crypto, ICT en netwerken. De sector beschikt op meerdere technologiegebieden over fundamenteel en toegepast onderzoek. Het opbouwen van offensieve cybercapaciteit gaat echter nog verder. De vraag is of daarbij een industriële capaciteit bij kan/mag ondersteunen. In elk geval zal daarbij geen afhankelijkheid van buitenlandse leveranciers geaccepteerd kunnen/mogen worden. *[ref. DIS]*
Samenvattend: Kennis en technologie op het gebied van cyber operations (offensieve cyber capaciteit) zijn van wezenlijk belang voor defensieoptreden in alle domeinen; het is onmisbaar binnen het concept van Multi Domein Operaties. Ook draagt het bij aan nationale veiligheid door bescherming van vitale infrastructuur, zowel vanuit afschrikking als vanuit preventieve inzet. Offensieve cyber is een nationale aangelegenheid die momenteel door Defensie zelf wordt ontwikkeld. De vraag is of daarbij een industriële capaciteit bij kan/mag ondersteunen. In elk geval zal daarbij geen afhankelijkheid van buitenlandse leveranciers geaccepteerd kunnen/mogen worden. [zie ook 4.10 Informatie(systemen) als doelwit en wapen; 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rol voor Defensie is: Developer.				
1.3 Cyber and Electromagnetic Activities (CEMA)	✓ Belangrijk voor het beheersen van het elektromagnetisch spectrum, inclusief GPS, radar, en communicatie. *[Ref. DSII; DN2024]*	✓ Vermindert risico op verstoring van civiele systemen (bijv. transport, gezondheidszorg). *[Ref. DB MH; VS NL]*	✓ Essentieel voor inzetzekerheid door onderbreking en verstoring van vijandelijke communicatie en door bescherming van eigen systemen. Zonder CEMA is inzetzekerheid van de krijgsmacht in het geding. *[Ref. DN2024; HCSS WB]*	✓ Nederland heeft een sterke basis in de technologieën die nodig zijn voor cyberweerbaarheid, zoals chipdesign, crypto, ICT en netwerken. De sector beschikt op meerdere technologiegebieden over fundamenteel en toegepast onderzoek. *[ref. DIS]*

Samenvattend: Kennis en technologie inzake CEMA zijn van wezenlijk belang voor defensieoptreden in alle domeinen; zonder actuele kennis en technologie inzake CEMA komt de inzetzekerheid van de krijgsmacht in het geding. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Nederland beschikt over een goede eigen industriële basis op dit gebied waarmee afhankelijkheden van buitenlandse actoren kan worden verkleind. [zie ook 4.10 Informatie(systemen) als doelwit en wapen; 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rol voor Defensie is: Developer.				
1.4 Cybersecurity & Cryptography	✓ Essentieel voor digitale soevereiniteit en bescherming van defensie-informatie en kritieke infrastructuur. *[Ref. DSII; DN2024; VS NL]*	✓ Beschermt vitale infrastructuur, persoonsgegevens en nationale systemen tegen digitale aanvallen. *[Ref. DB MH; MIVD; VS NL]*	✓ Randvoorwaarde voor veilige communicatie in operaties en interoperabiliteit met NAVO-partners. *[Ref. DN2024; HCSS WB]*	✓ Nederland heeft een sterke basis in de technologieën die nodig zijn voor cyberweerbaarheid, zoals chipdesign, crypto, ICT en netwerken. De sector beschikt op meerdere technologiegebieden over fundamenteel en toegepast onderzoek. Op dit moment is er voor cruciale componenten van cryptografie echter nog een grote afhankelijkheid van niet-Europese leveranciers. *[ref. DIS]*
Samenvattend: Kennis en technologie op het gebied van cyber security en cryptografie (ook een sterke relatie met post-quantum crypto, zie ook par. 10.4) zijn van wezenlijk belang; veilige communicatie is een randvoorwaarde voor defensieoptreden in alle domeinen. Ook draagt het bij aan nationale veiligheid door bescherming van vitale infrastructuur. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Cruciale componenten van cryptografie zijn nu echter nog vaak afkomstig van niet-Europese leveranciers; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. [zie ook 4.10 Informatie(systemen) als doelwit en wapen; 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rol voor Defensie is: Developer.				

6.2 Sensorsystemen

Overall analyse: Defensie heeft op basis van de behoeftes van de krijgsmacht (pull) en de kennis, technologische en industriële defensiebasis (push) vijf gebieden gekozen waar extra in wordt geïnvesteerd. Uit de bredere sterke basis, is Sensoren als één van deze vijf gebieden gekozen waar Defensie als SMART developer kan optreden. Binnen Nederland bestaat al een sterke radar-industrie waarbij Defensie, industrie en de kennisinstellingen samen in staat zijn om toonaangevende high-end radarsystemen te ontwikkelen waarmee Defensie binnen NAVO (mede-)koploper is. Defensie en de Nederlandse kennisinstituten en industrie hebben als ambitie om daarin voorop te blijven lopen in Europa en high-end radarchips en –technologie (o.a. compact, energiezuinig) te ontwikkelen, waarvan 50% van de componenten lokaal wordt geproduceerd, en de integratie en assemblage volledig in kan Nederland plaatsvinden. Ook op onderwater-akoestiek moet Nederland de komende jaren haar industriële positie versterken, om daarmee beter beschermd te zijn tegen (nieuwe) vormen van seabed warfare.
Door een grotere SMART rol (developer maar ook integrator en specifier) te vervullen, kan Nederland en Defensie in het bijzonder haar wezenlijke belangen (bescherming vitale infra, bescherming Noordzee en bescherming eigen eenheden) beter behartigen. Met de snel evoluerende variëteit aan complexe dreigingen is het hebben van een accurate en snelle Situational Awareness kritisch en zijn Multi Domein Operaties (binnen NAVO) en Informatiegestuurd Optreden strategische kernconcepten. Daarbij zijn multisensoren elementair en is het deels in eigen beheer kunnen ontwikkelen van sensoren en/of sensorsoftware van groot belang. De meest voor de hand liggende SMART-rollen voor de diverse subgebieden zijn: Developer, Integrator en Specifier.

Onderstaand volgt de systematische analyse van elk subgebied, gebaseerd op een analyse van de drie wezenlijke belangen en de industriële capaciteiten voor dat subgebied.

Subgebied	Nederlandse soevereiniteit	Veiligheid van onderdanen	Inzetzekerheid in defensiedomeinen	Industriële Capaciteiten
2.1 Radar	✓ Kritieke technologie en capaciteit voor autonome detectie en bewaking van het eigen luchtruim en de territoriale wateren. Daarmee wordt de soevereiniteit verdedigd. *[ref. DN2024; DSII; HCSS WB]*	✓ Kritieke technologie en capaciteit voor autonome detectie en bewaking van het eigen luchtruim en de territoriale wateren. Daarmee worden de veiligheid en economische belangen beschermd. *[ref. DN2024; DB MH]*	✓ Essentieel voor situational awareness in bijna alle domeinen, voor geïntegreerd optreden binnen NAVO en voor early warning capaciteit (evt. spacebased). Met de high-tech (mil specs) radarsystemen die binnen de NLD gouden driehoek worden ontwikkeld, verkrijgt Defensie	✓ Er is een sterke radar-industrie basis in NLD. Via Nederland-Radarland kan de marine als SMART developer/ integrator/ specifier zelf radars (mee-)ontwikkelen die het beste passen bij de NLD eisen en daarmee een grote effectiviteit en veiligheid garanderen voor de NLD fregatten.

			(en de marine i.h.b.) een unieke niche/excellence capaciteit. Vanwege het taakkritische karakter van radars dienen de specificaties ervan geheim te blijven. *[ref. DN2024; HCSS WB]*	✓ Defensie en de Nederlandse kennisinstituten en industrie hebben de ambitie geformuleerd om in 2035 voorop te lopen in Europa in de ontwikkeling van high-end radarchips en –technologie (o.a. compact, energiezuinig), waarvan 50% van de componenten lokaal worden geproduceerd; integratie en assemblage vinden volledig in Nederland plaats. *[ref. DSII]*
Samenvattend: Radar kennis, technologie en (sub)systemen zijn van wezenlijk belang. De marine is door de eigen NLD industriebasis in staat om de beste high-tech radars te ontwikkelen die bijdragen aan een hoge effectiviteit en veiligheid van de fregatten, en die daarmee zowel een NAVO capability invullen als ook de veiligheid in de territoriale wateren garanderen. In het luchtdomein zorgen deze in NLD ontwikkelde high-tech radars voor de bescherming van het nationale luchtruim. Sommige specificaties moeten geheim blijven vanwege de taakkritische prestaties [zie ook 4.1 Geheime opdrachten].Defensie heeft Sensoren als één van de vijf gebieden gekozen waar extra in wordt geïnvesteerd en waar Defensie als SMART developer kan optreden. Radars zijn binnen het gebied Sensoren essentieel voor de krijgsmacht van vandaag en morgen en Nederland heeft hier een leidende positie in internationale waardenketens, vanuit kennis- en industrieperspectief, onder meer op de ontwikkeling van high-end radarchips en -technologie. De meest voor de hand liggende SMART-rol voor Defensie is: Developer.				
2.2 Sonar	✓ Onderwatersystemen zoals sonar zijn een kritieke capaciteit voor de beheersing van maritieme soevereiniteit, o.a. voor het beschermen van (onderzeese) infrastructuur op/in de Noordzee en voor het beschermen van maritieme aanvoerlijnen tbv NAVO-operaties. *[ref. DSII; DN2024]*	✓ Bescherming van voor NLD vitale maritieme onderwater-infrastructuur (energie en datakabels, pijpleidingen) en van de civiele scheepvaart is van belang voor de economische, digitale en ook fysieke veiligheid van NLD. Detectie van onderwater-dreigingen zoals sabotage, mijnen	✓ Voor de bescherming en inzetbaarheid van de NLD maritieme vloot is effectieve detectiecapaciteit tegen de toenemende dreiging van onderzeeboten, ook in nabije wateren, essentieel. Zelf ontwikkelde sensoren (of deelsystemen zoals algoritmes) waarborgen dat de technologie en detectiemogelijkheden niet bekend zijn bij potentiële	✓ Hoewel de sonar ontwikkel-industrie grotendeels internationaal is, heeft Nederland via onder andere de kennisinstituten een SMART developer/specifier rol als het gaat om de sonar-algoritmes. Daarmee kan de marine high-end sonarprestaties verkrijgen. ✓ Nederland heeft als ambitie voor 2035 om Europees en NAVO-koploper te zijn in (onderwater)

		etc. is daarvoor een kritische enabler. *[ref. VS NL; DN2024]*	tegenstanders, waardoor het moeilijker wordt deze te omzeilen. Specificaties van deze systemen dienen zelfs geheim te blijven en maakt het nationaal ontwikkelen daarvan wenselijk. *[ref. DN2024; HCSS WB]*	akoestiek en daarmee ook een eigen ontwikkel-industrie na te streven, hetgeen gegeven de genoemde wezenlijke (veiligheids)belangen een kritische enabler is. *[ref. DSII]*
Samenvattend: Sonar kennis, technologie en (sub)systemen zijn van wezenlijk belang. Het verdedigen en beschermen van de eigen vloot, maar ook het beschermen van de havens en de vitale onderwater-infrastructuur, mede door de toenemende seabed warfare dreigingen, is voor Defensie en Nederland kritisch. Sommige specificaties moeten geheim blijven vanwege de taakkritische prestaties [zie ook 4.1 Geheime opdrachten]. Met de toenemende dreiging van vijandelijke onderzeeboten in nabije wateren is sonartechnologie- en capaciteit alsmaar belangrijker geworden, hetgeen ook een grotere nationale ontwikkeling van sonar (deel)systemen rechtvaardigt. Defensie vervult nu een SMART specifier rol in het algemeen en SMART developer rol op het gebied van software (algoritmes). Het lijkt voor de hand te liggen dat de SMART developer rol in de toekomst zal toenemen gezien de wezenlijke (veiligheids)belangen die de economische, digitale en ook fysieke veiligheid van NLD raken.				
2.3 Electro-Optics & Infrared	✓ Optische sensoren, zoals EO/IR-apparatuur, stellen de krijgsmacht in staat om op grote afstand en onder moeilijke omstandigheden (zoals 's nachts of bij slecht weer) gedetailleerde beelden te verkrijgen om zo grenzen effectief te bewaken en illegale activiteiten vroegtijdig te detecteren.	✓ Noodzakelijk voor civiel-militaire inzet zoals grensbewaking, rampenbestrijding, bescherming van burgerdoelen. *[ref. VS NL; DN2024]*	✓ Een belangrijk middel voor effectieve ISR, nauwkeurige targeting en wapen-doel geleiding en daarmee een kritische enabler voor bescherming van de eigen eenheden. Er is sterke focus op miniaturisatie, precisie, en integreerbaarheid in bredere C4ISR-systemen *[ref. DV2035; HCSS WB]* ✓ Binnen de strategische concepten Multi Domein Operaties en Informatiegestuurd optreden is de mix van verschillende sensoren, waaronder ook EO/IR sensoren, kritisch aangezien daarmee zowel veelsoortige informatie als redundantie kan worden verkregen.	✓ De NLD industriële sector op het gebied van elektro-optische systemen voor bewaking, beveiliging en detectie van lucht /land /zee doelen is relatief klein maar zeer gespecialiseerd, innovatief en sterk verweven met zowel de defensiesector als met internationale partners en toeleveringsketens. ✓ Defensie ambieert om in 2035 te beschikken over modulair inzetbare multisensorsystemen met hoogwaardige Nederlandse technologie geïntegreerd op alle bemenste en onbemenste platformen op land, lucht en zee. *[ref. DSII]*

Samenvattend: EO & IR kennis, technologie en (sub)systemen zijn van wezenlijk belang. Naast het belang ervan voor nationale soevereiniteit en bescherming, zijn ze met name kritische voor een effectieve en veilige inzet van defensie eenheden. Veel systemen zijn van de markt te verkrijgen. Mogelijk dat specifieke software nodig is voor nationale doelen en belangen, zoals grensbewaking en bewaking van vitale objecten, die Defensie dan in samenwerking met Nederlandse onderzoeksinstituten en bedrijven in eigen beheer kan beproeven. Om in de komende jaren strategische concepten zoals Multi Domein Operaties en Informatiegestuurd Optreden verder vorm te kunnen geven, zijn EO/IR (optische) sensoren een belangrijke schakel in de mix van multisensoren. In toenemende mate zal Defensie 'eigen' slimme software willen kunnen integreren in deze sensoren en in het netwerk van multisensoren. [zie ook 4.7 Integratievermogen; 4.9 Informatie(systemen) als middel] Daarmee zullen ook nationale ontwikkelingen op dit gebied toenemen. De meest voor de hand liggende SMART-rollen voor Defensie zijn: Integrator en Specifier.				
2.4 Non-traditional sensors	✓ Veel vitale infrastructuur en processen zijn afhankelijk van GPS, die verstoord kan worden. Alternatieve sensoren voor PNT zijn in ontwikkeling. Eigen soevereiniteit hierop wint aan belang, Europese samenwerking is daarbij wel aan te bevelen. *[ref. DV2035; DSII]*	✓ Bescherming of redundantie van PNT sensoren voor bescherming vitale infrastructuur en processen. ✓ Landgebonden akoestische sensoren zorgen voor snelle dreigingsdetectie van drone-aanvallen, een dreiging die toeneemt en gericht kan zijn tegen vitale infra en of high-level/massale events. ✓ Sensoren die biologische en chemische agentia kunnen detecteren en identificeren zijn kritisch voor terroristische B/C aanvallen. *[ref. VS NL; MIVD]*	✓ Inzetbaarheid van de krijgsmacht is in alle domeinen zeer sterk afhankelijk van PNT sensoren. C3I, inzet van drones, inzet van geleide wapens, logistiek etc., alle functies van optreden kunnen tegenwoordig niet meer zonder PNT. ✓ Landgebonden akoestische sensoren gericht op snelle dreigingsdetectie en bronlokalisatie van artillerie-, vuurwapen/sniper- en droneaanvallen zorgen voor een hoge mate van bescherming van militaire eenheden. De toenemende drone dreiging en ook artillerie dreiging vereisen een mix van sensoren. *[ref. DN2024; DV2035]*	✓ De NLD industriële sector is relatief klein, PNT-capaciteit is vaak ingebed in bredere platformen van internationale OEM's. Door de toename van drone dreigingen en GPS storingen, is er wel een groeimarkt voor alternatieve PNT (zoals quantumsensoren) en akoestische sensoren. ✓ Defensie ambieert om in 2030 te beschikken over een nationale modulaire en open PNT architectuur voor sensorfusie van diverse PNT-sensoren om robuuste plaats- en tijdbepaling mogelijk te maken in militaire toepassingen en kritieke infrastructuur. Dit zal een opschaling van NLD industrie op PNT-sensoren/architectuur vereisen. *[ref. DSII]*

Samenvattend: Met name PNT sensoren en de non-traditionele sensoren gericht op detectie van drones en detectie van B/C dreigingenvormen een wezenlijk belang. De NLD industriële sector is relatief klein, PNT-capaciteit is vaak ingebed in bredere platformen van internationale OEM's. Door de zeer sterke afhankelijkheid van PNT sensoren, met name voor de inzetbaarheid van de krijgsmacht, is een deels nationale ontwikkeling, eventueel in samenwerking met enkele strategische Europese partnerlanden, te overwegen. Daarnaast dienen de civiel-gedreven ontwikkelingen actief gevolgd te worden. De meest voor de hand liggende SMART-rollen voor Defensie zijn: een SMART specifier rol (akoestische sensoren) en deels een SMART developer rol (alternatieve PNT sensoren en architecturen).				
2.5 Sensor fusion	✓ Sensorfusie combineert data uit verschillende soorten sensoren tot één coherent en actueel beeld van de situatie. Dit zorgt voor een veel vollediger en betrouwbaarder inzicht dan afzonderlijke sensoren kunnen bieden. Hierdoor kan de krijgsmacht sneller en nauwkeuriger dreigingen detecteren en beoordelen in alle domeinen. Dit versterkt de soevereiniteit van een land, omdat het in staat is autonoom en effectief controle uit te oefenen over zijn grondgebied en luchtruim, zonder (teveel) afhankelijk te zijn van externe inlichtingen.	✓ Multi-sensor fusie is cruciaal bij het tijdig detecteren van de toenemende moeilijke (hybride) dreigingen (verdacht gedrag zoals sabotage, drones). Eigen kennis en technologie-ontwikkeling zorgt voor betere bescherming van vitale assets met een specifiek karakter. *[ref. VS NL]*	✓ Multi Domein Optreden is de kern van het toekomstig optreden in internationale coalities, met name NAVO. Sensor-fusie is een sine qua non voor dit type optreden, met name om ook niet-conventionele en nieuwe dreigingen te kunnen detecteren. Software en algoritmes die dit mogelijk maken dienen zoveel mogelijk binnen die coalities/partners ontwikkeld te worden om zo interoperabiliteit te waarborgen. ✓ Voor het verbeteren van de geformuleerde maatregelen voor informatiegestuurd optreden zal Defensie ook verdergaande integratie van sensoren, besluitvormers, (wapen)systemen en ondersteunende capaciteiten moeten realiseren. ✓ Defensie ambieert om in 2030 over hardware- en softwareoplossingen te beschikken voor data- en sensorfusie van sensoren in verschillende	✓ Hoewel in NLD weinig massaproductie van sensoren zelf bestaat, ligt de focus wel op het koppelen van sensoren tot geïntegreerde systemen (bv. in C4ISR-ketens). NLD bedrijven en kennisinstellingen leveren daarbij vooral software, algoritmen, en systeemarchitectuur. ✓ Defensie ambieert om in 2035 een datalaag te hebben met explainable AI en sensorfusie die grotere aantallen multifunctionele sensoren integreert op alle platformen. Nederlandse industrie zal daarbij als integrator hardware en softwarelagen leveren, terwijl Defensie eigenaar blijft van de militaire tactische software en AI.

			domeinen, waar nodig in lijn met NAVO-standaarden. ✓ Defensie ambieert om in 2030 te beschikken over geavanceerde, in Nederland ontwikkelde multisensortechnologie die *fit for purpose* is (met kleinere Size, Weight and Power – SWaP) zodat Defensie de beoogde (veelal kleine) onbemenste platformen kan invoeren. *[ref. DN2024, DSII, STRAIIK]*	
Samenvattend: Sensor fusie is van wezenlijk belang. Het is cruciaal voor de bescherming van het eigen grondgebied, de vitale infrastructuur en militaire eenheden in inzetgebieden. Nationale ontwikkelingen zullen toenemen, met name op software maar ook in toenemende mate hardware voor sensorfusie. Internationale samenwerking met partners zal daarbij wel een belangrijk element zijn, zeker met het oog op het toenemende belang Multi Domain Operaties en zeker ook joint en combined optreden binnen NAVO waarbij interoperabiliteit tussen sensoren noodzakelijk is. [zie ook 4.9 Informatie(systemen) als middel] De meest voor de hand liggende SMART-rollen voor Defensie zijn: een SMART integrator/specifier rol en op software (en deels hardware) niveau zelfs een SMART developer rol.				

6.3 Wapensystemen

Overall analyse: Soeverein militair optreden is onlosmakelijk verbonden met de beschikbaarheid en beheersing van wapensystemen. Het Basisgebied Wapensystemen raakt daarom rechtstreeks aan alle drie de wezenlijke veiligheidsbelangen: zonder regie over het ontwerp, de inzet en de beschikbaarheid van wapentechnologieën verliest Nederland een stuk beleidsvrijheid (soevereiniteit), kan het onvoldoende bescherming bieden aan civiele doelen (veiligheid onderdanen), en wordt operationele inzetbaarheid ondermijnd (inzetzekerheid). Binnen dit domein kunnen voor Defensie verschillende SMART-rollen worden onderscheiden: een ontwikkelrol (developer) op het gebied van smart munitie en basiswapentechnologie, een gebruikers- en specificatierol bij lethality, en een beperkte rol bij hypersonische wapens en directed energy weapons. Deze combinatie weerspiegelt zowel bestaande capaciteiten als strategische afhankelijkheden. Versterking van zeggenschap over kritieke wapensystemen – met name in precisie en effectkeuze – is essentieel om technologische autonomie en inzetzekerheid veilig te stellen. De meest voor de hand liggende SMART-rollen voor de diverse subgebieden zijn: Developer, Specifier, Buyer, Maintainer en User.

Onderstaand volgt de systematische analyse van elk subgebied, gebaseerd op een analyse van de drie wezenlijke belangen en de industriële capaciteiten voor dat subgebied.

Subgebied	Nederlandse soevereiniteit	Veiligheid onderdanen	Inzetzekerheid in defensiedomeinen	Industriële capaciteiten
3.1 Basic Weapon Technology	✓ Zelfstandig kunnen ontwikkelen en beheren van conventionele wapentechnologieën voorkomt strategische afhankelijkheid van buitenlandse actoren en versterkt nationale zeggenschap over specificaties, inzetregels en interoperabiliteit (technologische autonomie). *[ref. HCSS WB]*	✓ Basiswapentechnologie draagt slechts indirect bij aan civiele bescherming, maar speelt wel een rol in bij het beschermen van onderdanen tijdens een gewapend conflict. *[ref. DIS, DN2024]*	✓ Vormt fundament voor inzetbare wapencapaciteiten in alle domeinen; kennis van deze technologie is onmisbaar voor een effectieve en veilige inzet ervan. *[ref. HCSS WB, DIS, DN2024]*	✓ Nederland bezit beperkte eigen ontwikkelcapaciteit in fundamentele wapentechnologie. Er is wel een kennisbasis op gebied van ballistiek en explosieven-effecten. Nichecomponenten (zoals looptechniek en coatings) worden geleverd door enkele MKB's. De productiecapaciteit als geheel is afhankelijk van buitenlandse leveranciers. Het ontbreken van nationale kennis leidt tot directe afhankelijkheid van buitenlandse leveranciers voor onderhoud, aanpassing en inzetzekerheid. *[ref. HCSS WB, DIS*
Samenvattend: Basic Weapon Technology is van wezenlijk belang: het vormt een fundament voor inzetbare wapencapaciteiten in alle defensiedomeinen behalve het cyberdomein. Zonder basiskennis is er geen onderhoud, aanpassing of veilige inzet van wapensystemen mogelijk. Soevereine controle ontbreekt momenteel; afhankelijkheid van buitenlandse specificaties belemmert nationale inzetvrijheid. Gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. [zie ook 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rol voor Defensie is Developer vanwege de strategische noodzaak om technologie en specificaties te beheersen.				
3.2 High Energy Laser / Directed Energy Weapons	✓ Biedt potentieel strategisch voordeel bij opkomende dreigingen mits Nederland eigen DEW-capaciteit ontwikkelt; voorkomt afhankelijkheid van derden. *[ref. DIS, HCSS WB]*	✓ Potentieel inzetbaar tegen drones en raketten die civiele doelen zoals vliegvelden bedreigen. Vanwege de dichtbevolktheid en infrastructurele gevoeligheid van Nederland, zijn snelle defensieve systemen zoals	✓ DEW biedt potentieel snelle, domein overstijgende respons tegen high-speed dreigingen in met name het luchtdomein, en is daarmee een	✓ Nederland heeft geen operationele systemen of significante industriële footprint in DEW. R&D gebeurt via kennisinstituten en is gericht op testen en validatie, niet op implementatie. De technologie is nieuw en vereist voortdurende innovatie als Nederland hier onafhankelijk in wil kunnen optreden. *[ref. DIS, DSII, HCSS WB, STRAIIK]*

		DEW extra waardevol. Bijdrage is nog wel afhankelijk van volwassenwording van operationeel gebruik. *[ref. DIS, DV2035, HCSS WB]*	belangrijke *enabler* voor de bescherming van eigen eenheden. *[ref. DIS, DV2035, HCSS WB]*	
Samenvattend: DEW is van wezenlijk belang omdat het potentieel operationeel overwicht en bescherming tegen drones en raketten biedt. [zie ook 4.4 Operationeel voordeel] Bij civiele bescherming speelt DEW mogelijk een rol, mits er verdere ontwikkeling plaatsvindt. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Nederland heeft momentreel echter geen grote industrieel-technische kennisbasis op dit vlak, wat strategische afhankelijkheid creëert. Gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. [zie ook 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Buyer en Specifier.				
3.3 Guided and Hypersonic Weapons	✓ Deze systemen zijn essentieel voor deep precision strike-capaciteit binnen NAVO. Nederland beschikt hier zelf niet over. Deze afhankelijkheid beperkt de beleidsvrijheid om zelfstandig in te grijpen bij dreiging of escalatie, en ondermijnt de mogelijkheid tot nationale afschrikking op afstand. *[ref. DIS, DN2024, HCSS WB]*	✓ Deze wapens zijn niet ontworpen voor directe civiele bescherming, maar dragen indirect bij via strategische afschrikking van tegenstanders met langeafstands-capaciteiten. *[ref. DIS, DSII, DN2024, HCSS WB]*	✓ Belangrijk voor defensieoptreden in het lucht-, zee- en ruimtedomein. Zonder *guided/ hypersonic systems* is deelname aan high-end precisieoperaties beperkt. Nodig voor langeafstandsinzet en afschrikking. *[ref. DIS, DSII, DV2035, HCSS WB]*	✓ Nederland heeft geen eigen capaciteit voor ontwikkeling of productie van (hyper)sonische wapens. Er is volledige afhankelijkheid van bondgenoten (m.n. VS, Frankrijk) voor aanschaf en instandhouding. Bovendien is de 'toegang' hiertoe beperkt, omdat er niet veel leveranciers zijn. Dit zou ervoor kunnen pleiten om nationaal (danwel met enkele Europese partnerlanden) op ontwikkeling in te gaan zetten. *[ref. DIS, DN2024]*
Samenvattend: Gerichte en (hyper)sonische wapens zijn van wezenlijk belang omdat ze een operationeel voordeel bieden: ze zijn onmisbaar voor langeafstandsinzet en strategisch optreden. [zie ook 4.4 Operationeel voordeel] Indirect zijn ze relevant voor civiele veiligheid via afschrikking. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Momenteel beschikt Nederland niet zelf over deze systemen en is ook de toeleveringsketen beperkt, waardoor Nederland zeer afhankelijk is van enkele andere landen. [zie 4.8 Beheersing toeleveringsketen] Dit beperkt nationale afschrikking en beleidsvrijheid. Gezien de geopolitieke ontwikkelingen is streven naar meer (Europese) samenwerking en deels autonomie te overwegen. De meest voor de hand liggende SMART-rollen voor Defensie zijn momenteel: Buyer en Specifier.				

3.4 Lethality	✓ Vergroot autonomie in keuze voor effecttype, precisie, en proportionaliteit. Zonder zeggenschap over deze technologie is Nederland afhankelijk van externe kwaliteitsnormen. *[ref. DIS, DSII, HCSS WB]*	✓ Het effect voor onderdanen op NLD grondgebied is vooral indirect, maar er is wel effect op burgers in inzetgebieden. Precisie en effectselectie binnen lethale systemen dragen bij aan beperking van nevenschade, wat civiele bescherming in operatiegebieden versterkt (zeker bij operaties in stedelijk gebied). *[ref. DIS, DN2024]*	✓ Zorgt voor operationeel overwicht in verschillende scenario's. Doseerbare lethaliteit is van belang om collateral damage te minimaliseren. *[ref. DIS, DN2024]*	✓ Nederland speelt een rol in subsystemen, bijvoorbeeld precisie-onderdelen zoals fire control en sensors (kennisontwikkeling en integratie), maar heeft geen volledige systeemregie, geen ontwerpautoriteit en geen zelfstandige munitie-/effectproductie voor de lethale eindcomponenten. Doordat precisie munitiesystemen nu vaak afhankelijk zijn van externe leveranciers, creëert dit kwetsbaarheden. *[ref. DIS, DSII]*
Samenvattend: Kennis en technologie op het gebied van Lethality zijn van wezenlijk belang omdat systemen met verschillende/aanpasbare lethaliteit cruciaal zijn voor soevereine inzetkeuze, effectiviteit én beperking van nevenschade. Zonder eigen zeggenschap over effecttypes is Nederland afhankelijk van externe normen. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Nederland ontwikkelt deels subsystemen (zoals sensoren), maar niet de eindproducten. Specificatie en gebruiksvormgeving zijn vanuit nationaal oogpunt cruciaal. Gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. [zie ook 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Specifier en User.				
3.5 Smart munition production and safe use	✓ Soevereine controle over munitie is noodzakelijk om nationale inzetcriteria, proportionaliteit en interoperabiliteit te garanderen in nationale of coalitiecontext. Precisie- en slimme munitie zijn gevoelig en operationeel vertrouwelijk; nationale productie zou kwetsbaarheden beperken. *[ref. DIS,*	✓ Het effect voor onderdanen op NLD grondgebied is vooral indirect, maar er is wel effect op burgers in inzetgebieden: verhoogde precisie draagt bij aan beperking van nevenschade in inzetgebieden. *[ref. DIS, DN2024, VS NL]*	✓ Nationale beschikbaarheid van munitie garandeert continuïteit van operaties in (langdurige) missies. *[ref. DIS, DN2024]*	✓ Nederland beschikt via bedrijven en kennisinstituten over nichekennis op het gebied van munitie-integratie, veiligheid, en logistiek. Hier bestaat een bewezen eigen capaciteit. Voor grondstoffen en subsystemen is Nederland deels afhankelijk van buitenlandse toeleveranciers. *[ref. DIS, STRAIIK]*

	DN2024, HCSS WB, STRAIIK]			
Samenvattend: Slimme munitieproductie en het veilige gebruik daarvan is van wezenlijk belang omdat het gevoelige en operationeel vertrouwelijke processen betreft. Bovendien verhoogt het precisie en proportionaliteit, waarover soevereine controle gewenst is. Slimme munitie draagt eveneens bij aan ongewenste nevenschade bij defensieinzet. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand; nationale productie zou kwetsbaarheden beperken. [zie 4.8 Beheersing toeleveringsketen] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer, Maintainer en User; er is een expliciete nationale ambitie om (onderdelen van) slimme munitie nationaal te ontwerpen, integreren en in stand te houden.				

6.4 Platformsystemen

Overall analyse: Platformsystemen zijn de ruggengraat van de krijgsmacht en bepalen in hoge mate de inzetzekerheid van de krijgsmacht. Om die reden vervullen ze een wezenlijk belang. Voor maritieme platformen geldt dat de Marine een internationale toonaangevende (niche) positie heeft vanwege de SMART developer/integrator rol die ze kan vervullen doordat Nederland over een volledig en integraal marinebouwcluster beschikt dat in staat is om maritieme platformen geheel autonoom te ontwerpen en te ontwikkelen. Voor de andere platformsystemen (land, lucht) is Nederland afhankelijk van buitenlandse leveranciers (OEMs), veelal van partnerlanden, maar kan in de toeleveringsketen een grotere rol worden overwogen en geambieerd. Ook in de logistiek en het onderhoud van platformen zou een grotere rol niet alleen economische voordelen opleveren maar ook meer zeggenschap over de inzetbaarheid van deze platformen. Voor het ruimtedomein geldt dat Nederland wel zelfstandig in staat is om micro- of nanosatellieten te ontwikkelen, maar voor de grote(re) satellieten is er afhankelijkheid van buitenlandse leveranciers, veelal uit het civiele domein. De meest voor de hand liggende SMART-rollen voor de diverse subgebieden zijn: Developer, Integrator, Specifier, Maintainer en User.

Onderstaand volgt de systematische analyse van elk subgebied, gebaseerd op een analyse van de drie wezenlijke belangen en de industriële capaciteiten voor dat subgebied.

Subgebied	Nederlandse soevereiniteit	Veiligheid van onderdanen	Inzetzekerheid in defensiedomeinen	Industriële Capaciteiten
4.1 Land Systems	✓ Landsystemen hebben een belangrijke taak in de fysieke controle over het NLD grondgebied. Zonder adequate landcapaciteit kan een land zijn territoriale integriteit en soevereiniteit niet afdwingen, vooral bij grensoverschrijdende dreigingen.	✓ Landsystemen dragen bij aan civiele veiligheid bij terrorisme, pandemieën of militaire bijstand in eigen land. *[ref. DN2024]*	✓ Vereist voor optreden in hybride dreigingen en missies met lage tot hoge intensiteit. *[ref. DB MH, HCSS WB]* ✓ Voor nationale taakkritische/-specifieke functies zoals commando-/informatie-integratie worden subsystemen vaak nationaal (mee-)ontwikkeld om interoperabiliteit te combineren met autonomie. *[ref. DSII; HCSS WB]* ✓ Voor taakkritische landsystemen (met name de hoofdwapensystemen) is kennis wenselijk. Om als systeemintegrator te kunnen optreden, dus als SMART developer op het geïntegreerd niveau. *[ref. HCSS WB]*	✓ Nederland fungeert als toeleverancier voor buitenlandse OEMs (bv. CV90) en integreert componenten. Op sensoren heeft Nederland een nichepositie die ook in het landdomein verder kan worden uitgenut. [zie ook par. 6.2] ✓ Vanwege de variëteit aan landsystemen is schaalvoordeel in ontwikkeling en productie te behalen door Europese industriële samenwerking (bijv. PESCO). De nationale eisen zijn goed in lijn te brengen met de internationale eisen en met wat er op de markt beschikbaar is. *[ref. HCSS WB; DSII; DIS]* ✓ De NL industrie kan wel in toenemende mate een rol verkrijgen in de logistiek en het onderhoud van landsystemen. [zie ook par. 6.9] Door hier meer nationale autonomie op te verkrijgen, kan er ook meer gestuurd worden op de inzetbaarheid van deze systemen.
Samenvattend: Landsystems is van wezenlijk belang. Veel ontwikkeling en productie kan binnen internationale samenwerking worden gerealiseerd en waarbij Defensie als SMART user optreedt. Als het gaat om het inbrengen van specificaties van taakkritische/-specifieke subsystemen (C2) kan zelfs een SMART specifier rol worden vervuld. Op sensorontwikkeling en het integreren van sensoren binnen landsystemen kan Defensie een SMART integrator rol vervullen. Voor taakkritische landsystemen (met name de hoofdwapensystemen) is kennis wenselijk om als systeemintegrator te kunnen optreden, dus als SMART developer op het geïntegreerd niveau. [zie ook 4.7 Integratievermogen] Het ligt voor de hand om in toenemende mate ook een SMART maintainer rol te ambiëren, door de NLD industrie een rol in de logistiek en onderhoud van landsystemen te laten vervullen.				

4.2 Maritime Systems	✓ Marinebouw (inclusief systeemintegratie, ontwerp en onderhoud) is cruciaal voor strategische autonomie. *[ref. DSII; DIS]* ✓ Het handhaven van de maritieme veiligheid, het bestrijden van drugshandel en andere illegale activiteiten, en het bieden van hulp bij noodsituaties ter bescherming van de soevereiniteit van de overzeese Koninkrijksdelen.	✓ Maritieme systemen en platformen hebben een belangrijke taak in de bescherming van zeevaartroutes, havens en kritieke infrastructuur op en nabij de Noordzee. *[ref. DN2024; DV2035]* ✓ Bescherming van Nederlandse koopvaardijschepen, ook buiten de eigen territoriale wateren *[ref. HCSS WB]*	✓ Kerncapaciteit van de Nederlandse Marine en middel voor strategische afschrikking, maritieme mobiliteit en NAVO-opdrachten. *[ref. HCSS WB; DV2035]* ✓ Bijdrage aan anti-piraterij missies, zowel in NAVO- als EU-verband.	✓ Nederland bezit een volledig marinebouwcluster waarbij de gehele keten van kennis, ontwerp en uiteindelijk ontwikkeling van alle componenten van een maritiem systeem/platform voorhanden zijn. *[ref. DSII; DIS]* ✓ De Nederlandse marine heeft zelf een belangrijke bijdrage in deze keten, zowel in de ontwerpfase als de integratie-fase. ✓ Maritieme platformen worden veelal in relatief kleine series gebouwd waardoor schaalvoordeel door aankoop via buitenlandse leverancier minder speelt dan in het land- en luchtdomein, en waardoor ontwikkeling in eigen land ervoor kan zorgen dat de platformen beter aansluiten op specifieke nationale eisen ten aanzien van bemannings- en commandovoeringsconcepten.
Samenvattend: Maritime Systems vormen een cruciaal wezenlijk belang vanwege de bescherming van de overzeese Koninkrijksdelen, het beschermen van de Noordzee en de kritieke infrastructuur in de eigen territoriale wateren. Daarnaast heeft de Marine een internationale toonaangevende (niche) positie vanwege de SMART developer/integrator rol die ze kan vervullen doordat Nederland over een volledig en integraal marinebouwcluster beschikt dat in staat is om maritieme platformen geheel autonoom te ontwerpen en te ontwikkelen. Met dit Nederlands product 'koopt' de Marine de beste kwaliteit voor een goede prijs en tevens een product dat volledig is afgestemd op de Nederlandse maat van bedrijfsvoering (opleiding, logistiek, commandovoering etc.). [zie ook 4.3 Nederlandse karakteristieken; 4.13 Maatwerk voor kleine landen]				
4.3 Air Systems	✓ Air systems (F-16/-F35) zijn cruciaal voor de luchtruimbewaking van Nederland (Quick Reaction Alert taak).	✓ Cruciaal voor de luchtruimbewaking van Nederland (Quick Reaction Alert taak) en de bescherming van	✓ Verdediging tegen lucht-/raketdreiging en deelname aan NAVO high-end operations. *[ref. DV2035]*	✓ Nederlandse industrie levert hoogwaardige subsystemen (bv. landing gear, onderhoud F-35). *[ref. DSII; DIS]*

	✓ Echter Nederland is volledig afhankelijk van buitenlandse platforms zoals de F-35, met beperkte zeggenschap over updates en ITAR-onderwerpen. *[ref. DSII; HCSS WB]*	burgers in internationale conflictgebieden. ✓ Ook snelle inzet van helikopters bij nationale crises/rampen. *[ref. DN2024; DB MH]*	✓ Defensie gebruikt buitenlandse platforms (bv. F-35), maar heeft een onderhoudsrol en kan daardoor bijdragen aan inzetgereedheid. *[ref. DSII; DV2035]*	✓ De mate van integratie van de diverse functionele subsystemen in vliegende (bemenste) platformen is over het algemeen hoog, zowel technisch als in termen van certificering. Het ontwikkelen van geavanceerde militaire vliegende platformen is daarom voorbehouden aan een beperkte set van producenten, veelal geassocieerd met grotere landen. *[ref. HCSS WB]*
Samenvattend: Air systems zijn van wezenlijk belang vanwege de luchtruimbewaking van Nederland en de bijdrage die Nederland daarmee kan leveren aan (de snelle inzet bij) high-end NAVO-operaties. De mate van integratie van de diverse functionele subsystemen in vliegende platformen is over het algemeen hoog, waardoor de ontwikkeling ervan is voorbehouden aan een beperkte set van producenten. De mate van standaardisatie is groot, de ruimte voor (nationaal) maatwerk is klein. Nationale ontwikkeling van jachtvliegtuigen, helikopters en transportvliegtuigen is in de praktijk niet haalbaar. Wel kan Nederland participeren in multinationale ontwikkel- en productieprogramma's, in de praktijk veelal onder leiding van de VS, maar ook in Europees verband. Het ligt voor de hand dat Defensie de volgende SMART rollen vervuld: User, Maintainer of (op niches in deelsystemen) Developer.				
4.4 Space Systems	✓ Satellietontwikkeling voor tactische communicatie (bv. nanosats) wordt gepositioneerd als nichegebied met nationale ambities. In 2028 ambieert Defensie om strategische autonomie en soevereiniteit te waarborgen door een sterke Nederlandse OEM-waardeketen in het ruimtedomein. *[ref. DSII; HCSS WB]*	✓ Toegenomen belang voor civiele bescherming door early warning, communicatie en navigatie. *[ref. DV2035; DN2024]*	✓ De ruimte is het vijfde militaire operationele domein en is van onmisbaar strategisch, tactisch en operationeel belang voor het goed functioneren van de krijgsmacht. Het gaat daarbij met name om het gebruik van satellieten die essentieel zijn voor de navigatie, positie- en tijdsbepaling, communicatie en aardobservatie, ofwel het multidomein en informatiegestuurd optreden van de krijgsmacht. *[ref. DSII]*	✓ NLD industrie heeft een positie in kleine satellieten; grootschalige platforms worden alleen in andere landen ontwikkeld. *[ref. DSII; DIS]* ✓ Satellietcommunicatiesystemen zijn in het algemeen op de internationale markt verkrijgbaar, maar militaire eisen zoals beveiliging en robuustheid zijn daarbij wel aandachtspunten. ✓ Daarnaast zullen in belangrijke mate diensten worden ingekocht die geen bijzondere eigen ontwikkeling vergen (het Europese Galileo-programma is een voorbeeld). *[ref. HCSS WB]*

			✓ Belangrijk voor ISR, NAVO-communicatie, en interoperabiliteit met bondgenoten. *[ref. HCSS WB; DB MH]*	✓ Defensie heeft Ruimtetechnologie aangewezen als één van de 5 NLD gebieden waarin extra wordt geïnvesteerd, met het oogmerk om daarin ook als SMART developer op te treden.
Samenvattend: Het steeds grotere belang van space systems voor C4ISR, gekoppeld aan de groeiende mogelijkheden om nationaal satellieten te kunnen lanceren en inzetten, rechtvaardigt een koppeling van ruimtetoepassingen in het militaire domein aan wezenlijke belangen. Tegelijk geldt dat een belangrijk deel van de ruimte-infrastructuur internationaal is en in toenemende mate commercieel, met name het inkopen van diensten die geen bijzondere eigen ontwikkeling vergen. Dit gebied vraagt een combinatie van mee ontwikkelen op het gebied van per missie operationeel in te zetten micro- of nanosatellieten en het volgen van de ontwikkelingen in de commerciële dienstensector voor aardobservatie, communicatie en navigatiediensten. Gezien de geopolitieke ontwikkelingen lijkt het wel belangrijk om afhankelijkheden van niet-Europese leveranciers te beperken. Samenwerking met Europese ruimtevaartpartners is daarom cruciaal. Het ligt voor de hand dat Defensie op niches een SMART developer rol zal vervullen (mede ook vanwege de ambitie om Ruimtetechnologie als één van de 5 NLD-gebieden aan te wijzen), en voor de rest een SMART specifier rol. [zie ook 4.13 Maatwerk voor kleine landen]				
4.5 Power & Energy Resilience	✓ De afhankelijkheid van andere, niet-partnerlanden voor energie, grondstoffen en halffabricaten en de bedreiging door spionage in Nederland, verzwakt niet alleen het economisch verdienvermogen, maar ondergraaft ook de slagkracht van de krijgsmacht. Daarom wordt ingezet op het verminderen en voorkomen van risicovolle strategische afhankelijkheden, het beschermen van vitale processen en het voorkomen van ongewenste	NVT	✓ Bevoorradings-onafhankelijke energievoorziening verhoogt mobiliteit en voortzettingsvermogen en inzetduur. *[ref. HCSS WB; DV2035]* ✓In geval van een nationale black out zal Defensie haar nationale taken moeten kunnen vervullen (*last man standing).* Redundantie (resilience) in energiebehoefte is daarvoor een pre. ✓ Kennis en in enige mate grip op voortstuwingstechnologie (emissieloos, hybride) is essentieel voor autonomie over energieverbruik en inzetcondities. *[ref. DSII; HCSS WB]*	✓ Innovatie vindt in Nederland plaats bij Defensie zelf, kennisinstituten en private partijen; maar producten en systemen worden internationaal aangeschaft. *[ref. DSII]* ✓ Voor voortstuwings- en energiesystemen van oppervlakteschepen kan, op basis van eigen ontwerp, gebruik worden gemaakt van de civiele ontwikkelingen en beroep op de markt worden gedaan.

	overdracht van kennis en technologie, via onder meer Nationale Grondstoffen Strategie [2022] en Risicovolle Strategische Afhankelijkheden [kamerbrief 13 jan. 2025]. *[ref. DSII]*			
Samenvattend: Power & Energy resilience zijn van wezenlijk belang voor de inzetzekerheid van de krijgsmacht, zowel voor nationale als internationale taken. Veel technologie en systemen zijn civiel beschikbaar, vaak ook bij internationale leveranciers. Daarnaast zal Defensie vanwege de huidige afhankelijkheid van niet-partnerlanden meer zelfvoorzienend moeten worden, al dan niet via samenwerking met sterke partnerlanden. [zie ook 4.11 Toegang tot capaciteiten; 4.12 Strategische autonomie en continuïteit] Voor maritieme systemen ligt het voor de hand dat Defensie in elk geval als SMART specifier/integrator moet kunnen optreden.				
4.6 Signatures	✓ Eigen ontwikkeling danwel controle van signaturen van militaire platformen minimaliseert het risico dat vijanden inzicht krijgen in kwetsbaarheden of sterktes van nationale systemen. *[ref. DSII; HCSS WB]*	NVT	✓ Vermindert kans op detectie van eigen eenheden in vijandelijke omgeving, verhoogt operationele overleving en daarmee ook inzetzekerheid. *[ref. HCSS WB; DV2035]* ✓ In 2029 beschikken eenheden van CZSK over een geautomatiseerde coördinatie voor de inzet van hardkill, softkill en signatuurmanagement door de eigen eenheid om daarmee overlevingsvermogen te vergroten.*[ref. DSII]*	✓ Ontwikkeling van kennis bij kennisinstituten en defensiegerelateerde industrie (deels ook ontwikkeling), maar veelal afhankelijk van buitenlandse systemen en materialen. *[ref. DSII]* ✓ Hoewel Nederland slimme materialen als focusgebied heeft gedefinieerd, richten de voorziene slimme materialen zich niet direct op het verminderen van signaturen (maar wel op bescherming tegen munitie en explosieven). [zie ook par. 6.10]
Samenvattend: Signaturen zijn van wezenlijk belang omdat ze de overlevingskans van Defensie eenheden bepalen. Hoewel eigen ontwikkeling een voordeel in autonomie en soevereiniteit oplevert, zeker in een wereld van snel veranderende geopolitieke ontwikkelingen en relaties, is Nederland afhankelijk van buitenlandse leveranciers van platformen die ook de signaturen van die platformen bepalen. Met de kennis die Defensie zelf in huis heeft en die er bij de defensiegerelateerde kennisinstituten is, ligt het voor de hand dat Defensie in elk geval een SMART specifier rol zou kunnen vervullen. Voor de maritieme platformen geldt hier een uitzondering vanwege de eigen ontwerp- en ontwikkelcapaciteit: hier kan Defensie de SMART developer rol vervullen.				

6.5 C3I en Digitalisering

Overall analyse: Het basisgebied C3I en Digitalisering is van wezenlijk belang voor de Nederlandse krijgsmacht. De onderliggende subgebieden zijn essentieel voor het Defensieoptreden in alle domeinen; zonder betrouwbare informatie, communicatie en Command & Control is defensieinzet vrijwel onmogelijk. Nationale zeggenschap over dit soort systemen voorkomt dat politieke en/of operationele sturing afhankelijk wordt van externe partijen. Het minimaliseren van afhankelijkheden van buitenlandse partijen (zoals cloud- en backboneproviders, software- en hardwareleveranciers) ligt daarom voor de hand. Op veel subgebieden zijn er momenteel echter (soms aanzienlijke) afhankelijkheden van deze buitenlandse leveranciers. Gezien de geopolitieke ontwikkelingen is streven naar meer autonomie in dit basisgebied te overwegen. De voor de hand liggende SMART-rollen zijn wisselend: overwegend Developer en Specifier en soms tevens User en Maintainer.

Onderstaand volgt de systematische analyse van elk subgebied, gebaseerd op een analyse van de drie wezenlijke belangen en de industriële capaciteiten voor dat subgebied.

Subgebied	Nederlandse soevereiniteit	Veiligheid van onderdanen	Inzetzekerheid in defensiedomeinen	Industriële Capaciteiten
5.1 Network Infrastructure & Communication	✓ Onafhankelijke controle over tactische en strategische netwerken is essentieel om cruciale communicatie niet. afhankelijk te maken van derden. *[ref. DIS; HCSS WB]*	✓ Ondersteunt civiele bijstand (C2000, netwerken voor rampenbestrijding). Bescherming van communicatie-infrastructuur is randvoorwaarde. *[ref. HCSS WB; VS NL]*	✓ Veilige netwerken zijn cruciaal voor interoperabiliteit en commandovoering in alle defensiedomeinen. Betrouwbare communicatie is een randvoorwaarde voor elk defensieoptreden. *[ref. DN2024; DIS]*	✓ Nederland beschikt wel over enige niche-kennis in (tactische) communicatie, maar is momenteel in grote mate afhankelijk van buitenlandse leveranciers zoals cloud- en backboneproviders. *[ref. DIS]*
Samenvattend: Samenvattend: Kennis en technologie inzake Network Infrastructure & Communication zijn van een wezenlijk belang. Network Infrastructure & Communication is cruciaal voor defensieoptreden in alle domeinen; betrouwbare communicatie is een randvoorwaarde voor elke defensieinzet. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Op dit moment is Defensie echter nog sterk afhankelijk van buitenlandse toeleveranciers zoals cloud- en backboneproviders; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. [zie ook 4.9 Informatie(systemen) als middel; 4.12 Strategische autonomie en continuiteit] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer en Maintainer.				

5.2 Information Technology (IT)	✓ Zeggenschap over eigen IT-architectuur voorkomt strategische kwetsbaarheden en datalekken. *[ref. DIS; DV2035]*	✓ IT-weerbaarheid voorkomt maatschappelijke verstoring door cyberaanvallen. ✓ IT is onderdeel van de nationale vitale infrastructuur. *[ref. HCSS WB; DN2024]*	✓ IT is onmisbaar voor informatiegestuurd optreden en integratie van wapensystemen. Betrouwbare IT is een randvoorwaarde voor elke defensieinzet *[ref. DIS; DV2035]*	✓ Nederland heeft een aantal sterke cybersecurity-capaciteiten (o.a. cryptografie en netwerken), maar is momenteel nog in grote mate afhankelijk van internationale hardware- en softwareleveranciers. [zie ook par. 6.1] *[ref. DIS]*
Samenvattend: Kennis en technologie inzake Information Technology (IT) zijn van een wezenlijk belang. IT is onmisbaar voor defensieoptreden in alle domeinen. Zeggenschap over eigen IT-architectuur voorkomt strategische kwetsbaarheden en datalekken. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Op dit moment is Defensie echter nog sterk afhankelijk van internationale hardware- en softwareleveranciers; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. [zie ook 4.9 Informatie(systemen) als middel; 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Maintainer en Specifier.				
5.3 Intelligence	✓ Een zelfstandige inlichtingenpositie versterkt soevereine beleidskeuzes en inzetbesluiten. *[ref. DIS; DN2024]*	✓ Inlichtingen zijn een randvoorwaarde voor bescherming van burgers in conflictgebieden en tegen (hybride) dreigingen. *[ref. HCSS WB; VS NL]*	✓ Intelligence is cruciaal bij het maken van onderbouwde keuzes wat betreft militaire inzet en is essentieel voor defensieoptreden in dynamische omgevingen. *[ref. DIS; DV2035]*	✓ De intelligence taak is in Nederland belegd bij de MIVD en AIVD. Deze diensten maken tevens gebruik van strategische partnerschappen met buitenlandse diensten. Ook enkele andere Nederlandse niche-spelers dragen bij aan analysecapaciteit. Er zijn wel beperkingen in autonome SIGINT/IMINT-verwerking. *[ref. DIS]*

Samenvattend: Kennis en technologie op het gebied van Intelligence zijn van een wezenlijk belang. Intelligence is essentieel voor defensieoptreden in alle domeinen: het is cruciaal bij het maken van onderbouwde keuzes wat betreft militaire inzet en is essentieel voor defensieoptreden in dynamische omgevingen. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Op dit moment is Defensie echter nog deels afhankelijk van buitenlandse partijen bij de verwerking van bepaalde soorten intelligence; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. [zie ook 4.9 Informatie(systemen) als middel; 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Specifier en Maintainer.				
5.4 Decision Support & Human Control	✓ Besluitvorming op basis van eigen informatiesystemen vermindert het risico van buitenlandse beïnvloeding en versterkt strategische autonomie. *[ref. DIS; HCSS WB]*	✓ Dit heeft vooral indirect effect: degelijke besluitvorming voorkomt fouten en escalatie die schadelijke gevolgen voor burgers kunnen hebben. *[ref. DIS]*	✓ Belangrijk voor informatiegestuurd optreden in alle domeinen. *[ref. DV2035; DIS]* ✓ Maakt ook de versnelling van C2 mogelijk om zo de tegenstander voor te blijven. Tevens betere en snellere besluiten met minder mensen gebaseerd op meer informatie (of soms data).	✓ Er lopen in Nederland enkele initiatieven op AI en decision support [zie ook par. 6.10], maar voor kerntechnologieën en grootschalige applicatieontwikkelingen is Nederland momenteel sterk afhankelijk van buitenlandse leveranciers. *[ref. DIS]*
Samenvattend: Kennis en technologie op het gebied van Decision Support & Human Control zijn van een wezenlijk belang. Decision Support & Human Control is belangrijk voor defensieoptreden in alle domeinen; besluitvorming op basis van eigen informatiesystemen en algoritmiek vermindert het risico van buitenlandse beïnvloeding. Ook is besluitvorming erg bepaald door de Nederlandse cultuur en wijze van optreden en vereist daardoor vaak maatwerk. [zie ook 4.3 Nederlandse karakteristieken] Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Op dit moment is Defensie echter nog sterk afhankelijk van buitenlandse leveranciers; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. De meest voor de hand liggende SMART-rollen voor Defensie zijn: Specifier en Developer.				
5.5 Command & Control (C2)	✓ Nationale zeggenschap over C2-systemen, -processen en -concepten voorkomt dat politieke en/of operationele sturing afhankelijk wordt van externe partijen. *[ref. DIS; HCSS WB]*	✓ Essentieel bij nationale inzet (rampenbestrijding, evacuaties); voorkomt miscommunicatie. *[ref. DN2024; HCSS WB]*	✓ Essentieel voor defensieoptreden in alle domeinen. Zonder C2 is defensieinzet vrijwel onmogelijk *[ref. DIS; DV2035]*	✓ Nederland bezit wel enige nichekennis wat betreft commandosystemen, maar volledige C2-integratiecapaciteit ontbreekt. *[ref. DIS]*

Samenvattend: Kennis en technologie op het gebied van Command & Control (C2) zijn van een wezenlijk belang. C2 is belangrijk voor defensieoptreden in alle domeinen en vormt een integrale component in het optreden; zonder C2 is defensieinzet vrijwel onmogelijk. [zie ook 4.3 Nederlandse karakteristieken] Nationale zeggenschap over C2-systemen, -processen en -concepten voorkomt dat politieke en/of operationele sturing afhankelijk wordt van externe partijen. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Op dit moment is Defensie echter nog voor een aanzienlijk deel afhankelijk van buitenlandse leveranciers; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. De meest voor de hand liggende SMART-rollen voor Defensie zijn: Maintainer en Specifier.				
5.6 Digital Transformation	✓ Zonder regie op digitale transformatie dreigt verlies van sturingskracht op technologie-adoptie en interoperabiliteit, waardoor Nederland niet/minder soeverein is in het ontwikkelen van rijksbrede digitalisering. *[ref. DN2024; DIS]*	✓ Dit heeft vooral indirect effect: het draagt bij aan de weerbaarheid van vitale systemen (bijvoorbeeld logistiek en medische inzet). *[ref. HCSS WB; VS NL]*	✓ Digitale transformatie is belangrijk voor informatiegestuurd en adaptief optreden in moderne conflicten. *[ref. DV2035; DN2024]*	✓ Nederland investeert o.a. via BITS/DIANA in innovaties. Civiele technologie is over het algemeen leidend, maar er zijn defensiespecifieke groeizones zoals AI en edge computing. Deels is Nederland nog wel afhankelijk van buitenlandse kennis en technologie. *[ref. DN2024]*
Samenvattend: Kennis en technologie op het gebied van Digital Transformation zijn van een wezenlijk belang. Digital Transformation is belangrijk voor defensieoptreden in alle domeinen met het oog op informatiegestuurd en adaptief optreden in moderne conflicten. [zie ook 4.9 Informatie(systemen) als middel] Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Op dit moment is Defensie echter nog deels afhankelijk van buitenlandse leveranciers; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. De meest voor de hand liggende SMART-rollen voor Defensie zijn: Specifier en User.				

6.6 Bescherming

Overall analyse: Het basisgebied Bescherming omvat een breed kennis-, technologie- en industriegebied, en is van wezenlijk belang voor de veiligheid van Nederland, haar burgers en de krijgsmacht. Het betreft niet alleen de fysieke veiligheid maar ook digitale, economische, ecologische en sociale veiligheid. Aangezien landen een eigen taak en verantwoordelijkheid hebben tegen met name hybride en terrorisme dreigingen, en die dreigingen veelal tegen specifieke zwakheden van een land zijn gericht, is het onder eigen beheer hebben van verdedigingsmiddelen een kritische succesfactor. Nederland (en dito de krijgsmacht) heeft op tal van gebieden de mogelijkheden om SMART developer, SMART integrator of SMART specifier te zijn. Daarbij geldt dat internationale samenwerking met vertrouwde partners en met mogelijke onderlinge afhankelijkheden in de keten goed denkbaar is.

Onderstaand volgt de systematische analyse van elk subgebied, gebaseerd op een analyse van de drie wezenlijke belangen en de industriële capaciteiten voor dat subgebied.

Subgebied	Nederlandse soevereiniteit	Veiligheid van onderdanen	Inzetzekerheid in defensiedomeinen	Industriële Capaciteiten
6.1 CBRN	✓ Voor bescherming tegen aanslagen of aanvallen met chemische, biologische, radiologische of nucleaire (CBRN) wapens is zelfstandige capaciteit belangrijk om afhankelijkheid van andere actoren te beperken.	✓ De dreiging van terroristische aanslagen op Nederlands grondgebied met inbegrip van aanslagen of aanvallen met CBRN-middelen wordt als reëel risico gezien. Bescherming daartegen is derhalve noodzakelijk. *[ref. RRNV]*	✓ Recente conflicten en oorlogen hebben laten zien dat ook militaire eenheden doelwit kunnen zijn van CBRN-aanvallen danwel in CBRN-*contaminated* gebieden moeten optreden. ✓ Door de democratisering van technologie en i.h.b. ook CBR-wapens groeit het gevaar dat een tegenstander nog onbekende biologische, chemische of radiologische strijdmiddelen ontwikkelt en inzet. De verspreiding van tactische ('kleinschalige') kernwapens vergroot de kans op escalatie. *[ref. DV2035]*	✓ NLD sector is compact en met name gericht op chemische sensoren. ✓ Voor nucleaire/radiologische componenten is er een sterke afhankelijkheid van NAVO/EU partners. ✓ Biologische detectie is innovatief en biedt kansen. *[ref. TV2024]*
Samenvattend: CBRN-kennis, -technologie en -(sub)systemen zijn van wezenlijk belang. Voor CBRN-bescherming in het kader van de nationale veiligheid en ingezette eenheden is nationale autonomie gewenst. [zie ook 4.2 Existentiële dreigingen] Daarbij kan ook een wederkerige samenwerking met vertrouwde internationale partners een rol spelen, bijvoorbeeld door met hen (opnieuw) goede afspraken te maken over wederzijdse kennisuitwisseling en het delen van (dure) testfaciliteiten. Voor B/C bescherming is de mate waarop Nederland autonomie kan verkrijgen groter dan voor R/N-bescherming gezien de industriële positie. Biologische detectie is innovatief en heeft ook veel civiele toepassingen, en biedt daardoor zelfs kansen op groei van eigen industrie. Op R/N-bescherming zal binnen de EU/NAVO samenwerking dienen plaats te vinden. De meest voor de hand liggende SMART rollen voor Defensie zijn: Developer rol op B/C-bescherming (met bi-/trilaterale partners) en Specifier/User rol op R/N-bescherming.				

6.2 Ballistic Protection	✓ De NLD soevereiniteit wordt versterkt wanneer NLD zich kan verdedigen tegen langeafstands-raketten zoals ballistische raketten. Daarmee wordt het grondgebied, de bevolking en vitale infrastructuur beschermd tegen strategische aanvallen. Ook behoudt NLD zo controle over zijn veiligheid en onafhankelijkheid, zelfs onder dreiging van geweld op afstand. *[ref. VS NL]*	✓ Nieuwe technologische ontwikkelingen (hypersonische raketten en autonome wapensystemen) zorgen voor een toenemende 'nabijheid' van (militaire) dreiging. Daarmee is de veiligheid van het eigen grondgebied en de burgers een toenemende zorg. *[ref. VS NL; MIVD]*	✓ De oorlog in Oekraïne heeft het belang van een effectieve luchtverdediging nog eens benadrukt. Naast deze vorm van actieve verdediging is passieve verdediging ook noodzakelijk. Dat betreft onder meer hardening door het gebruik van materialen die bescherming bieden tegen de uitwerking van projectielen en explosieven. ✓ Omdat een volledige afweer tegen luchtaanvallen (zeker met het oog op de explosieve groei van bewapende drones) niet haalbaar is, is bescherming van platformen, systemen en gebouwen essentieel voor de (langdurige) inzet van defensie. Het gaat dan om o.a. lichtgewicht, slagvaste composietstructuren, speciale staalsoorten en thermisch geharde legeringen (o.a. voor voer-, vaar- en vliegtuigen) en explosie-absorberende bouwdelen voor militaire kampen of C2-centra.	✓ Ballistische bescherming richt zich met name op materialen. Deze sector is technologisch goed ontwikkeld, met een sterke focus op high-tech materialen, lichte composieten, keramiek, metaalbewerking, textielinnovatie en slimme coatings. De sector is kleinschalig maar kennisintensief. [zie ook par. 6.10] ✓ Defensie wil in 5 NLD gebieden uitblinken, waarvan slimme materialen er een van is. De toepassing van slimme materialen is breed, maar een belangrijke toepassing ligt in de bescherming van materieel en personeel. [zie ook par. 6.10] *[ref. DSII]* ✓ NLD ambieert om Nederlandse industriepartijen voor minimaal 3 OEM's ten minste de "second source supplier" te laten zijn voor het aanleveren van composiettoepassingen voor integratie in militaire platformen (1 x maritiem, 1 x land, 1 x lucht), van multifunctionele glasvezelversterkte composieten die aan de blast en ballistische eisen voldoen en lichter zijn dan stalen alternatieven. *[ref. DSII]*

Samenvattend: Kennis, technologie en (sub)systemen voor ballistische bescherming zijn van wezenlijk belang. Ze spelen een cruciale rol in het waarborgen van de soevereiniteit en de fysieke veiligheid van Nederland door bescherming te bieden tegen ballistische aanvallen en tegen gewapende drones. [zie ook 4.2 Existentiële dreigingen] Daarnaast draagt het bij aan de inzetgereedheid van militaire eenheden door hen te voorzien van de nodige bescherming om effectief te kunnen opereren en schade aan materieel te beperken waardoor langdurige inzet mogelijk is, hetzij door snelle reparatie danwel door graceful degradation. Ook kan de NLD industriesector op het gebied van (slimme) materialen bijdragen aan de defensiebehoefte en een sterke internationale positie voor Nederland. Daarbij geldt dat internationale samenwerking met vertrouwde partners en met mogelijke onderlinge afhankelijkheden in de keten goed denkbaar is. De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer en Specifier.				
6.3 Soldier Protection	NVT	NVT	✓ Bescherming van in het kader van de nationale veiligheid ingezette nationale eenheden is niet alleen politiek en moreel van het hoogste belang, maar is ook van invloed op langdurige inzet van de krijgsmacht (voortzettingsvermogen). ✓ Binnen de NAVO is vaak nationaal maatwerk nodig voor persoonlijke uitrusting ter bescherming van de militairen. Dit vereist in elk geval (minimaal) een SMART specifier rol.	✓ Er zijn Nederlandse bedrijven die zich richten op individuele soldatenuitrusting, o.a. composiet materialen voor persoonlijke bescherming (helmen, vesten, kleding). [zie ook par. 6.10]
Samenvattend: Bescherming van ingezette nationale eenheden is een wezenlijk belang. SMART specifier-/developer-schap voor het ontwerpen en bouwen van de geïntegreerde, vaak gelaagde, bescherming van eenheden is gewenst. [zie ook 4.7 Integratievermogen] Kennis van specifieke fysieke beschermingsmiddelen wordt veelal gedeeld met vertrouwde partners, vaak met dezelfde of vergelijkbare systemen en personele eisen en behoeften. [zie ook 4.3 Nederlandse karakteristieken] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer en Specifier.				
6.4 EOD & MCM	✓ De groeiende hybride dreiging waaronder sabotage en explosieven-/mijnendreiging gericht tegen (onderwater-) infrastructuur kan ook cascade effecten hebben	✓De genoemde dreiging is niet alleen gericht tegen objecten/infra maar kan ook nevenschade in termen van mensenlevens veroorzaken.	✓ EOD- en MCM-capaciteiten zorgen ervoor dat explosieven en mijnen (land- of zeemijnen) tijdig worden opgespoord en geneutraliseerd, wat directe bescherming biedt aan militair personeel.	✓ Het Nederlandse speelveld is klein maar gespecialiseerd, met een combinatie van innovatieve MKB-bedrijven, kennisinstellingen en grotere defensiegerichte spelers.

	op de digitale, economisch, ecologische en fysieke veiligheid van Nederland, en raakt daarmee ook aan de soevereiniteit van NLD. *[ref. DB MH]* ✓ Het hebben van adequate EOD- en MCM-capaciteit is van belang voor de soevereiniteit/integriteit van Nederland. Deze is met name in het kader van Host Nation Support kritisch, om daarmee een veilige doorvoer van NAVO-materieel en -personeel te garanderen.	✓ Daarnaast kan deze dreiging zich ook manifesteren in de publieke ruimte, en daardoor de veiligheid van Nederlandse burgers in gevaar brengen. *[ref. RRNV]*	✓ Een effectieve EOD/MCM-ondersteuning zorgt ervoor dat eenheden niet/minder vastlopen of vertraagd worden, waardoor de slagkracht en snelheid van optreden minder beperkt wordt. ✓ Lidstaten van NAVO en EU worden geacht bij te dragen aan collectieve veiligheid met specifieke capaciteiten, waaronder EOD en MCM. Zonder deze bijdragen wordt een land minder geloofwaardig als bondgenoot.	✓ De NLD maritieme industrie biedt NLD de SMART developer/integrator rol op MCM. ✓ Enkele bedrijven bieden geavanceerde drones, robotica en sensorsystemen die bruikbaar zijn voor EOD en MCM, en/of zijn gespecialiseerd in autonome systemen [zie ook par. 6.8], remote sensing en AI-toepassingen ten behoeve van EOD en MCM.
Samenvattend: EOD- (Explosieven Opruimingsdienst) en MCM- (Mine Counter Measures) capaciteiten zijn van wezenlijk belang. Ze leveren een bijdrage aan de bescherming van de nationale veiligheid, infrastructuur en de openbare orde (inclusief burgers), het vrijhouden van zeevaartroutes en toegang tot havens, en de strategische afschrikking en geloofwaardigheid. [zie ook 4.2 Existentiële dreigingen] In tijden van een crisis als gevolg van explosieven/mijnen-dreigingen/aanslagen is het toegang hebben tot eigen kritieke technologie en systemen voor EOD en MCM belangrijk. Het voorkomt vertraging of uitval bij toelevering, onderhoud of upgrades in geopolitiek gespannen tijden. [zie ook 4.11 Toegang tot capaciteiten] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer en Integrator, en in sommige gevallen Specifier.				
6.5 Counter Terrorism & Security	Zie 6.1, 6.2, 6.4	Zie 6.1, 6.2, 6.4	Zie 6.1, 6.2, 6.4	Zie 6.1, 6.2, 6.4

Samenvattend: Bescherming van de nationale veiligheid is een wezenlijk belang. Het gaat hier om het beschermen en beveiligen van personen, materieel, informatie en infrastructuur tegen dreigingen zoals terrorisme, sabotage, spionage en ondermijning. [zie ook 4.2 Existentiële dreigingen] Het betreft dan inzet van middelen tegen o.a. CBRN, explosieven en (zee-)mijnen. Aanvullend ook nog middelen tegen afluisteren en cyberdreigingen. Al deze middelen (kennis, technologie en systemen) worden al afgedekt in andere Defensie-deelgebieden.				
6.6 (Counter) Hybrid	✓ Hybride dreigingen zijn complex en pluriform en zijn erop gericht om een staat te destabiliseren en daarmee ook de soevereiniteit van een land aan te tasten. Veelal zijn deze dreigingen ook gericht op specifieke doelen in een staat. Daarbij kan in beginsel geen beroep gedaan worden op collectieve verdediging, en is een land zelf verantwoordelijk om deze dreigingen te pareren. *[ref. DB MH]*	✓ Vanwege het pluriforme karakter zijn hybride dreigingen gericht op de economische, digitale, ecologische en sociale veiligheid van een land. Schade in deze gebieden raakt vaak ook de veiligheid en welzijn van burgers. *[ref. DB MH]*	✓ Ook de inzet van Nederlandse eenheden, zowel in missiegebieden als in eigen land, kan bedreigd worden door de inzet van hybride dreigingen door een (niet-)statelijke actor. Daarmee is ook de inzetgereedheid van de krijgsmacht een doelwit. ✓ De Nederlandse krijgsmacht heeft op specifieke onderdelen middelen om zichzelf en deels ook Nederland (in samenwerking met andere publiek-private organisaties) te verdedigen tegen hybride dreigingen. Denk aan Cyber middelen, EOD capaciteiten, CBRN detectie en bescherming capaciteiten, Intell capaciteiten. [zie ook par. 6.1, 6.5] *[ref. DN2024]*	✓ Tegenstanders gebruiken vaak civiele technologieën bij hybride dreigingen, zoals bij het genereren van desinformatie of cyberaanvallen. Daarom moet Defensie ook op minder militair-specifieke technologie kennis opbouwen. Daar kunnen civiele kennisinstituten in toenemende mate een rol spelen voor Defensie. *[ref. DSII]* ✓ Met name het verdedigen tegen hybride dreigingen vereist een whole-of-society aanpak waarbij publiek-private samenwerking essentieel is. Bedrijven kunnen informatie, kennis en middelen leveren op tal van gebieden. ✓ Gezien de eigen verantwoordelijkheid van Nederland om zich tegen hybride dreigingen te verdedigen, is daarom een eigen ontwikkelcapaciteit noodzakelijk. Dat geldt ook voor Defensie, dat daarbij verschillende rollen kan spelen: SMART developer (cyber), SMART developer (Intell), SMART

				specifier (CBRN), SMART integrator (EOD/MCM).
Samenvattend: Kennis, technologie en systemen ter verdediging tegen hybride dreigingen zijn van wezenlijk belang. Gezien de eigen verantwoordelijkheid van Nederland om zich tegen hybride dreigingen te verdedigen, is daarom een eigen ontwikkelcapaciteit noodzakelijk. [zie ook 4.2 Existentiele dreigingen] Defensie kan op bepaalde terreinen een bijdrage hieraan leveren. Verder is Defensie zelf verantwoordelijk voor de verdediging van eigen eenheden tegen hybride dreigingen, zowel bij inzet in eigen land als in missiegebieden. Aangezien hybride dreigingen veelal gericht zijn tegen kwetsbaarheden van een staat/organisatie is een tailor-made aanpak bij de verdediging ertegen het meest effectief. [zie ook 4.3 Nederlandse karakteristieken] Daarmee kan Defensie op bepaalde gebieden het beste een actieve rol hebben bij het ontwikkelen van middelen. Defensie kan verschillende SMART-rollen vervullen, variërend van Developer tot Specifier.				

6.7 Menselijk Presteren & Medicijnen

Overall analyse: Het Basisgebied Menselijk Presteren & Medicijnen is van wezenlijk belang voor de gereedstelling, inzetbaarheid en bescherming van Nederlandse militairen. De vier onderliggende subgebieden vormen samen het fundament onder elke militaire operatie. Zonder zeggenschap over training, gezondheid en prestatievermogen verliest Defensie operationele autonomie en neemt de afhankelijkheid van buitenlandse normen en voorzieningen toe. De bijdrage aan de veiligheid van onderdanen is vooral indirect, via beperking van fouten en inzet van medische capaciteit in civiele noodsituaties. In termen van inzetzekerheid is dit basisgebied cruciaal: fysieke en mentale paraatheid, opleidingskwaliteit, cognitieve weerbaarheid en zorgcontinuïteit bepalen direct de gereedheid en het volhoudingsvermogen van krijgsmachteenheden. Nederland beschikt over sterke kennisinstellingen, een eigen medisch systeem (DGO), en een ontwikkelpositie in simulatie en training. De meest voor de hand liggende SMART-rollen zijn daarom overwegend Developer, Specifier en Maintainer, met ruimte voor verdere versterking in met name het cognitieve domein.

Onderstaand volgt de systematische analyse van elk subgebied, gebaseerd op een analyse van de drie wezenlijke belangen en de industriële capaciteiten voor dat subgebied.

Subgebied	Nederlandse soevereiniteit	Veiligheid van onderdanen	Inzetzekerheid in defensiedomeinen	Industriële Capaciteiten
7.1 Human Performance & Resilience	✓ Selectie, inzet en ondersteuning van personeel valt onder nationale wetgeving en verantwoordelijkheid. Zonder nationale zeggenschap over human performance-capaciteiten verliest Nederland operationele regie. *[ref. DIS; DN2024]*	✓ Bevordering van fysieke en mentale weerbaarheid van militairen verhoogt inzetveiligheid, maar heeft slechts indirecte impact op civiele bescherming. ✓ Het bevorderen van mentale weerbaarheid tegen ongewenste buitenlandse beïnvloeding kan wel van directe invloed zijn op de veiliggheid van onderdanen. *[ref. DIS; HCSS WB; DV2035]*	✓ Essentieel voor duurzame inzetbaarheid van personeel in het algemeen, maar ook zeker onder hoge belasting, o.a. in langdurige of extreme missies. Een relatief kleine krijgsmacht maakt individueel prestatieniveau van militairen extra cruciaal. *[ref. DIS; DV2035, HCSS WB]*	✓ Nederland beschikt over kennisinstellingen voor onderzoek en een medisch militair ecosysteem. Door constante veranderingen in dreigingen en operaties is continue innovatie nodig rondom mentale en fysieke weerbaarheid. *[ref. DIS, HCSS WB]*
Samenvattend: Fysieke en mentale weerbaarheid zijn van wezenlijk belang voor duurzame inzetbaarheid van personeel in zware omstandigheden. Zonder nationale regie verliest Defensie controle over selectie, training en inzetnormen. Defensie heeft ontwikkelambities in de domeinen van human enhancement, mentale weerbaarheid en arbeidsextensieve capaciteiten, veelal ook op maat gesneden voor de Nederlandse defensieorganisatie. [zie ook 4.3 Nederlandse karakteristieken] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer en Specifier.				
7.2 Training, Education & Simulation	✓ Zeggenschap over militaire training en educatie is belangrijk om eigen inzetcriteria, strategische cultuur en ethiek te borgen. [zie ook par. 10.9] *[ref. DIS; HCSS WB]*	Bijdrage van training, opleiding en simulatie aan de veiligheid van onderdanen is indirect. Goede training beperkt wel risico op fouten met nevenschade tot gevolg. *[ref. DN2024; HCSS WB]*	✓ Direct bepalend voor inzetvaardigheid en interoperabiliteit. Training is essentieel voor operationele gereedheid. ✓ Simulatie verhoogt operationele effectiviteit zonder fysieke risico's. [zie ook par. 6.10] *[ref. DIS; DN2024; DV2035; HCSS WB]*	Diverse Nederlandse bedrijven en instellingen ontwikkelen simulatie- en opleidingssystemen. Trainingsmethodieken moeten voortdurend vernieuwen om relevant te blijven bij veranderende dreigingen. *[ref. DIS, HCSS WB]*

Samenvattend: Opleiding en simulatie is van wezenlijk belang voor operationele gereedheid en interoperabiliteit. Nationale zeggenschap is benodigd om doctrines en opleidingsnormen in lijn te houden met eigen inzetprincipes. [zie ook 4.3 Nederlandse karakteristieken] Nederland beschikt over een goede kennisbasis. De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer en Specifier.				
7.3 Effects in the Cognitive Domain	✓ Informatieoperaties, beïnvloedingscampagnes en cognitieve paraatheid raken direct aan nationale besluitvormings-autonomie en weerbaarheid tegen beïnvloeding. *[ref. DB MH; HCSS WB]*	✓ Effectieve cognitieve capaciteiten kunnen de bevolking weerbaar maken tegen ongewenste buitenlandse inmenging en zo bijdragen aan het voorkomen van escalatie en/of maatschappelijke destabilisatie. Nederland is kwetsbaar voor buitenlandse beïnvloeding door zijn open, democratische structuur en het intensieve gebruik van digitale media. *[ref. DN2024; HCSS WB]*	✓ Steeds belangrijker in hybride conflicten. Relevantie stijgt voor missievoorbereiding, situational awareness en force protection. *[ref. DIS; DV2035]*	✓ Nederland bouwt capaciteit op in samenwerking met NAVO-partners, onderzoeksinstituten en universiteiten, maar heeft nu beperkte controle over tooling of inzetmiddelen. Dit is van wezenlijk belang omdat capaciteiten in het cognitieve domein strategische communicatie, beïnvloeding, en bescherming tegen hybride dreigingen verbeteren. [zie ook par. 6.6] Aangezien technologie in dit veld snel evolueert (bijv. AI) is voortdurende innovatie noodzakelijk. *[ref. DIS, HCSS WB]*
Samenvattend: Informatiebewerking en cognitieve weerbaarheid zijn van wezenlijk belang vanwege het beschermen van de nationale bevolking en de defensieorganisatie tegen (hybride) oorlogvoering. Ze beïnvloeden besluitvorming, situational awareness en maatschappelijke stabiliteit. [zie ook 4.2 Existentiële dreigingen] Daarbij spelen ook ethische en juridische aspecten een belangrijke rol die veelal nationaal bepaald zijn. [zie ook 4.3 Nederlandse karakteristieken; 4.13 Maatwerk voor kleine landen] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer en Specifier.				
7.4 Military Health	✓ De medische ondersteuning van de krijgsmacht moet binnen Nederlandse wet- en regelgeving worden georganiseerd; medische zorg voor uitgezonden eenheden vereist soeverein inrichtingsvermogen. *[ref. DIS]*	✓ Het effect op onderdanen is grotendeels indirect, maar militaire gezondheidszorg kan ook worden ingezet bij rampen en crises om de civiele gezondheidszorg te ondersteunen. *[ref. DN2024; HCSS WB]*	✓ Onmisbaar voor continuïteit van inzet in conflictgebieden. Medische evacuatie, preventie en behandeling bepalen inzetduur. *[ref. DIS; DV2035]* ✓ Tijdens veel NAVO-uitzendingen wordt momenteel de zorg (met name personeel maar ook faciliteiten) vanuit verschillende landen ingericht. Uitzondering is	✓ Nederland heeft een militair geneeskundig systeem met eigen capaciteit (Defensie Gezondheidszorg Organisatie), inclusief ruimte voor innovatie. Medische zorg vereist robuuste logistiek en leveringszekerheid van medische middelen (medicatie, materiaal). *[ref. DIS, HCSS WB]*

			de zorg aan boord van maritieme platforms. Indien Nederland bijvoorbeeld in het kader van bescherming van Caribisch Nederland militaire zorg moet leveren, kan niet worden teruggevallen op andere landen.	
Samenvattend: Een soevereine medische keten is van wezenlijk belang voor inzetzekerheid en bescherming van personeel in missies. Civiele inzet bij rampen versterkt de brede maatschappelijke waarde. De medische ondersteuning van de krijgsmacht moet binnen Nederlandse wet- en regelgeving worden georganiseerd. [zie ook 4.13 Maatwerk voor kleine landen] Defensie streeft naar instandhouding en versterking van zijn eigen militaire medische systeem. De meest voor de hand liggende SMART-rollen voor Defensie zijn: Maintainer en Developer.				

6.8 Autonome & Onbemande Systemen

Overall analyse: Kennis en technologie op het gebied van Autonome & Onbemande Systemen is van wezenlijk belang voor de Nederlandse krijgsmacht. De onderliggende subgebieden zijn belangrijk om het toekomstige gevecht te kunnen winnen, op zee, te land en in de lucht. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Op veel subgebieden zijn er momenteel echter afhankelijkheden van buitenlandse leveranciers. Gezien de geopolitieke ontwikkelingen is streven naar meer autonomie in dit basisgebied te overwegen. Defensie heeft daarom ook Intelligente systemen (waaronder onbemenste systemen) als één van de vijf NLD gebieden gekozen, waar extra in wordt geïnvesteerd. De meest voor de hand liggende SMART-rollen voor Defensie zijn overwegend Developer en Specifier, en soms Maintainer.

Onderstaand volgt de systematische analyse van elk subgebied, gebaseerd op een analyse van de drie wezenlijke belangen en de industriële capaciteiten voor dat subgebied.

Subgebied	Nederlandse soevereiniteit	Veiligheid van onderdanen	Inzetzekerheid in defensiedomeinen	Industriële Capaciteiten
8.1 Unmanned Systems	✓ Zelfstandig gebruik en ontwikkeling van onbemenste systemen voorkomt afhankelijkheid van derden bij militaire operaties en surveillance. *[ref. DIS; STRAIIK; DV2035]*	✓ Onbemenste systemen kunnen risicovolle taken overnemen van personeel, wat de bescherming van defensiepersoneel (burgers en militairen) vergroot. *[ref. DIS; DV2035]* ✓ Ook kunnen deze nationaal ingezet worden in crisis- en rampensituaties en daarmee ook zorgen voor veiligheid van burgers.	✓ Onmisbaar voor ISR, force protection, en logistieke ketens in moderne operaties. ✓ Onbemenste systemen worden breed ingezet in het land-, lucht-, zee-, en ruimtedomein. ✓ Noodzakelijk om meer gevechtskracht te leveren. ✓ Ze zorgen voor massa en snelheid van het Defensieoptreden. *[ref. DIS; DV2035]*	✓ Nederland ontwikkelt zelf kleinere unmanned aircraft systems (UAS) en investeert in een productie-ecosysteem. Verschillende Nederlandse bedrijven ontwikkelen subsystemen; grootschalige platformontwikkeling is nog wel grotendeels afhankelijk van internationale leveranciers. [zie ook par. 6.4] *[ref. DIS; STRAIIK]* ✓ Intelligente systemen (waaronder onbemenste systemen) is één van de vijf NLD gebieden. *[ref. DSII]*
Samenvattend: Kennis en technologie op het gebied van Unmanned Systems zijn van wezenlijk belang; deze systemen zijn belangrijk voor diverse soorten defensieoperaties in het land-, lucht-, zee-, en ruimtedomein. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Hoewel de Nederlandse industriële basis op dit technologiegebied relatief snel groeit, is Defensie voor grootschalige platformontwikkeling vooralsnog echter nog grotendeels afhankelijk van internationale leveranciers; gezien de geopolitieke ontwikkelingen is streven naar nog meer autonomie te overwegen. [zie ook 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer, Maintainer en Specifier.				
8.2 Autonomy	✓ Autonomie bepaalt de mate van inzetvrijheid en politieke zeggenschap: wie heeft grip op de algoritmes op basis waarvan inzetbesluiten worden genomen, hoe vindt ethische controle plaats. ✓ Zonder nationale capaciteit ontstaan	NVT	✓ Belangrijk voor real-time besluitvorming bij multidomein optreden en bij swarming-concepten. Zonder autonomie zijn reactietijden te traag. *[ref. DIS; DV2035]* ✓ Menselijke controle is nodig om te bewaken dat systemen binnen ethische en juridische grenzen functioneren. Autonome	✓ Nederland beschikt wel over fundamentele kennis bij onderzoeksinstituten, maar mist capaciteiten voor grootschalige (combat-grade) implementatie. De afhankelijkheid van buitenlandse partijen is groot. *[ref. DIS; STRAIIK]* ✓ Intelligente systemen (waaronder onbemenste systemen) is één van de vijf NLD gebieden. *[ref. DSII]*

	afhankelijkheden in gedrag, updatebeheer en ethische kaders. *[ref. DIS; HCSS WB]*		systemen waar geen adequate menselijke controle wordt uitgeoefend en/of systemen die beslissingen nemen op basis van foutieve input kunnen burgerslachtoffers veroorzaken. [zie ook par. 6.10] *[ref. DIS; DV2035]*	
Samenvattend: Kennis en technologie op het gebied van Autonomy zijn van wezenlijk belang voor defensieoptreden in alle domeinen. Autonomy is belangrijk voor real-time besluitvorming bij multidomein optreden en bij swarming-concepten. Menselijke controle is nodig om te bewaken dat systemen binnen ethische en juridische grenzen functioneren; Nederland blijft immers verantwoordelijk voor het gebruik van geweld van haar eigen autonome systemen. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Voor grootschalige (combat-grade) implementatie is Defensie nu echter nog grotendeels afhankelijk van internationale leveranciers; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. [zie ook 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Specifier en Developer.				
8.3 Human-Machine Teaming	✓ Grip op human-machine-teaming-concepten bepaalt hoe systemen in coalitieverband opereren. ✓ Nationale zeggenschap vereist interoperabele, ethisch verantwoorde teaming-architecturen. *[ref. DIS; HCSS WB]*	NVT	✓ Onmisbaar in C2 en ISR (operationeel en tactisch) en bij de inzet van robotica en swarm control. Mens-systeem integratie is belangrijk voor inzetzekerheid. ✓ Goede human-machine teaming vermindert cognitieve belasting en fouten van defensiepersoneel en voorkomt daarmee mogelijk ook burgerslachtoffers. *[ref. DIS; DV2035]*	✓ Nederland ontwikkelt al wel simulatie- en teamingconcepten, maar er is nog geen end-to-end systeembouw, daarvoor is er nog afhankelijkheid van buitenlandse partijen. Nichekennis wat betreft integratie is wel groeiende. *[ref. DIS; STRAIIK]*

Samenvattend: Kennis en technologie op het gebied van Human-Machine Teaming zijn van wezenlijk belang voor defensieoptreden; mens-systeem integratie is belangrijk voor de inzetzekerheid bij diverse soorten defensieoperaties. [zie ook 4.7 Integratievermogen] Gezien de snelheid van het gevecht van de toekomst is dit de manier om effectief invulling te geven aan C2 op de verschillende niveau's van militair optreden. Goede human-machine teaming vermindert bovendien cognitieve belasting en fouten van defensiepersoneel en voorkomt daarmee mogelijk ook burgerslachtoffers. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Hoewel de Nederlandse industriële basis op dit gebied groeit, is Defensie vooral op het vlak van end-to-end systeembouw echter nog grotendeels afhankelijk van internationale partijen; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. Nationale zeggenschap vereist interoperabele, ethisch verantwoorde teaming-architecturen. [zie ook 4.3 Nederlandse karakteristieken; 4.13 Maatwerk voor kleine landen]
De meest voor de hand liggende SMART-rollen voor Defensie zijn: Specifier en Developer.

6.9 Logistiek

Overkoepelende analyse: Het defensie-basisgebied Logistiek is van wezenlijk belang, met name voor de (langdurige) inzetgereedheid van de krijgsmacht, zowel voor taken in eigen land als voor operaties in EU-/NAVO-verband. Materiële gereedheid en de logistieke ondersteuning van de eigen ingezette eenheden is een nationale verantwoordelijkheid. Samenwerking met (inter)nationale leveranciers en onderhoudsbedrijven is belangrijk, met name vanwege schaalgrootte en expertise. Een bepaalde mate van nationale controle over de logistieke middelen (voorraden, transport, onderhoud) is meer dan wenselijk, omdat daarmee de inzetgereedheid voldoende kan worden gewaarborgd. Dit kan onder meer door strategische publiek-private samenwerkingen aan te gaan, in eigen land of in de regio. De meest voor de hand liggende SMART-rollen voor Defensie variëren van User en Maintainer tot Buyer, Specifier en Integrator.

Onderstaand volgt de systematische analyse van elk subgebied, gebaseerd op een analyse van de drie wezenlijke belangen en de industriële capaciteiten voor dat subgebied.

Subgebied	Nederlandse soevereiniteit	Veiligheid van onderdanen	Inzetzekerheid in defensiedomeinen	Industriële Capaciteiten
9.1 Smart and predictive maintenance	✓ Beheer over eigen onderhoudscapaciteit voorkomt operationele blokkades door externe leveranciers. Noodzakelijk voor strategische autonomie. *[ref. DIS; HCSS WB]*	NVT	✓ Nationale zeggenschap over onderhoud en instandhouding voorkomt belemmeringen in ondersteuning van ingezette eenheden, inclusief technologische back-up. *[ref. DIS; HCSS WB]* ✓ Onderhoud en instandhouding van platforms en munitie is essentieel voor langdurige inzet in meerdere domeinen. *[ref. HCSS WB; DIS]* ✓ Productie van materieel op locaties dichtbij conflictgebieden is niet vanzelfsprekend. Dat betekent dat bepaalde capaciteiten in NLD moeten worden behouden of ontwikkeld om de (cruciale) wapensystemen van de krijgsmacht – en haar bondgenoten - te kunnen produceren, op te kunnen schalen en te ondersteunen. Dat kan betekenen dat voor specifieke wapensystemen in nationale capaciteiten (zoals productie, logistiek) moet worden geïnvesteerd om risicovolle strategische afhankelijkheden af te bouwen. *[ref. DSII]*	✓ Nederland beschikt over publieke en private logistieke netwerken, waarbij ook een rol voor defensie-industrie in onderhoud (bijvoorbeeld bij voertuigen en marineschepen) is voorzien. *[ref. DIS; STRAIIK]* ✓ Maintenance Valley is een cluster van bedrijven, kennisinstellingen en overheden die samenwerken op het gebied van onderhoud, met name voor hightech systemen in de luchtvaart en defensie. Dit initiatief, waarbij Vliegbasis Woensdrecht een centrale rol speelt, zorgt voor het versterken van de militaire paraatheid van Nederland en haar bondgenoten, het stimuleren van de regionale economie, en het bevorderen van innovatie in de defensie- en logistieke sector.

Samenvattend: Kennis, technologie en tools op het gebied van Smart and Predictive Maintenance zijn van wezenlijk belang. Een deel van de kennis, technologie en tools is civiel/internationaal verkrijgbaar. Het onderhoud kan weliswaar vaak uitbesteed worden aan de leveranciers, maar dit kan risico's opleveren en beperkt de eigen strategische autonomie als het gaat om leveringszekerheid van onderdelen en kan daarmee de beschikbaarheid en inzet van eenheden beperken. [zie ook 4.8 Beheersing toeleveringsketen] Strategische publiek-private samenwerking, bijvoorbeeld in de (eigen) regio) kan ervoor zorgen dat Defensie meer zeggenschap hierover behoudt en daarmee tevens bijdraagt aan economische en innovatie doelen. De meest voor de hand liggende SMART-rol voor Defensie is: Maintainer.				
9.2 Supply chain management	✓ Beheer over eigen bevoorradingscapaciteit voorkomt operationele blokkades door externe leveranciers. Noodzakelijk voor strategische autonomie. *[ref. DIS; HCSS WB]*	NVT	✓ Nationale zeggenschap over bevoorrading en instandhouding voorkomt belemmeringen in ondersteuning van ingezette eenheden, inclusief technologische back-up. *[ref. DIS; HCSS WB]*	✓ Bevoorrading en onderhoud wordt grotendeels door Defensie zelf uitgevoerd, met een relatief beperkte rol voor private partners. Denk hierbij aan werk van BEVO, Genie, en Geneeskundige Dienst. ✓ Reserveonderdelen worden veelal geleverd door (inter)nationale industrie.
Samenvattend: Zonder eigen materieellogistieke capaciteit zoals bevoorrading is voortzettingsvermogen afhankelijk van derden. Dit raakt aan inzetzekerheid en soevereiniteit. Voor materieellogistieke diensten moet de betrouwbaarheid, beschikbaarheid en eventueel snelheid van dienstverlening, en daarmee het vertrouwen in de dienstverlener, gegarandeerd zijn. Dit pleit voor nationale dienstverleners of poolvorming met vertrouwde partners. [zie ook 4.8 Beheersing toeleveringsketen] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Buyer, Maintainer en Integrator.				
9.3 Transport	✓ Het hebben van eigen transportcapaciteit (weg, lucht, spoor, zee) voorkomt afhankelijkheid van externe aanbieders voor het strategisch verplaatsen van eenheden en materieel. *[ref. DIS; HCSS WB]* ✓Nederland heeft in het kader van de NATO Host Nation Support taak de	✓ Belangrijk bij ondersteuning van civiele autoriteiten bij rampen, evacuaties en noodhulp. Transportmiddelen vormen ook schakel in civiele-militaire samenwerking. *[ref. DN2024]*	✓ Transport is essentieel voor verplaatsing en bevoorrading van eenheden, vooral (maar niet alleen) in grootschalige of langdurige operaties. *[ref. DN2024, DIS]*	✓ Nederland heeft eigen capaciteit via DOSCO en Defensie Vervoersorganisatie, aangevuld met civiele inhuur. Strategische en tactische transportmiddelen zijn deels nationaal beschikbaar. *[ref. DIS; STRAIIK]*

	verplichting om logistieke steun te verlenen bij de doorvoer van troepen en materieel door Nederland.			
Samenvattend: Transport is van wezenlijke belang, het vormt immers de fysieke backbone van alle operaties. Nationale controle waarborgt strategische vrijheid en reactietijd in crisissituaties, zowel in eigen land (ook in het kader van NATO Host Nation Support) als in missiegebieden. Hiervoor hoeft geen eigen ontwikkeling plaats te vinden, maar is het op tijd verkrijgen van deels civiele transportmiddelen en deels militaire transportmiddelen als SMART Buyer mogelijk. [zie ook 4.11 Toegang tot capaciteiten] Vanwege tijdige beschikbaarheid en inzetgereedheidseisen is een SMART Maintainer-rol, al dan niet in samenwerking met (nationale) industrie, ook voor de hand liggend.				
9.4 Life Cycle Support Analysis	NVT	NVT	✓ Het betreft kennis, methoden en tools (software) die de planning (inclusief levensduurkosten) van de gehele levensduur van een systeem/platform ondersteunen. Veel daarvan is internationaal verkrijgbaar, met name vanuit NAVO(-landen). Wel is kennis nodig om deze te tailoren naar de NLD specifieke situatie (schaalgrootte, organisatie-inrichting, risico-acceptatie, bedrijfsvoering etc.) ✓ Een goede ondersteuning van de levensduur(kosten) van een platform zorgt voor een optimale inzetgereedheid van personeel en materieel.	✓ Kennis en tooling is aanwezig bij nationale leveranciers van defensiematerieel en bij kennisinstellingen.
Samenvattend: Kennis en tools voor Life Cycle Support Analysis is van wezenlijk belang omdat het zorgdraagt voor een zo optimaal mogelijke inzet van schaarse middelen (personeel, materieel, infrastructuur) en daarmee bijdraagt aan de inzetgereedheid en het voortzettingsvermogen van de Nederlandse krijgsmacht. De meest voor de hand liggende SMART-rollen voor Defensie zijn: Specifier, Buyer en User.				

6.10 Defensie-toepasbare sleuteltechnologieën en -methodologieën

Overall analyse: Het basisgebied Defensie-toepasbare sleuteltechnologieën en -methodologieën is een divers en breed basisgebied, en is van wezenlijk belang voor defensieoptreden in alle domeinen. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand. Nederland heeft op diverse subgebieden een eigen kennispositie, bij kennisinstellingen en ook binnen de Defensieorganisatie zelf. Alleen wat betreft de subgebieden Quantum Technologies en Semiconductor Technologies is Nederland momenteel nog afhankelijk van internationale partijen; daar valt te overwegen om meer autonomie na te streven. De meest voor de hand liggende SMART-rollen voor Defensie zijn overwegend Developer en Specifier, en soms User of Integrator.

Onderstaand volgt de systematische analyse van elk subgebied, gebaseerd op een analyse van de drie wezenlijke belangen en de industriële capaciteiten voor dat subgebied.

Subgebied	Nederlandse soevereiniteit	Veiligheid van onderdanen	Inzetzekerheid in defensiedomeinen	Industriële Capaciteiten
10.1 AI, Data Science & Machine Learning	✓ Autonomie over algoritmes en inzetlogica is cruciaal voor strategische besluitvorming en inzetvrijheid. *[ref. DSII]*	✓ AI ondersteunt bij identificatie van dreigingen, versnelt reactietijd en voorkomt menselijke fouten. *[ref. DSII]*	✓ AI speelt een sleutelrol bij informatiegestuurd optreden, surveillance, logistiek en cyberactiviteiten in alle defensiedomeinen. *[ref. DSII]*	✓ Nederland heeft een sterke industrieel-technologische kennispositie via zowel kennis-instellingen als bedrijven. *[ref. DSII]* ✓ Intelligente systemen (waaronder AI & Data Science) is één van de vijf NLD prioritaire gebieden. *[ref. DSII]*
Samenvattend: Kennis en technologie op het gebied van AI, Data Science & Machine Learning zijn van wezenlijk belang voor defensieoptreden in alle domeinen. AI speelt een sleutelrol bij informatiegestuurd optreden, surveillance, logistiek en cyberactiviteiten in alle defensiedomeinen. Autonomie over algoritmes en inzetlogica is cruciaal voor strategische besluitvorming en inzetvrijheid. [zie ook 4.9 Informatie(systemen) als middel] Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand, zeker omdat Nederland beschikt over een goede industrieel-technologische kennisbasis op dit vlak. Defensie heeft dan ook Intelligente systemen (waaronder AI&Data Science) aangewezen als één van de 5 NLD prioritaire gebieden waar extra in wordt geïnvesteerd. De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer en Specifier.				

10.2 Advanced Materials & Additive Manufacturing	✓ Beschikbaarheid van nationale producenten voorkomt strategische afhankelijkheden van buitenlandse leveranciers. *[ref. DSII]*	NVT	✓ Essentieel voor onderhoud en productie van onderdelen en munitie; verbetert de beschikbaarheid van wapensystemen. *[ref. DSII]*	✓ Nederland beschikt over hoogwaardige materiaaltechnologie bij zowel kennisinstituten als bedrijfsleven. *[ref. DSII]* ✓ Slimme materialen is één van de 5 NLD prioritaire gebieden. *[ref. DSII]*
Samenvattend: Kennis en technologie op het gebied van Advanced Materials & Additive Manufacturing zijn van wezenlijk belang voor defensieoptreden in alle domeinen; het is essentieel voor onderhoud en productie van onderdelen en munitie en verbetert de beschikbaarheid van wapensystemen. [zie ook 4.8 Beheersing toeleveringsketen] Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt dan ook voor de hand, zeker omdat Nederland beschikt over een goede industrieel-technologische kennisbasis op dit vlak. Defensie heeft Slimme Materialen aangewezen als één van de 5 NLD gebieden waar extra in wordt geïnvesteerd, met het oogmerk om daarin ook als SMART Developer op te treden. Naast de SMART-developer rol kan Defensie ook nog de SMART Maintainer rol vervullen.				
10.3 Modelling & Simulation	✓ Soevereine ondersteuning bij inzetvoorbereiding, capaciteitsplanning en doctrineontwikkeling voorkomt mogelijke ongewenste beïnvloeding door buitenlandse actoren *[ref. DSII]*	✓ Verbetert de veiligheid tijdens opleiding, training en testfases zonder fysieke risico's voor militairen en/of burgers. *[ref. DSII]*	✓ Biedt ondersteuning bij inzetvoorbereiding, capaciteitsplanning en doctrineontwikkeling. *[ref. DSII]*	✓ Nederland beschikt over kennis en technologie bij zowel kennisinstituten als bedrijfsleven. [*ref. DSII]*
Samenvattend: Kennis en technologie op het gebied van Modelling & Simulation zijn van wezenlijk belang voor defensieoptreden in alle domeinen als ondersteuning bij inzetvoorbereiding, capaciteitsplanning en doctrineontwikkeling. [zie ook 4.3 Nederlandse karakteristieken] Soevereine beschikking over deze technologie voorkomt mogelijke ongewenste beïnvloeding door buitenlandse actoren. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt dan ook voor de hand, zeker omdat Nederland beschikt over een goede industrieel-technologische basis op dit vlak. De meest voor de hand liggende SMART-rollen voor Defensie zijn: User en Specifier.				

10.4 Quantum Technologies	✓ Strategische controle is belangrijk met het oog op potentieel disruptieve capaciteiten in communicatie en sensing. *[ref. DSII]*	✓ Toepasbaar op veilige communicatie en op detectie van dreigingen in het algemeen. *[ref. DSII]*	✓ Belangrijk voor precisienavigatie, detectie, cyberverdediging (crypto) en snelheid van besluitvorming in toekomstscenario's. *[ref. DSII]*	✓ Nederland beschikt momenteel wel over een initiële onderzoekspositie, maar niet over militaire implementatiecapaciteit. *[ref. DSII]* ✓ Quantum is één van de 5 NLD prioritaire gebieden. *[ref. DSII]*
Samenvattend: Kennis en technologie op het gebied van Quantum Technologies zijn van wezenlijk belang voor defensieoptreden in alle domeinen: dit is met name belangrijk voor precisienavigatie, detectie en cyberverdediging in toekomstscenario's. Quantum technologies biedt potentieel disruptieve capaciteiten in communicatie en sensing, zowel een kans als een bedreiging. [zie ook 4.4 Operationeel voordeel] Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt dan ook voor de hand. Vooral wat betreft militaire implementatiecapaciteit is Nederland nu echter nog afhankelijk van internationale partijen; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. Defensie heeft Quantum aangewezen als één van de 5 NLD prioritaire gebieden waar extra in wordt geïnvesteerd. De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer en Specifier.				
10.5 Semiconductor Technologies	✓ Belangrijk voor soevereine controle over digitale systemen. *[ref. DSII]*	✓ Indirect kunnen civiele technologieën ook door tegenstanders worden gebruikt als wapen bij hybride dreigingen, zoals bij het genereren van desinformatie of cyberaanvallen die de burgerbevolking kunnen treffen. *[ref. DSII]*	✓ Onmisbaar in vrijwel alle wapensystemen, sensorsystemen, communicatie en IT. ✓ In eerste instantie civiele technologieën kunnen bij hybride dreigingen ook door tegenstanders worden gebruikt als wapen, zoals bij het genereren van desinformatie of cyberaanvallen, en spelen een cruciale rol in de wereldwijde wedloop. Daarom is het verstandig als Defensie ook op minder militair-specifieke technologie kennis opbouwt. *[ref. DSII]*	✓ Nederland heeft een unieke positie in specifieke niches, maar is daarnaast voor een groot deel afhankelijk van buitenlandse leveranciers; defensietoepassingen betreft vooral subsystemen. *[ref. DSII]*

Samenvattend: Kennis en technologie op het gebied van Semiconductor Technologies zijn van wezenlijk belang: dit basisgebied is onmisbaar in vrijwel alle wapensystemen, sensorsystemen, communicatie en IT. Het technologiegebied is belangrijk voor soevereine controle over digitale systemen. Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt dan ook voor de hand. Op dit moment is Nederland echter nog deels afhankelijk van buitenlandse partijen; gezien de geopolitieke ontwikkelingen is streven naar meer autonomie te overwegen. [zie ook 4.8 Beheersing toeleveringsketen; 4.12 Strategische autonomie en continuïteit] De meest voor de hand liggende SMART-rollen voor Defensie zijn: Developer en Specifier.				
10.6 Operational Analysis	✓ Autonomie bij het onderbouwen van beleidskeuzes, inzet, logistiek en capaciteitsplanning. *[ref. DSII]*	NVT	✓ Onderbouwt beleidskeuzes, inzet, logistiek en capaciteitsplanning. *[ref. DSII]*	✓ Nederland heeft hiervoor een eigen kennispositie, zowel bij kennisinstellingen als binnen de defensieorganisatie zelf. *[ref. DSII]*
Samenvattend: Kennis en technologie op het gebied van Operational Analysis zijn van wezenlijk belang bij het onderbouwen van beleidskeuzes, inzet, logistiek en capaciteitsplanning, die veelal maatwerk vereisen. [zie 4.13 Maatwerk voor kleine landen] Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand, zeker omdat Nederland beschikt over een goede kennisbasis op dit vlak. [zie 4.5 Brede kennisbasis] De meest voor de hand liggende SMART-rollen voor Defensie zijn: User en Specifier.				
10.7 Strategic Foresight & Analysis	✓ Autonomie bij het anticiperen op dreigingen, disruptie en innovatiebehoeften. ✓ Vormt de basis voor beleidsontwikkeling, waarbij vaak maatwerk aan de orde is. *[ref. DSII]*	✓ Versterkt anticipatie op dreigingen, disruptie en innovatiebehoeften die ook voor de burgerbevolking van belang kunnen zijn. *[ref. DSII]*	✓ Versterkt anticipatie op dreigingen, disruptie en innovatiebehoeften. ✓ Vormt de basis voor beleidsontwikkeling, waarbij vaak maatwerk aan de orde is. *[ref. DSII]*	✓ Nederland heeft hiervoor een eigen kennispositie, zowel bij kennisinstellingen als binnen de Defensieorganisatie zelf. *[Ref. DSII]*
Samenvattend: Kennis en technologie op het gebied van Strategic Foresight & Analysis zijn van wezenlijk belang bij het anticiperen op dreigingen, disruptie en innovatiebehoeften. Het vormt de basis voor beleidsontwikkeling, waarbij vaak maatwerk aan de orde is. [zie 4.13 Maatwerk voor kleine landen] Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt dan ook voor de hand, zeker omdat Nederland een goede kennisbasis heeft op dit vlak. [zie 4.5 Brede kennisbasis] De meest voor de hand liggende SMART-rollen voor Defensie zijn: User en Specifier.				

10.8 Human Resource Management & Organization	✓ Autonomie bij gereedstelling, duurzaamheid en inzetbaarheid van de krijgsmacht. *[ref. DSII]*	NVT	✓ Bevordert welzijn, inzetbaarheid en effectiviteit van defensiepersoneel. ✓ Essentieel voor gereedstelling, duurzaamheid en inzetbaarheid van de krijgsmacht. ✓ Vaak is maatwerk vereist, gericht op de karakteristieken van de Nederlandse krijgsmacht. *[ref. DSII]*	✓ Nederland heeft hiervoor een eigen kennispositie, bij kennisinstellingen en ook binnen de Defensieorganisatie zelf. *[ref. DSII]*
Samenvattend: Kennis en technologie op het gebied van Human Resource Management & Organization zijn van wezenlijk belang voor gereedstelling, duurzaamheid en inzetbaarheid van de krijgsmacht. Het bevordert welzijn, inzetbaarheid en effectiviteit van defensiepersoneel. Daarbij is vaak maatwerk vereist, gericht op de karakteristieken van de Nederlandse krijgsmacht. [zie 4.3 Nederlandse karakteristieken; 4.13 Maatwerk voor kleine landen] Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt dan ook voor de hand, zeker omdat Nederland een goede kennisbasis heeft op dit vlak. De meest voor de hand liggende SMART-rol voor Defensie is: User.				
10.9 Ethics & Legal	✓ Autonomie bij het opstellen en handhaven van criteria voor (en tijdens) defensie-inzet.	✓ Beschermt tegen misbruik en 'escalation of force', verhoogt publieke legitimiteit, en verlaagt daarmee het risico op sociale onrust door bijvoorbeeld ongewenste buitenlandse inmenging. *[ref. DSII]*	✓ Biedt kader voor inzetcriteria en interoperabiliteit met bondgenoten. ✓ Beschermt tegen misbruik en 'escalation of force', verhoogt maatschappelijk draagvlak voor defensieinzet, en verlaagt daarmee het risico op sociale onrust door bijvoorbeeld ongewenste buitenlandse inmenging *[ref. DSII]*	✓ Nederland heeft hiervoor een eigen kennispositie, bij kennisinstellingen en ook binnen de Defensieorganisatie zelf. *[ref. DSII]*
Samenvattend: Kennis en technologie op het gebied van Ethics & Legal zijn van wezenlijk belang voor het opstellen en handhaven van inzetcriteria alsmede interoperabiliteit met bondgenoten. Daarbij is vaak maatwerk vereist, gericht op de Nederlandse samenleving en de karakteristieken van de Nederlandse krijgsmacht. [zie 4.3 Nederlandse karakteristieken; 4.13 Maatwerk voor kleine landen] Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand, zeker aangezien Nederland beschikt over een goede kennisbasis op dit vlak. De meest voor de hand liggende SMART-rol voor Defensie is: Specifier.				

10.10 System Engineering & Innovation	✓ Autonomie inzake systeemspecificatie en functionele integratie. *[ref. DSII]*	NVT	✓ Belangrijk voor innovatie, capaciteitsontwikkeling, systeemontwikkeling en systeemmodernisering. ✓ Door integrale ontwerpkeuzes kunnen (veiligheids)eisen vroegtijdig geborgd worden. *[ref. DSII]*	✓ Nederland heeft hiervoor een eigen kennispositie, bij kennisinstellingen en ook binnen de Defensieorganisatie zelf. *[ref. DSII]*
Samenvattend: Kennis en technologie op het gebied van System Engineering & Innovation zijn van wezenlijk belang voor innovatie, capaciteitsontwikkeling en systeemontwikkeling. Het levert een grote bijdrage aan systeem-integratie en het voortdurende innoveren en aanpassen van bestaande capaciteiten. [zie ook 4.6 Innovatie gedurende levensduur; 4.7 Integratievermogen] Het minimaliseren van afhankelijkheden van buitenlandse partijen ligt daarom voor de hand, zeker omdat Nederland beschikt over een goede kennisbasis op dit vlak. De meest voor de hand liggende SMART-rollen voor Defensie zijn: Specifier en Integrator.				

Referenties

Ministerie van Defensie (2018). Defensienota 2018: Investeren in onze mensen, slagkracht en zichtbaarheid. *[afkorting: DN2018]*

The Hague Centre for Strategic Studies (2018). Wezenlijke belangen en de nationale defensie gerelateerde industriële en technologische basis. *[afkorting: HCSS WB]*

Nota Defensie Industrie Strategie (2018). *[afkorting; DIS]*

Ministerie van Defensie (2020). Defensievisie 2035: Vechten voor een veilige toekomst. *[afkorting: DV2035]*

Rijksbrede Risicoanalyse Nationale Veiligheid (2022), Analistennetwerk Nationale Veiligheid. *[afkorting: RRNV]*

Rijksoverheid (2023). De Veiligheidsstrategie voor het Koninkrijk der Nederlanden. *[afkorting: VS NL]*

Ministerie van Defensie (2024). Defensienota 2024: Sterk, slim, samen. *[afkorting: DN2024]*

Technologieverkenning 2024 (2024), TNO 2024 R10818 *[afkorting: TV2024]*

Dreigingsbeeld militaire en hybride dreigingen (2024). *[afkorting: DB MH]*

Militaire Inlichtingen en Veiligheidsdienst (2025). Openbaar Jaarverslag 2024. *[afkorting: MIVD]*

Defensie Strategie voor Industrie en Innovatie 2025-2029 (2025). *[afkorting: DSII]*

Strategische Actieagenda Industrie, Innovatie en Kennis – Defensie 2025 (2025). *[afkorting: STRAIIK]*

Defence, Safety & Security

Oude Waalsdorperweg 63
2597 AK Den Haag
www.tno.nl

TNO innovation for life