Impulsprogramma Defensie

Oriëntatieroadmap

Ruimtevaart & Defensie

“Space4Defense”

Document opgesteld door Flanders Space,
de cluster van de Vlaamse ruimtevaartactoren, op vraag van WEWIS

Vlaamse Ruimtevaartindustrie
Vereniging zonder winstoogmerk
IBAN BE07 9733 9977 9066

Berkenrodelei 33
Tel +32 (0)477 22 88 67
www.vri.vlaanderen

B-2660 Hoboken
contact@vri.vlaanderen
BTW BE 0455.534.170

INHOUD

1. Inleiding: visie en context

1.1. Ruimtevaart in defensie: strategisch domein van de 21ste eeuw

Ruimtevaart is niet langer het exclusieve domein van wetenschappelijke exploratie of commerciële satellietdiensten. In het huidige geopolitieke landschap is de ruimte uitgegroeid tot een cruciaal strategisch domein voor defensie. Van communicatie en navigatie tot aardobservatie, surveillance en cyberbeveiliging: militaire operaties zijn steeds afhankelijker van ruimtecapaciteiten.

Tegelijkertijd brengt deze afhankelijkheid nieuwe dreigingen met zich mee. Deze variëren van cyberaanvallen, jamming en spoofing, misinformatie en het risico op botsingen in de ruimte door de toename van het aantal satellieten. De ruimte is daarmee uitgegroeid tot een nieuwe dimensie van veiligheid en militaire paraatheid. Dit doet een nieuwe geopolitieke wedloop ontstaan: landen investeren fors in ruimtecapaciteiten om strategisch voordeel te behalen of zich te verdedigen tegen aanvallen op hun ruimteinfrastructuur.

De technologische innovaties en evoluties bieden kansen voor de Vlaamse ruimtevaartindustrie om kritieke technologie en diensten te ontwikkelen die bijdragen aan de Europese *Defence Technological and Industrial Base* (EDTIB). Het Vlaamse ruimtevaartecosysteem is immers sterk verweven met Europese programma's en is dus goed geplaatst om mee de vruchten te plukken van de massale investeringen die de komende jaren zullen gebeuren in het domein van veiligheid en defensie.

Deze oriëntatieroadmap positioneert Vlaanderen binnen een Europese en trans-Atlantische context. Ze sluit aan bij Europese beleidsinitiatieven zoals de EU Space Strategy for Security and Defence, de NAVO-doelstelling om minstens 5% van het bbp te spenderen aan Defensie, nieuwe ESA-programma's rond veiligheid en defensie, de EDA Captech Space en andere Europese steuninstrumenten zoals het Europese Defensiefonds (EDF). De inhoud van de oriëntatieroadmap is technologisch en toegepast: we vertrekken van concrete toepassingsdomeinen die zich op het kruispunt tussen ruimtevaart en defensie bevinden en leggen daarin de focus op bouwstenen die binnen een realistische termijn tot concrete resultaten kunnen leiden.

Alvorens dieper in te gaan op de Vlaamse sterktes voor Space4Defense lichten we de Europese en Belgische beleidscontext toe die het belang van een Vlaamse programma rond veiligheid en defensie onderstrepen dat als doel moet hebben om Vlaamse spelers te positioneren op Europese markten en binnen grote consortia.

De domeinen waarin de ruimtevaartindustrie vandaag actief is, worden grotendeels bepaald door de initiatieven van Europese instanties. Ook de Belgische Defensie aligneert zich daar deels op voor Space4Defense ontwikkelingen. Denk hierbij aan het Europese Defensieagentschap (EDA) en de CapTech vergaderingen, NAVO DIANA en NAVO-Innovatiefonds en uiteraard de Europese Ruimtevaartorganisatie (ESA).

1.2. Europese initiatieven

Naast de NAVO zet ook de Europese Unie stevig in op defensie. Het creëren van ruimtelijke autonome capaciteit, veerkracht, regelgeving, technologische innovatie en samenwerking staan daarin centraal.

De EU Space Strategy for Security and Defence legt de nadruk op:

- De **bestaande Flagship satellietprogramma's** Galileo (navigatie), Copernicus (aardobservatie), SSA (ruimtebewaking) en GOVSATCOM (overheidscommunicatie) volledig uitrollen met bijkomende diensten rond defensie en aanvullen met IRIS^2 voor veilige connectiviteit
- **IRIS^2** (Infrastructure for Resilience, Interconnectivity and Security by Satellite) beoogt tegen 2027 een constellatie van honderden LEO- en MEO-satellieten te hebben voor veilige connectiviteit voor overheden en breedbandinternet voor burgers
- **Een breed regelgevend kader** met wetgeving rond objectdetectie, Space Traffic Management en duurzaamheid in ruimteactiviteiten, inclusief anti-botsing en cyber-securitystandaarden. De recent gepubliceerde EU Space Act vormt hier een belangrijke eerste stap
- **Een versterking van de ruimtevaart- en defensietechnologische en industriële basis (EDTIB) en hernieuwde samenwerking**, **onderzoek en gezamenlijke inkoop** via de Europese defensie-industrieprogramma's zoals het *European Defence Industry Programme* (EDIP), het *EU Defence Innovation Scheme* (EUDIS) en het EDF-programma.
- **Een geïntegreerde defensiecapaciteit creëren** waarbij dual use Satcom en aardobservatie gecombineerd wordt met traditionele defensiesectoren zoals luchtverdediging, cyber, waarschuwing op zee, enz.

Ook de Europese ruimtevaartorganisatie ESA maakt een opvallende koerswijziging en begeeft zich steeds nadrukkelijker op het terrein van defensie. Traditioneel richtte ESA zich uitsluitend op civiele en wetenschappelijke missies, maar geopolitieke spanningen en technologische ontwikkelingen hebben geleid tot een herdefiniëring van haar rol. De nieuwe defensiegerichte initiatieven van ESA, waar normaliter eind 2025 belangrijke beslissingen over worden genomen door de Ministers bevoegd voor ruimtevaart, zijn:

- Een nieuw aardobservatieprogramma **European Resilience from Space (ESR)** bedoeld om Europa's capaciteit voor inlichtingenvergaring te versterken. Dit systeem zou real-time beeldvorming mogelijk maken en meerdere observaties per uur kunnen uitvoeren en zodoende helpen bij snelle respons in crisissituaties zoals natuurrampen, cyberaanvallen of geopolitieke conflicten;
- **Groeiende politieke steun** om ESA te laten evolueren naar defensietoepassingen. Zo werkt de Europese Commissie samen met ESA aan het *Earth Observation Government Service*-project, dat dual use toepassingen onderzoekt;
- **Sterk inzetten op het gebruik van de ruimte en ruimtevaartinfrastructuur voor veiligheid en veerkracht**, eerder dan voor offensieve doeleinden. Het gaat daarbij vooral om beveiligde satellietcommunicatie, aardobservatie en *Space Situational Awareness*.

1.3. Opportuniteiten op Belgisch vlak

In het STAR-plan en in de Strategische Visie 2025 wordt ruimtevaart door de Belgische defensie expliciet vermeld als domein waarin militaire en duale projecten kunnen worden gefinancierd. De vorige Belgische regering heeft in het kader van de Belgische deelname aan de ESA-programma's beslist om 100 miljoen euro uit het Defensiebudget toe te wijzen aan bepaalde ESA-programma's en -activiteiten die in de periode 2023-2029 tegemoetkomen aan de Belgische veiligheids- en defensiebehoeften. Op die manier wordt een deel van DIRS-budget (*Defence Industry and Research Strategy*) gereserveerd voor ruimtevaart en cyberprojecten.

De Belgische Defensieruimtevaartstrategie wil, binnen een bredere Europese en trans-Atlantische context, bijdragen aan een veilige en beveiligde ruimte en een duurzame toegang verlenen tot veerkrachtige diensten van hoge kwaliteit voor de Belgische defensie en de veiligheidsdiensten. Er wordt daarbij gefocust op de volgende vijf domeinen:

- ***Space Situational Awareness*** **(SSA)**, voor het volgen van kunstmatige ruimteobjecten door naar de ruimte te kijken. Dit wordt door Defensie als een eerste Flagshipmissie gezien
- ***Space-Based Information, Surveillance & Reconnaissance*** **(SB-ISR)**, waarbij het aardoppervlak vanuit de ruimte wordt geobserveerd en geanalyseerd (*Space Based Earth Observation* - SBEO). Dit wordt beschouwd als een tweede Flagshipmissie
- Het ontwikkelen van capabilities rond **Satellietcommunicatie (Satcom)** om een veilig en stabiel communicatienetwerk via satelliet(en) te bieden
- ***Positioning, Navigation & Timing*** **(PNT)**, waarbij de beschikbaarheid en nauwkeurigheid van navigatie- en plaatsbepalingssystemen wordt gegarandeerd via toegang tot *Global Navigation Satellite Systems* (GNSS, zoals de Amerikaanse GPS en Europese Galileoconstellaties)
- Het ontwikkelen van technology building blocks en satellietplatformen die langetermijnoperaties in **VLEO (Very Low Earth Orbit)** toelaten.

1.4. De weerhouden toepassingsdomeinen binnen Space4Defense

Uit bovenstaand overzicht blijkt dat de Europese programma's en initiatieven, behoudens enkele nuances, steeds inzetten op dezelfde soort capaciteiten die voor Space4Defense relevant zijn. Eigen aan de organisaties is dat ze die (soms) een andere naam geven, maar uiteindelijk komt het neer op ontwikkelingen binnen gelijkaardige toepassingsdomeinen, met name:

- **Space Situational Awareness** met aandacht voor *Space Surveillance & Tracking* (SST) om satellieten en ruimtepuin te volgen om botsingen te voorkomen, de detectie van Near-Earth Objects (NEO) en het voorspellen van zonne-uitbarstingen die systemen kunnen verstoren (*Space Weather Events*)
- **Space Based Earth Observation** om de effectiviteit van militaire operaties aan de hand van aardobservatiedata te verhogen
- Satellietcommunicatie (**Satcom**) die beveiligde spraak-, data- en videocommunicatie tussen commandocentra, troepen, schepen en vliegtuigen moet toelaten met een wereldwijde dekking met versleutelde en beveiligde connectiviteit
- **Positioning, Navigation & Timing** (PNT) met focus op real-time coördinatie van troepen (Command & Control), *Global Navigation Satellite System* (GNSS) geleide raketten en drones die tot op de meter nauwkeurig zijn, synchronisatie van netwerken en de detectie

van jamming en spoofing (verstoring van het signaal) om ook tegenmaatregelen te kunnen nemen.

In het kader van de oriëntatieroadmapoefening worden deze domeinen weerhouden. Ze komen immers steeds terug in de diverse beleidsinitiatieven en stroken bovendien goed met de Vlaamse sterktes. Een ontluikende technologie, die nog in de onderzoeksfase zit, is het gebruik van VLEO-satellieten voor aardobservatiemissies. Die ontwikkeling nemen we mee in de EO-roadmap.

1.5. Kansen van morgen

Ruimtevaart is vandaag onmisbaar geworden voor veiligheid en defensie. Het is een strategische domein net zoals land, zee, lucht en cyber. Ruimtegebaseerde systemen ondersteunen vrijwel alle aspecten van militaire operaties. De dreigingen in de ruimte maken het noodzakelijk om de eigen infrastructuur te beschermen. Zowel binnen Europa en op Belgisch vlak worden stappen gezet om capaciteiten te ontwikkelen die de autonomie, de veerkracht en de weerbaarheid verhogen.

Met een succesvolle ruimtevaartindustrie, toonaangevende kennisinstellingen en universiteiten beschikt Vlaanderen over voldoende troeven om een belangrijke rol te spelen in het domein van Space4Defense. Om de opportuniteiten ten volle te benutten, is het noodzakelijk om een Vlaams beleid rond O&O&I in defensie en ruimtevaart te ontwikkelen, gebaseerd op de Vlaamse sterktes en binnen de eigen bevoegdheden.

De Space4Defense oriëntatieroadmap vertaalt de Vlaamse sterktes naar concrete innovatiepaden voor defensie. Ze richt zich daarbij op de 4 hierboven vermelde toepassingsdomeinen en levert voor elk domein: (1) een visie en een doelstelling, (2) prioritaire uitdagingen en innovatiedoelen, (3) technologische bouwstenen (4) een idee van projectthema's voor de toekomst.

2. Stakeholdermapping

2.1. Inleiding

De Vlaamse ruimtevaartsector kan terugblikken op een succesvolle periode. De oprichting in 1995 van de vzw Vlaamse ruimtevaartindustrie (VRI) was een katalysator in het samenbrengen van bedrijven, kennis- en onderwijsinstellingen die in Vlaanderen actief zijn in dit domein. De bedrijfsorganisatie telt vandaag 48 leden en is representatief voor de verschillende activiteiten in de ruimtevaart. In 2018 werd ze door VLAIO erkend als clusterorganisatie. Sinds 2021 coördineert VRI op vraag van de Vlaamse Regering het impulsprogramma Flanders Space dat de ruimtevaarteconomie in Vlaanderen verder gestalte wil geven.

De gecumuleerde omzet van de VRI-leden is sinds 1985 onafgebroken toegenomen met quasi een verdubbeling van de gezamenlijke omzet elke 10 jaar. De sector groeide tot 380 miljoen euro in 2023 en die evolutie zal zich de komende jaren doorzetten dankzij het toenemend socio-economisch belang van ruimtevaart in Europa en in de wereld en dankzij nieuwe toepassingsdomeinen zoals die voor veiligheid en defensie.

2.2. Vlaamse sterktes relevant voor Space4Defense

De Vlaamse ruimtevaartactoren hebben van bij het begin ingezet op de ontwikkeling van strategische niches. Veelal bieden zij een deel van een totaaloplossing aan en werken daarom bijna altijd samen in een consortium met andere partners. Door hun expertise en kennis zijn ze een gewaardeerde partner in Europese ruimtevaartprojecten.

Tot de belangrijkste expertisecentra, zowel binnen de universiteiten, onderzoekscentra en de industrie, die tevens relevant zijn voor defensietoepassingen, behoren:

- **Imaging4Space, beeldsensoren en camera's**: vandaag is ongeveer 25% van het ledenbestand van Flanders Space actief op het vlak van de ontwikkeling en de productie van beeldsensoren, imagers, detectoren, instrumenten, camera's en afgeleide producten en diensten. De Vlaamse ruimtevaartindustrie is dus zeer goed vertegenwoordigd in het ecosysteem van de aardobservatie. Evoluties rond hogere resoluties, multi- en hyperspectrale gevoeligheden bieden kansen om nieuwe, innovatieve technologie voor defensieapplicaties in Vlaanderen te ontwikkelen
- **Fotonica on a chip**, ook wel geïntegreerde fotonica genoemd, is een revolutionaire technologie waarbij lichtdeeltjes (fotonen) in plaats van elektronen worden gebruikt om informatie te verwerken en te transporteren. Het is een veelbelovende innovatie in de wereld van chips en micro-elektronica waarin in Vlaanderen, vooral bij de kennisinstellingen en universiteiten, reeds veel onderzoek naar gebeurt. Voor ruimtevaart en defensie laat dit robuuste, veilige communicatie en navigatie toe (bv. dankzij hoge datasnelheden en de miniaturisatie). De Vlaamse kennisinstellingen en universiteiten die hierrond werken zijn lid van Flanders Space of hebben samenwerking met één of meerdere leden
- Op basis van het Vlaamse marktleiderschap rond **satellietcommunicatie**, wordt meegewerkt aan de uitrol van flexibel inzetbare en beveiligde satellietcommunicatie waarbij interoperabiliteit tussen Europese agentschappen en manschappen centraal staat. Het EDF-project 'European Protected Waveform', waarin verschillende Flanders Space leden het voortouw nemen, is daar een voorbeeld van

- Ook **energievoorziening en -productie** via efficiënte powercomponenten en germanium gebaseerde halfgeleider wafers voor de productie van zonnecellen is een Vlaams speerpunt met enkele spelers die hierin wereldleider zijn
- De meest geavanceerde **sensoren, meetsystemen en halfgeleiders** die bovendien stralingshard zijn, worden in onze regio ontwikkeld
- Vlaanderen beschikt over een ecosysteem dat accurate **GNSS-ontvangers en positioneringssystemen** op de markt brengt. De uitdagingen rond miniaturisatie, energieverbruik, datafusie en verbeterde accuraatheid laten de ontwikkeling van nieuwe toepassingen toe, zowel voor het civiele als voor het militaire domein. De *Public Regulated Service* (PRS) is een speciaal beveiligde dienst van het Europese satellietnavigatiesysteem Galileo waarin ook Vlaamse ruimtevaartactoren actief zijn. Daarbij wordt gefocust op het aanleveren van diensten voor politie, civiele bescherming, douane, brandweer en defensie
- Met de PROBA-satellieten (Project for On-Board Autonomy) speelt Vlaanderen een hoofdrol in de **combinatie van technologische demonstraties met wetenschappelijke missies**
- Tot slot behoren de Vlaamse universiteiten en kennisinstellingen bij de wereldtop voor wat betreft het **ruimtevaartonderzoek** rond de impact van straling op astronauten, gesloten life support systemen voor de ruimte, de planetaire terugkeer uit de ruimte, materiaalonderzoek en celbiologie en de bouw en exploitatie van instrumenten voor grote astrofysische ruimtevaartmissies

2.3. Indeling op basis van Technology Domains

Bekijken we het Vlaamse ruimtevaartecosysteem vanuit het standpunt van de *Technology Domains* (die onder andere door ESA en NASA worden gebruikt), dan krijgen we volgende beeld:

- Space Systems & Satellite Tech: 11 actoren
- Materials, Manufacturing & Industrial Engineering: 6 actoren
- Sensors, Instrumentation & Electronics: 9 actoren
- Software & Digital: 8 actoren
- Incubation & Consulting: 6 actoren
- Research & Development: 8 actoren

Het gedetailleerd overzicht van de ecosysteemmapping met vermelding van de 48 ruimtevaartactoren kan bij Flanders Space worden geconsulteerd.

2.4. Key lessons learned

- Heterogeen landschap: doorheen de jaren zijn in Vlaanderen sterke niches ontwikkeld, vooral in het upstream segment van de ruimtevaart gericht op de ontwikkeling van infrastructuur voor lancering in de ruimte. Het gaat om een veelvoud van competenties die verschillend zijn van bedrijf tot bedrijf.
- Er is een bepaalde mate van afhankelijkheid van *prime contractors* en Europese O&O-programma's, vooral in de ontwikkelingsfase van nieuwe technologie. Ruimtevaart is een risicovolle en kapitaalintensieve activiteit. Het is daarom belangrijk om voldoende hoog in de waardeketen in te breken en een systeemoplossing te kunnen aanbieden.

Vlaamse actoren zijn zeer succesvol om hun producten en diensten op commerciële markten te verkopen. Ze zetten op die manier een sterke hefboom op de ontvangen O&O-financiering.

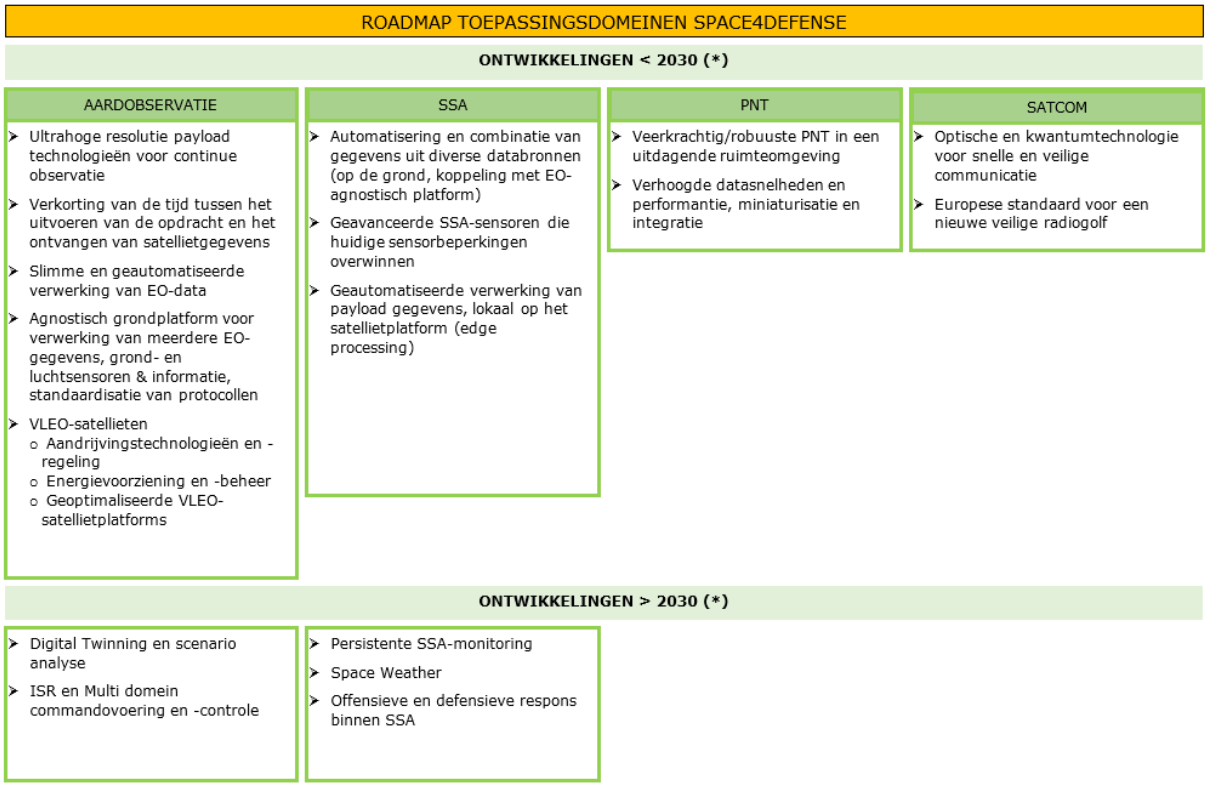
- Het is een uitdaging, zeker voor KMO's en starters, om een beeld te krijgen van de capaciteiten die moeten ontwikkeld worden voor de defensiemarkten
- Er is nood aan verdere strategische positionering en consolidatie van de posities door voldoende langetermijnprogramma's en meerjarenfinanciering.
- De clusterwerking via Flanders Space is een belangrijke hefboom om het bestaande netwerk verder uit te breiden, om actoren – zeker ook buiten de ruimtevaartsector – met elkaar te laten samenwerken en nieuwe toepassingen te ontwikkelen.

3. Space4Defense roadmap

Voor elk van de 4 toepassingsdomeinen is de roadmap opgebouwd op basis van de volgende structuur:

- De **visie en het doel** dat we nastreven ('Mission')
- **Focus**: welke problemen en uitdagingen lossen we op?
- **Bouwstenen**: wat willen we doen binnen het toepassingsgebied? Welke concrete innovatiedoelen/technologische ontwikkelingen willen we bereiken?
- Welke **projecten** (innovatiekansen) zouden er binnen het toepassingsgebied mogelijk zijn (dit is louter ter inspiratie en niet-limitatief)

De globale oriëntatieroadmap ziet er als volgt uit:



Figuur 1: Visuele Space4Defense oriëntatieroadmap

(*) Het onderscheid tussen ontwikkelingen tot 2030 en deze erna is gemaakt op basis van de huidige inputs van de leden. Indien tijdens de uitvoering van de oriëntatieroadmap blijkt dat bepaalde ontwikkelingen eerder moeten gebeuren, dan is dat uiteraard mogelijk.

Elk van de pijlers wordt hierna verder toegelicht. Ook geven we een aanzet tot mogelijke synergieën tussen Space4Defense en de andere toepassingsdomeinen.

3.1. Pijler 1 — Aardobservatie

➢ Visie

EO-vermogen is essentieel voor strategische en tactische besluitvorming. Vlaanderen richt zich op multisensor *payloads* (Electro-Optical, Radio Frequency (RF) monitoring, Synthetic Aperture Radar (SAR), multi/hyperspectraal, infrarood,…) in een veerkrachtig en flexibel netwerk met aangepast grondstation. Op korte termijn willen we de capaciteiten operationaliseren binnen het GALO-concept (Global coverage All weather LEO Observation). Het verzekert een permanente, bijna real-time data acquisitie in alle weersomstandigheden en biedt zo een strategisch voordeel voor defensietoepassingen. Op langere termijn gaat het om de ontwikkeling van digital twins, simulatie en scenario-analyse met multidomein command & control

➢ Focuslaag en bijbehorende bouwstenen (innovatiedoelen)

De focus ligt op technologische bouwstenen die bijdragen aan de volgende generatie oplossingen rond aardobservatie voor militaire doeleinden. De volgende innovatie-uitdagingen zijn daaraan verbonden:

- Ultrahoge resolutie payload technologieën voor continue observatie, ongeacht de observatie- en weersomstandigheden
    - Sensoren met hoge precisie/efficiënte resolutie voor RF, SAR, infrarood, hyperspectraal
    - Miniaturisatie en energie-efficiëntie van *payloads* (zogenaamde edge ontwikkelingen, dus op de chip)
- Verkorting van de tijd tussen het uitvoeren van de opdracht en het ontvangen van satellietgegevens
    - Slimme en geautomatiseerde taakuitvoering
    - Geautomatiseerde, door AI ondersteunde, geolocatie
    - Satellietcommunicatie tussen systemen
- Slimme en geautomatiseerde verwerking van EO-data
    - De behoefte aan menselijke tussenkomst zoveel mogelijk minimaliseren
    - Gefedereerde, gemeenschappelijke infrastructuur voor het veilig beheren van grote hoeveelheden data
- Ontwikkeling van een aangepaste, data agnostische, grondinfrastructuur
    - Momenteel gaat veel aandacht naar satelliet- en upstreamontwikkelingen, maar de vraag rijst of hiermee de volledige defensiewaardeketen wordt aangesproken. Om de defensiebehoeften adequaat in te vullen, is ook de verwerking, de integratie en de interpretatie van de reeds wereldwijd beschikbare datastromen cruciaal. Daarvoor is de uitbouw van een aangepast grondsegment essentieel. Dit platform moet cross-domein functioneren, interoperabele standaarden definiëren die de gemakkelijke uitwisseling van gegevens toelaten en in staat zijn om gegevens afkomstig van diverse aardobservatieconstellaties en andere sensoren (van andere platformen zoals bv. drones) efficiënt te verwerken en te benutten

- VLEO-satellieten
    - Door hun lagere omloopbaan, bieden VLEO-platformen een lagere latentie (vertraging in de dataoverdracht over een datacommunicatienetwerk), hogere resolutie en meer beelden per omloopbaan, maar ze vergen ook drag compensatie (tegengaan van de atmosferische weerstand), duurzame energievoorziening en robuuste platformen. Vlaanderen kan zich binnen dit domein richten op efficiënte elektrische voortstuwing, een geoptimaliseerd aerodynamisch ontwerp, attitude controlesystemen, verbeterde communicatie en de ontwikkeling van het satellietplatform

➢ Voorbeelden van onderzoek en ontwikkelingen:

- Sensortechnologie, payloadontwikkelingen, miniaturisatie, fotonicaoplossingen, data en AI gedreven optimalisaties, anomaliedetectie, mobiele grondstations, in-orbit demonstratie voor VLEO,...

3.2. Pijler 2 – Space Situational Awareness (SSA)

➢ Visie

SSA waarborgt veiligheid en soevereiniteit in de ruimte. Vlaanderen kan focussen op geautomatiseerde, bijna real-time visualisatie van de bedreigingen door de integratie van diverse sensoren (radar, optisch, RF, infrarood) en AI-gestuurde gedragstypologie. Op korte termijn is end-to-end automatisering van de dataverzameling en initiële dreigingsclassificatie belangrijk. Op langere termijn vormen voortdurende tracking en observatie en een mogelijke defensieve beschermingsactie belangrijke actielijnen, net zoals het onderzoek naar de impact van het zonneweer op ruimteinfrastructuur.

➢ Focuslaag en bijbehorende bouwstenen

- Automatisering en combinatie van gegevens uit diverse databronnen (koppeling met het hierboven beschreven EO-agnostisch platform)
    - De hierboven beschreven grondinfrastructuur moet ook toelaten om SSA-data te verzamelen en te verwerken
    - Datafusie en -analyse, aangevuld met AI capabilities zowel op het niveau van de satelliet en op de grond, moet leiden tot het beter waarnemen en volgen van objecten in de ruimte en het nemen van snellere beslissingen over bedreigingen
- Ontwikkeling van geavanceerde SSA-sensoren die de huidige sensorbeperkingen overwinnen
    - Gelet op de Vlaamse expertise rond Imaging4Space, kan Vlaanderen een leidende rol nemen in de ontwikkeling van sensortechnologie
- Geautomatiseerde verwerking van gegevens
    - Edge computing en edge processing, dus op het niveau van de satelliet, zijn veelbelovende technologieën die er ook voor zorgen dat alleen de meest waardevolle data vanuit de ruimte naar de grond wordt gestuurd

- Voorbeeldonderzoek
    - Sensortechnologie, ontwikkeling AI capabilities met machine learning, ontwikkelingen rond voorspellingen, impact en risicoanalyse en scenario building, stralingshardheid van componenten, defensieve acties waarbij botsingen worden gemeden,...

3.3. Pijler 3 - PNT capaciteiten

➢ Visie

PNT waarborgt veiligheid en soevereiniteit op aarde. Vlaanderen focust op robuuste, veerkrachtige en veilige Positioning, Navigation & Timing door integratie van multi GNSS-constellaties, de uitbouw van terrestriële back-upsystemen, de ontwikkeling van geavanceerde ontvangers, kwantumtechnologie en beveiligde satellietdiensten voor kritieke applicaties en overheidsdiensten.

➢ Focuslaag en bijbehorende bouwstenen

- De accuraatheid en precisie van PNT en navigatiesignalen verhogen wat een grote impact heeft op zowel civiele als militaire toepassingen
    - De combinatie van hybride en multi-constellaties (diverse satellieten in verschillende omloopbanen, gecombineerd met terresteriële signalen,...) met multi-frequenties leidt tot een betere robuustheid van systemen en biedt weerstand tegen jamming en spoofing
    - Multi GNSS-constellaties dragen bij aan missiekritieke nauwkeurigheid: in militaire operaties kan een verschil van enkele meters het succes of falen van een missie bepalen
    - De precisie van drones en UAVs wordt aanzienlijk verbeterd
- De ontwikkelingen rond kwantumtechnologie kunnen veelbelovend zijn voor Vlaamse actoren om de coördinatie en de betrouwbaarheid van systemen die op GNSS steunen te verhogen
- Andere interessante bouwstenen betreffen innovaties in onboard receivers, de miniaturisatie van PNT-ontvangers, het verhogen van de snelheidsprestaties van elektronica en dataverwerking, enz.
- Vlaanderen kan binnen dit domein verder bouwen op de kennis inzake micro-elektronica, fotonica, kwantumtechnologie en AI.

De mogelijkheden binnen PNT moeten nog verder met de industrie en de kennisinstellingen worden uitgewerkt

➢ Voorbeeldonderzoek

- Projecten rond multi-constellaties (LEO-PNT), multi-frequentie en alternatieve PNT-bronnen, evoluties van standregelingssystemen voor (kleine) satellieten, spectrum monitoring en geolocatie, onderzoek rond atoomklokken en kwantumtechnologie, machine learning,....

3.4. Pijler 4 - Satcom ontwikkelingen

- Visie

Satcom waarborgt veiligheid, connectiviteit en strategische autonomie in communicatie. Vlaanderen focust op veilige, hoge bandbreedte satellietcommunicatie door integratie van multi-orbit capaciteiten (LEO, MEO, GEO), optische en kwantumcommunicatie en AI-gestuurde netwerkoptimalisatie. De inzet is zowel voor civiele (bescherming kritieke infrastructuur, rampenbeheer, maritiem, luchtvaart) als militaire toepassingen (communicatie in combinatie met aardobservatie, voor het verzamelen van inlichtingen en het uitvoeren van bewaking en verkenning en in het kader van Europese samenwerking).

- Focuslaag en bijbehorende bouwstenen

Zelfs in een regio zoals Vlaanderen waar de terrestriële telecominfrastructuur volledig geïntegreerd is via ondergrondse en bovengrondse bekabeling (coax, glasvezel, 5G torens) kan satellietcommunicatie nog steeds een belangrijke complementaire rol spelen. Bovendien zijn er binnen Vlaanderen enkele wereldspelers actief op vlak van Satcom technologie die kunnen bijdragen aan de uitbouw van een Vlaams ecosysteem en oplossingen voor specifieke use cases kunnen ontwikkelen, zoals de beveiliging van de offshore eilanden op de Noordzee, van havens en kritieke infrastructuur of een back-up satcominfrastructuur voorzien ingeval van natuurrampen (overstromingen, elektriciteitspanne, storm), congestie van bestaande netwerken of in afgelegen gebieden waar geen terrestriële oplossingen voor handen zijn. Specifiek voor defensie biedt satellietcommunicatie ondersteuning bij militaire operaties, grensbewaking en diplomatieke missies.

In al deze toepassingsgebieden zullen de laatste innovaties qua beveiliging en satcomtechnologie ingezet worden, zoals daar zijn:

- Verhogen van de datasnelheden van satelliet naar de grond en de verwerking van de ontvangen data
- Ontwikkeling van hybride satcom architecturen (radiofrequentie, optisch, software defined radio) en een naadloze overgang van de signalen tussen de infrastructuur waardoor interoperabiliteit met de netwerken op de grond verzekerd wordt
- Optische en kwantumontwikkelingen voor hogesnelheid en beveiligde satellietcommunicatie via geavanceerde encryptie, cyber hardening, anti-jamming/spoofing/intrusie technologie
- Integratie van de European Protected Waveform in Europese satellietcommunicatiesystemen
- Nieuwe productiemethodes en standaarden voor satcom hardware

De mogelijkheden binnen het satcom domein moeten nog verder met de industrie en de kennisinstellingen worden uitgewerkt.

- Voorbeeldonderzoek

- O&O&I rond optische communicatie, high-power lasers, grondstationinfrastructuur die de snel bewegende LEO-satellieten volgt, versleuteling en verwerking van de data, kwantumtechnologie, toekomstige Direct-to-Device (D2D)-verbindingen, AI en automatisatie voor de routering van gegevens en detectie van jamming/spoofing/intrusie,...

3.5. Mogelijke synergieën

De Vlaamse ruimtevaartactoren hebben de ambitie om gerichte bruggen te slaan tussen andere toepassings- en technologiedomeinen waarin Vlaanderen sterk staat. De evolutie naar een ruimtevaarteconomie impliceert immers het gebruik van ruimtedata en -infrastructuur om toegevoegde waarde te creëren, een datagedreven besluitvorming toe te laten en de groei in diverse economische sectoren te stimuleren.

De onderstaande tabel laat zien welke cross-domein synergieën mogelijk zijn. Tijdens de uitvoering van de verschillende Vlaamse oriëntatieroadmaps, moeten deze wisselwerkingen uiteraard verder verduidelijkt worden.

CROSS-DOMEIN SYNERGIEEN MET SPACE4DEFENSE						
TOEPASSINGSDOMEIN – MARITIEM	TOEPASSINGSDOMEIN – AI	TOEPASSINGSDOMEIN – CYBER	TOEPASSINGSDOMEIN – COUNTER UAV	TOEPASSINGSDOMEIN – ENERGY, ENVIRONMENT, GEO-INTEL	TOEPASSINGSDOMEIN – BIOTECH	TOEPASSINGSDOMEIN – HYPERSONICS
Mogelijke synergieën • Bescherming van kritieke maritieme infrastructuur • Maritime Domain Awareness (MDA) • Militaire mobiliteit en dual use infrastructuur • Autonome systemen en maritieme robotica	**Mogelijke synergieën:** • AI For Sensing • AI Compute • AI For Communication • AI For Operational Support	**Mogelijke synergieën:** • Security and resilience built-in for software- and hardware-based defense technology • Develop and integrate emerging security technology • Technology to support and enable Cyber Operations	**Mogelijke synergieën:** • Evolutie naar multi-sensor integratie • Adaptiviteit en AI-ondersteunde detectie • Netwerk-gebaseerde en gedistribueerde detectie • Transponders en elektronische ID-modules • Visuele en elektro-optische identificatie • Interceptor drones: mobiele neutralisatie in real-time	**Mogelijke synergieën:** • Onboard: Multibron-sensing en fusie voor situationeel overzicht • Onboard: Realtime edgeintelligentie • Onground: Veilige, veerkrachtige en soevereine geo-datainfrastructuur	**Mogelijke synergieën:** • Nog te Onderzoeken	**Mogelijke synergieën:** • Nog te Onderzoeken

4. Conclusie

Het belang van ruimtevaart binnen het domein van de veiligheid en defensie zal de komende jaren alleen maar toenemen. De geopolitieke situatie leidt er nu al toe dat deze component cruciaal is om de strategische autonomie, de veerkracht en de beveiliging van systemen en

mensen in Europa te waarborgen. Diensten en toepassingen gebaseerd op satellieten en satellietdata zijn onmisbaar geworden voor defensie en voor het samenleving in haar geheel.

De Vlaamse ruimtevaartsector, die binnen de civiele ruimtevaart een indrukwekkend en succesvol track record heeft opgebouwd door in te zetten op strategische niches, is goed geplaatst om een belangrijke rol te spelen in de ontwikkelingen rond Space4Defense. Het netwerk van bedrijven, kennisinstellingen en universiteiten is de afgelopen jaren sterk uitgebreid en werkt via de clusterorganisatie Flanders Space mee aan de uitbouw van een ruimtevaarteconomie. De kennis en de expertise van de actoren op het vlak van beeldvorming en -verwerking, satellietcommunicatie, navigatie en positiebepaling en het vermogen om de ruimteomgeving rondom de aarde te begrijpen, te monitoren en te voorspellen zijn sterke troeven die ook voor het defensiedomein relevant zijn.

Deze oriëntatieroadmap vertrekt vanuit die Vlaamse sterktes en geeft aan waar we in Vlaanderen een leidende rol kunnen spelen. Om de sterke posities te consolideren, verder uit te bouwen en er nieuwe te ontwikkelingen is steun van de overheid noodzakelijk via een ondersteunend O&O&I-steuninstrumentarium. In het kader van een dergelijk programma dient de oriëntatieroadmap verder uitgewerkt en omgezet te worden in concrete projecten en doelstellingen en dit in nauwe samenwerking met Flanders Space.

***

Impulsprogramma Defensie

Oriëntatieroadmap

Maritieme veiligheids- en defensiesystemen

Document opgesteld door de Blauwe Cluster

Inhoudsopgave

Visie en context:

Het maritieme domein ontwikkelt zich wereldwijd tot een strategisch gebied waar economische, veiligheids- en technologische belangen samenkomen. Waar zeegebieden vroeger hoofdzakelijk handelsroutes en energiecorridors vormden, zijn ze vandaag ook de frontlinie van geopolitieke spanningen en technologische competitie. Infrastructuur op en onder zee, datanetwerken en maritieme logistiek zijn niet langer louter civiele assets, maar vitale componenten van nationale en Europese veiligheid.

De recente toename van incidenten op zee illustreert de kwetsbaarheid van deze infrastructuren voor sabotage, spionage en ongewenste verkenningsactiviteiten. Ook het in kaart brengen van kritieke infrastructuur en de inzet van autonome, onbemande vaartuigen versterken de complexiteit van het dreigingsbeeld. Tegelijk brengt de toenemende digitalisering van maritieme systemen – van scheepsnavigatie tot offshore-controleplatformen – nieuwe risico's met zich mee.

Tegen deze achtergrond groeit de nood aan een versterkte en toekomstgerichte maritieme defensie-industrie. Vlaanderen beschikt hiervoor over een uitzonderlijke uitgangspositie: een sterk maritiem en technologisch ecosysteem waarin industrie, kennisinstellingen, havens en defensieactoren elkaar versterken. In dit ecosysteem komen kritieke infrastructuren samen – van logistiek en energie tot datacommunicatie en offshore-technologie – waardoor Vlaanderen uitermate geschikt is om nieuwe maritieme defensietechnologieën te ontwikkelen, te testen en te valoriseren.

Een toekomstgerichte maritieme defensiestrategie moet hierop anticiperen door:

• **Versterking van defensie-expertise:** Vlaanderen is voortrekker in autonome onderwatersystemen en mijnenbestrijdingscapaciteiten, domeinen waarin we nationaal en internationaal een voortrekkersrol vervullen.

• **Bescherming van vitale en kritieke infrastructuur:** Offshore energie, datakabels, pijpleidingen en logistieke hubs vragen om doorgedreven monitoring, digitale beveiliging en snelle responscapaciteiten.

• **Cyberveiligheid en digitale weerbaarheid:** De digitalisering van maritieme systemen vereist geavanceerde dreigingsdetectie, veilige communicatie en robuuste gegevensinfrastructuren.

• **Interoperabiliteit en samenwerking:** Efficiënte samenwerking tussen civiele, militaire en private actoren vraagt open standaarden, gedeelde situational awareness en innovatieve ecosystemen.

Naast de Vlaamse ambities past deze versterking perfect binnen het bredere Europese veiligheidskader, zoals uiteengezet in de *White Paper for European Defence – Readiness 2030*. De Europese Unie erkent het strategisch belang van het maritiem domein als vitaal onderdeel van haar defensie- en weerbaarheidsstrategie. Daarbij ligt de nadruk op de bescherming van onderzeese infrastructuur, versterking van maritieme situational awareness en interoperabiliteit binnen NAVO-verband.

De Europese Unie koppelt haar ambities inzake maritieme veiligheid en defensie nadrukkelijk aan de versterking van de **Europese Defensietechnologische en Industriële Basis (EDTIB)**. De EU erkent dat strategische autonomie in het maritieme domein niet alleen afhankelijk is van militaire capaciteit, maar ook van een robuuste industriële onderbouw die innovatief, interoperabel en minder afhankelijk is van derde landen.

Binnen deze Europese agenda tekenen zich volgende prioriteiten af:

- **Bescherming van kritieke maritieme infrastructuur:** Europa onderkent een stijgende dreiging van sabotage aan pijpleidingen, datakabels en offshore-installaties. De Noordzee wordt daarbij expliciet genoemd als kwetsbare regio voor hybride dreigingen. Er wordt ingezet op versterkte onderzeese surveillance, elektronische beveiliging en snellere responsmechanismen.
- **Maritime Domain Awareness (MDA):** De EU streeft naar een versterkt maritiem beeld door integratie van data uit lucht-, zee- en onderwatersensoren, ondersteund door AI en satelliettechnologie. Dit sluit nauw aan bij Vlaamse initiatieven rond sensorfusion en digital twins.
- **Militaire mobiliteit en dual-use infrastructuur:** De Europese Commissie identificeert maritieme logistieke knooppunten zoals havens als essentiële schakels voor militaire mobiliteit. Investeringen in robuuste, interoperabele en beveiligde havencapaciteit worden als prioritair bestempeld. Vlaamse industriële spelers kunnen hierin een sleutelrol opnemen door technologieën te leveren die zowel civiele als militaire toepassingen ondersteunen.
- **Autonome systemen en maritieme robotica:** De EU stimuleert gezamenlijk onderzoek en ontwikkeling in domeinen zoals onbemande vaartuigen (UUV's, USV's), mijnenbestrijding en onderwaterverkenning – technologieën waarin Vlaanderen al vooroploopt en verdere synergie kan worden gezocht met Europese programma's zoals het *European Defence Fund (EDF)* en *PESCO*-projecten.
- **Cyber- en elektronische oorlogsvoering:** Gezien de toenemende digitalisering van maritieme systemen, wordt sterk ingezet op cyberweerbaarheid en bescherming van het elektromagnetisch spectrum, inclusief voor maritieme en onderzeese assets. Dit sluit aan bij de Vlaamse focus op AI-gestuurde cyberdetectie en end-to-end beveiligingsarchitecturen.
- **Publiek-private samenwerking en innovatie:** De EU ziet in maritieme veiligheid een strategische sector waarin innovatieve kmo's en kennisinstellingen een sleutelrol spelen. Vlaanderen kan dankzij zijn sterke technologische basis en industriële maturiteit een proactieve partner zijn in pan-Europese defensie-ecosystemen.

Vlaanderen positioneert zich met deze roadmap als **proactieve industriële en technologische partner** binnen Europese en NAVO-initiatieven voor maritieme veiligheid, surveillance en hybrid threat detection in het Greater North Sea Basin. De verdere sensorificatie van de Noordzee – van onderzeese sensoren tot UAV-observatiesystemen – draagt bij aan de NAVO-doelstelling van *Full Ocean Space Situational Awareness* en versterkt de Vlaamse rol in de ontwikkeling van dual-use technologieën.

Ook de Vlaamse havens ondersteunen deze ambitie als facilitatoren van innovatie en samenwerking. Ze fungeren als industriële en logistieke knooppunten binnen de Europese military mobility corridors, en dragen zo bij aan de militaire weerbaarheid van deze corridors. De ontwikkeling van een sterke defensie-industrie komt daarmee niet enkel de militaire capaciteitsopbouw ten goede, maar versterkt ook Vlaanderens economische en technologische positie binnen Europa. . Ook de NATO benadrukt het belang van 'layered resilience', waarin industriële innovatie en veiligheid elkaar wederzijds versterken.

Vlaanderen, broedplaats voor maritieme innovatie

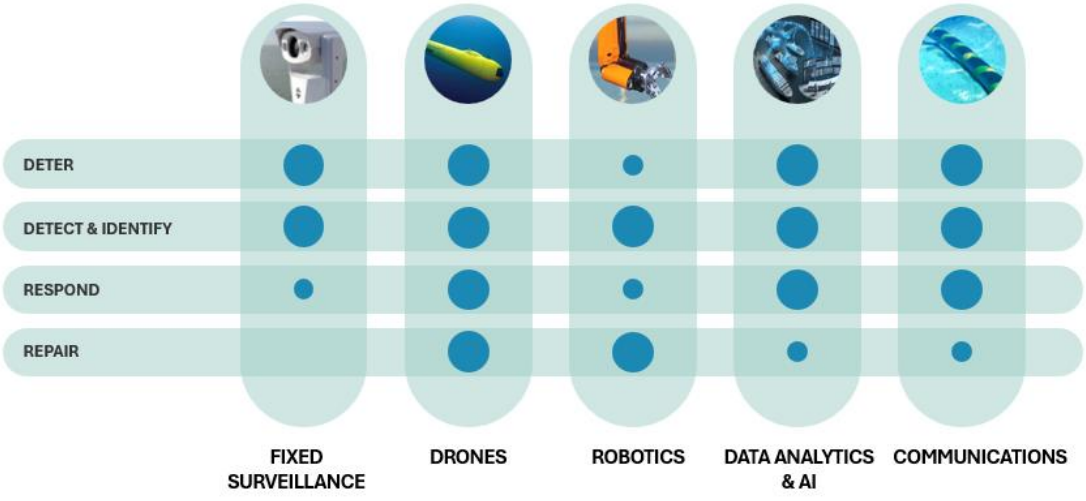
Het Vlaamse ecosysteem voor maritieme veiligheid en defensie is veelzijdig en sterk in opmars. Het steunt op een stevige basis van overheid en marine, gecombineerd met een intensieve samenwerking tussen onderzoeksinstellingen en innovatieve bedrijven. Vooral de wisselwerking tussen kennisinstellingen en kmo's vormt een motor voor vernieuwing: Vlaanderen ontwikkelt technologische oplossingen die zowel defensie-specifieke toepassingen als dual-use technologieën mogelijk maken, met toepassingen in havens, offshore energie en maritieme veiligheid en defensietoepassingen.
Binnen het Vlaamse maritieme defensie-ecosysteem tekenen zich duidelijke zwaartepunten af. Vlaanderen beschikt over een **kritische massa** in specifieke domeinen waar kennis, industrie en internationale samenwerking reeds sterk ontwikkeld zijn, naast enkele **groeidomeinen** waarin verdere consolidatie en opschaling wenselijk is.

Vlaanderen behoort tot de Europese top in **Mine Countermeasures (MCM)** en **autonome onderwatersystemen**. De combinatie van technologische innovatie, operationele kennis en samenwerking met de Belgische marine maakt dat Vlaanderen internationaal erkend wordt als **voortrekker in onderwaterdrones, mijnendetectie en -ruiming**. Deze expertise vormt een belangrijke toegangspoort tot Europese en NAVO-programma's.

In domeinen zoals **AI-gestuurde datafusion, maritieme cyberveiligheid, geautomatiseerde maritieme systemen** en **sensorintegratie** is Vlaanderen sterk in kennisontwikkeling en pilootprojecten, maar is terzelfdertijd verdere industrialisatie en clustering nodig om een duurzame marktpositie te verwerven. Initiatieven zoals testzones in havenomgevingen en gezamenlijke onderzoeksprojecten met defensie kunnen deze groei versnellen.

Vlaanderen bouwt daarnaast aan opkomende sterktes in **predictieve AI-toepassingen, digital twins, sensornetwerken** en **dual-use robotica**. Deze niches hebben een hoog innovatiepotentieel en kunnen uitgroeien tot technologische specialisaties.

Om dit innovatieve potentieel tastbaar te maken, kunnen we het Vlaamse maritieme defensie-ecosysteem opdelen in een aantal **technologische kerndomeinen**. Elk van deze domeinen vertegenwoordigt een cruciale schakel binnen het bredere maritieme veiligheidslandschap en weerspiegelt tegelijk de sterke kennisbasis en industriële capaciteiten die Vlaanderen vandaag in huis heeft. Samen vormen ze het fundament waarop Vlaanderen zijn rol als toonaangevende speler in maritieme veiligheid, defensie en dual-use technologie verder kan uitbouwen.



Fixed surveillance

Systemen die ontworpen zijn om binnen een afgebakende zone activiteiten te **monitoren of te detecteren, via passieve of actieve technieken**. Deze installaties zijn **stationair** en beschikken niet over autonome responsmogelijkheden.
Voorbeelden:

- Subsea Surveillance Systems: Permanente of semi-permanente systemen die op de zeebodem of in de waterkolom worden ingezet om onderwaterobjecten of -activiteiten te detecteren, volgen en classificeren. Ze maken gebruik van actieve en passieve sonar, distributed acoustic sensing (DAS), magnetische anomaliedetectoren ...
  Toepassing: bewaken van kritieke onderzeese infrastructuur, detectie van onderwaterdreigingen (zoals duikers of onbemande onderwaterdrones).
- Surface & Air Surveillance Systems: Vaste systemen die op land, offshore installaties of platformen geplaatst worden om oppervlakteschepen en andere objecten te monitoren. Ze gebruiken technologieën zoals kust- en offshore radars, vaste camera's (incl. 360°), satellietmonitoring, drone-detectiesensoren en AIS-gebaseerde systemen.
  Toepassing: detecteren en volgen van vaartuigen en objecten op en boven het water, visuele monitoring, en versterken van situational awareness rond strategische infrastructuur.

Drones

Mobiele robotsystemen die **autonoom** of **semi-autonoom** opereren in lucht-, zee-, onderwateromgevingen. Ze verzamelen gegevens, voeren monitoring uit of vervullen specifieke taken op locatie. **Mobiliteit** is hierbij de kernfunctie, in tegenstelling tot vaste installaties.
Voorbeelden:

- Unmanned Aerial Vehicles (UAVs): Op afstand of autonoom bestuurde vliegsystemen die opereren zonder piloot aan boord. (onder verschillende vormen: fixed-wing -lange afstand en grote payloads, rotary-wing (VTOL en precisie, …)
  Toepassing: inlichtingen en verkenning (ISR), luchtbewaking, maritieme patrouilles, militaire operaties…
- Unmanned Surface Vehicles (USVs): Autonome of semi-autonome vaartuigen die aan of nabij het zeeoppervlak opereren zonder bemanning aan boord. Ze maken gebruik van geavanceerde navigatie, sensoren, communicatiesystemen en efficiënte voortstuwing.
  Toepassing: inlichtingenvergaring, mijnendetectie en -ruiming, anti-onderzeebootoperaties, bevoorrading, directe inzet en datatransmissie.
- Autonomous Underwater Vehicles (AUVs): Onbemande onderwaterrobots die zelfstandig missies uitvoeren. Ze zijn uitgerust met navigatiesystemen, sonar, optische camera's en sensoren, en vereisen vaak complexe communicatieoplossingen.
  Toepassing: inspectie van onderzeese infrastructuur, detectie en neutralisatie van dreigingen, onderwaterzoekacties.

Geautomatiseerde systemen en robotics

Autonome of semi-autonome fysieke systemen die ingebouwd zijn in infrastructuren of eraan gekoppeld zijn. Ze voeren **vooraf ingestelde of AI-gestuurde acties** uit als reactie op externe stimuli.
Voorbeelden:

- Onboard Control & Operational Systems: Geautomatiseerde systemen die in schepen of vaste maritieme installaties geïntegreerd zijn om kernoperaties te beheren en te optimaliseren. Dit omvat o.a. automatische piloten, dynamische positioneringssystemen, geïntegreerde brugfuncties...
  Toepassing: verhogen van efficiëntie, veiligheid en prestaties; verminderen van menselijke tussenkomst; optimaliseren van operationele betrouwbaarheid.

- Integrated Safety & Security Systems: Automatiseringssystemen die ontworpen zijn om veiligheidsrisico's en beveiligingsinbreuken binnen maritieme infrastructuren te monitoren, detecteren en daarop te reageren. Voorbeelden zijn detectie, toegangscontrole, noodrespons en screeningtechnologieën.
  Toepassing: voorzien in real-time waarschuwingen en geautomatiseerde tegenmaatregelen; versterken van fysieke veiligheid en bescherming tegen dreigingen.

Communicatiesystemen

Technologieën die zorgen voor de **overdracht, routering en integriteit van data, commando's of alarmen** tussen fysieke en digitale componenten.
Voorbeelden:

- Operational Technology (OT) Networks: Netwerken en systemen die de fysieke processen en apparaten binnen maritieme operaties aansturen. Ze omvatten o.a. SCADA-systemen, voortstuwing en machineriebeheer, navigatiesystemen (GPS, ECDIS, radar), brugsystemen en veiligheidsnetwerken zoals HVAC en branddetectie.
  Toepassing: directe controle van scheeps- en havenoperaties, essentieel voor cyber-fysieke veiligheid en operationele continuïteit.
- Information Technology (IT) Networks: Netwerken en systemen gericht op dataverwerking, informatiebeheer en administratieve functies. Denk hierbij aan cargo- en milieubeheersystemen, toegangs- en screeningsoplossingen, bemannings- en welzijnstoepassingen en shore-to-ship data exchange.
  Toepassing: ondersteunt administratieve, logistieke en operationele processen, en faciliteert veilige data-uitwisseling tussen systemen.
- External Communication Systems: Infrastructuren en protocollen die communicatie mogelijk maken tussen maritieme assets en externe entiteiten. Hierbij gaat het om satellietcommunicatie (Satcom), maritieme radiolinks (GMDSS), 5G-nodes, onderzeese kabelrepeaters, AIS en GNSS/GPS.
  Toepassing: waarborgt dataoverdracht, commandotransmissie en verspreiding van waarschuwingen over het volledige maritieme domein.

Data-analytics en artificiële intelligentie

Software en systemen die verzamelde data **analyseren** en **interpreteren**, en **voorspellingen** maken – zoals patroonherkenning, dreigingsclassificatie, gedragsmodellering en operationele optimalisatie.
Voorbeelden:

- Threat Detection & Anomaly Identification: AI- en machine learning-modellen identificeren afwijkingen, verdachte patronen of ongeautoriseerde activiteiten in maritieme data. Ze maken gebruik van technieken zoals machine learning, deep learning en reinforcement learning.
  Toepassing: real-time detectie van indringers, navigatie-anomalieën, ongeautoriseerde toegang en onregelmatige datatransmissies.
- Predictive Analytics & Risk Assessment: AI-gestuurde systemen analyseren data om dreigingen of operationele problemen vroegtijdig te voorspellen en risico's in kaart te brengen. Hierbij worden onder meer deep learning, NLP en grafengebaseerde AI ingezet.
  Toepassing: voorspellend onderhoud, maritieme dreigingsanalyse, cyberrisico-inschatting voor autonome vaartuigen en forecasting van cyberaanvallen.
- Data Integration & Situational Awareness: Geavanceerde AI/ML-platformen combineren data uit uiteenlopende bronnen tot een uniform beeld dat gebruikt kan worden voor situational awareness en besluitvorming. Technieken zoals federated learning en blockchain-enhanced AI versterken de veiligheid en betrouwbaarheid van de data.

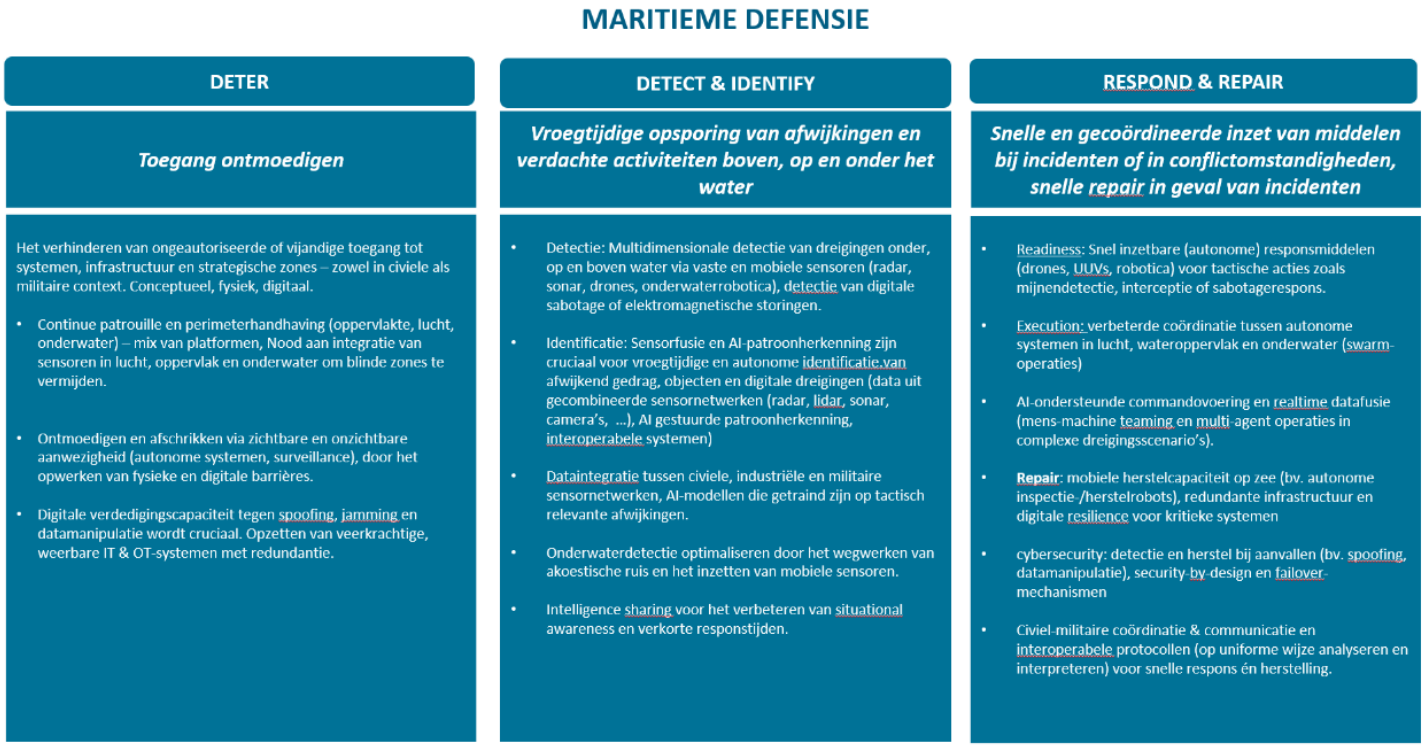
Toepassing: synthese van multisource-data, beveiligde data-uitwisseling, privacybeschermde analyses en verbeterd overzicht van het maritieme domein.

Maritieme defensie oriëntatie roadmap

Maritieme defensie wordt in dit kader benaderd aan de hand van het **DDIRR-principe**: Deter, Detect, Identify, Respond & Repair. Dit model biedt een strategische structuur om een breed scala aan dreigingen te beheersen in het maritiem domein – gaande van cyberaanvallen tot onderwaterinfiltraties, mijnenleggers, sabotageacties of conventionele militaire dreigingen.

Dit principe is van toepassing op zowel **civiel-militaire infrastructuur** (zoals havens, windparken en datakabels) als op **militaire operaties** (zoals naval defence en mine countermeasures).

De integratie van een herstelcomponent ('Repair') is cruciaal voor duurzame veerkracht in een zeer dynamische omgeving



Deter– Vijandelijke aanwezigheid en acties ontmoedigen en verhinderen

Deter richt zich op het **ontmoedigen** van toegang tot maritieme zones of systemen, door het opwerpen van zowel conceptuele, fysieke als digitale barrières. Denk aan **permanente aanwezigheid** via onbemande patrouillesystemen, detectienetwerken die onderwaterzones beveiligen, en aan digitale infrastructuur die bestand is tegen sabotage of penetratie. Zowel het inzetten van zichtbare capaciteiten als **cyberweerbaarheid** zijn hier belangrijk. Deter houdt ook in dat je aangeeft over de **capaciteit** en de **wil** te beschikken om tegenacties te ondernemen indien onze belangen zouden geschaad worden.

Capability gaps & noden:

- **Permanente situational awareness:** de continue monitoring van maritieme zones via onderwater- en oppervlaktepatrouilles, onbemande vaartuigen (USV's, AUV's) en geïntegreerde sensornetwerken. Vlaamse bedrijven en kennisinstellingen ontwikkelen technologieën voor real-time detectie, identificatie en dreigingsanalyse die rechtstreeks inzetbaar zijn binnen militaire operaties of als onderdeel van collectieve defensie.
- **Bescherming en versterking van maritieme infrastructuur:** ontwikkeling van detectie- en beschermingssystemen voor onderzeese kabels, energieverbindingen, pijpleidingen en havennetwerken. Hierbij spelen Vlaamse spelers in op defensiebehoeften aan **subsea surveillance systems, intrusion detection, digitale barrièretechnologieën** en **autonome inspectiesystemen**.
- **Digitale en cyberweerbaarheid:** versterking van maritieme OT- en IT-systemen tegen sabotage en cyberpenetratie, door inzet van **AI-gestuurde dreigingsdetectie, beveiligde communicatie, en resilient data-infrastructuren**. Deze technologieën hebben zowel civiele als militaire relevantie en zijn onmisbaar voor de beveiliging van command-and-control-systemen.

De industriële toepassingen binnen deze pijlers sluiten rechtstreeks aan bij concrete defensieve capaciteiten. Ze versterken onder meer het vermogen tot maritieme inlichtingen- en verkenningsoperaties (Intelligence, Surveillance and Reconnaissance – ISR), de bescherming van NAVO- en EU-ondersteunende infrastructuren, en de onderwaterdomeinbewaking en -afscherming (Underwater Domain Protection).

Detect & Identify – Dreigingen onder, op en boven water vroegtijdig herkennen

Deze fase concentreert zich op het **detecteren** én **identificeren** van afwijkende bewegingen, gedrag of objecten die kunnen wijzen op een dreiging. Dat kunnen mijnen zijn, onbemande (vijandelijke) vaartuigen, cyberattacks of verdachte patronen in scheepsvaartbewegingen.

Identificatie vereist sensorfusie, AI-gestuurde patroonherkenning en interoperabele systemen die kunnen opereren in **drie dimensies**: boven, op en onder het water.

Capability gaps & noden:

- Onvoldoende data integratie tussen civiele/industriële, militaire sensornetwerken.
- AI-systemen zijn nog niet getraind genoeg voor automatische identificatie van tactisch relevante doelen in deze complexe maritieme omgeving.
- Onderwaterdetectie wordt beperkt door akoestische beperkingen en een gebrek aan mobiele sensoren.
- Detectie van digitale sabotage of elektromagnetische storingen moet verder ontwikkeld worden.

Respond – Gecoördineerde respons op gedetecteerde dreiging of vijandelijke actie

De responsfase draait om **snelle** inzet van middelen na detectie. Denk aan het neutraliseren van mijnen, het onderscheppen van vijandige UUV's, of het veiligstellen van beschadigde installaties. In een hybride context omvat dit ook civiel-militaire coördinatie en het herstellen van controle over systemen na cyberaanval.

Capability gaps & noden:

- Te weinig respons capaciteit die flexibel inzetbaar is.
- Beperkte swarm-coördinatie tussen autonome platforms onder, op en boven water.
- Real-time communicatie is kwetsbaar in jamming-omgevingen of bij verlies van satellietnavigatie-informatie.
- Besluitvormingstools zijn onvoldoende afgestemd op multi-agent-operaties in complexe dreigingsscenario's.

Repair – Herstel van systemen, infrastructuur en operationele capaciteit

Repair is een kritische component binnen maritieme defensie: na een aanval, explosie, storing of sabotage moeten systemen, infrastructuur en netwerken snel worden **hersteld** om operationeel te blijven of opnieuw inzetbaar te worden. Dit betreft niet alleen **fysiek** herstel (bv. schade aan schepen, kabels, boeien, platformen, maar ook functioneel herstel van **digitale** systemen en sensornetwerken.

Capability gaps & noden:

- Er is een gebrek aan mobiele herstelcapaciteit op zee: autonome of robot systemen die lokaal schade kunnen beoordelen en beperken.
- Onderwaterinfrastructuur (bv. kabels, sensoren) is moeilijk bereikbaar en traag te herstellen zonder geavanceerde UUV's en interventierobots.
- Digitale systemen zijn vaak niet ontworpen op resilience: er is nood aan redundantie, automatische isolatie en alternatieve-systemen bij bijvoorbeeld cyberintrusies of inbraak op digitale systemen.

Innovatie kansen

Fixed Surveillance

Binnen vaste surveillancesystemen liggen de innovatiekansen in multimodale detectie waarbij bijvoorbeeld radarinstallaties op zee, slimme boeien aan het wateroppervlak en sonarvelden onder water gezamenlijk opereren als één sensorisch ecosysteem. AI-gestuurde patroonherkenning kan deze systemen in staat stellen om afwijkingen vroegtijdig te signaleren, of die nu afkomstig zijn van verdachte vaartuigen aan de oppervlakte, lage-vliegende objecten in de lucht of onderwateractiviteit zoals duikers of UUV's. Door sensorfusion en digital twins kunnen alle gegevens uit deze drie lagen – bijvoorbeeld door visuele camera's op schepen, hydrofoons op de zeebodem en luchtverkeersmonitoring via UAV's – worden geïntegreerd in een real-time situatiebeeld, waarmee niet alleen actuele dreigingen worden gesignaleerd, maar ook voorspellingen kunnen worden gedaan over potentiële incidenten of schade. Dit maakt het mogelijk om zowel civiele infrastructuur zoals windparken te beschermen als vijandelijke activiteiten onder water vroegtijdig te detecteren in een militaire context.

Innovatiekansen:

- Combinatie van verschillende monitoringssystemen:
  - Lucht: radarinstallaties, luchtcamera's, luchtverkeersmonitoring, …
  - Oppervlak: maritieme radars, visuele camera's, slimme boeien, …
  - Onder water: sonarvelden, hydrofoons, zeebodemsensoren, …
- Multimodale detectie met AI-gestuurde patroonherkenning en automatische anomaliedetectie.
- Sensorfusie en digital twins voor realtime situational awareness, inclusief voorspelling van dreigingen en schade.
- Bescherming van zowel kritieke infrastructuur (windparken, datakabels, terminals) als inzet in oorlogsvoering (vroege detectie van vijandelijke onderwateractiviteit, mijnendetectie).

Drones en autonome vaartuigen (UAVs, USVs, UUVs)

Autonome vaartuigen en drones vormen een nieuwe generatie inzetmiddelen die het maritieme domein in drie dimensies kunnen bestrijken: door de lucht (UAVs), op het water (USVs) en onder water (UUVs). Deze platforms opereren zelfstandig en zijn gericht op het uitvoeren van verkennings-, bewakings- en responsmissies, vaak zonder directe menselijke tussenkomst. De meerwaarde van deze systemen zit in hun mobiliteit, flexibiliteit en de mogelijkheid tot gecombineerde inzet, waarbij verschillende platformen gecoördineerd samenwerken in zogenaamde 'swarm operations'. Zo kan een UAV een gebied vanuit de lucht monitoren, terwijl een USV het wateroppervlak bewaakt en een UUV simultaan onderzeese inspecties uitvoert of mijnen opspoort.

De nadruk binnen dit domein ligt op de ontwikkeling van systemen die met behulp van artificiële intelligentie hun missie kunnen plannen, kunnen reageren op veranderende omstandigheden en met andere vaartuigen kunnen samenwerken. Cruciaal daarbij is de betrouwbaarheid van hun navigatie- en communicatiesystemen, zeker in omgevingen waar GPS-verstoring of elektronische tegenmaatregelen (zoals spoofing of jamming) kunnen voorkomen. Door redundante technologieën, zoals visuele herkenning gecombineerd met magnetische of inertiële referenties, kunnen deze autonome systemen blijven functioneren.

Autonome vaartuigen en drones zijn bij uitstek geschikt voor taken waarbij bereik, snelheid en coördinatie van groot belang zijn. Ze bieden *situational awareness* in complexe of hybride dreigingsscenario's, en kunnen snel reageren op gebeurtenissen. Binnen een maritieme verdedigingsstrategie vormen ze zo een flexibele, inzetbare laag die dreigingen vroegtijdig kan detecteren en desnoods autonoom kan neutraliseren.
Deze systemen zijn ook van strategisch belang voor mine countermeasures, waarbij UUV's ingezet worden voor het detecteren, classificeren en neutraliseren van zeemijnen in complexe operationele omgevingen.

Drie-dimensionaal inzetbaar:

- UAVs: boven water – verkenning, patrouille, inspectie, logistiek
- USVs: op water – perimeterbewaking, mijnendetectie, responsplatform
- UUVs: onder water – inspectie, mijnenbestrijding, verkenning en combat support

Innovatiekansen:

- Volledig autonome systemen: Vaartuigen en drones die dankzij AI zelf missieplanning, navigatie en adaptieve respons uitvoeren, zonder continue menselijke tussenkomst.
- Geïntegreerd maritiem dreigingsbeeld: Multi-platform sensorinput (lucht, wateroppervlak, onderwater) samenbrengen in één beslissingsmodel voor een coherent beeld.
- Cyber- en signaalresistentie: Bescherming tegen spoofing en jamming via redundante methodes (visueel, inertieel, magnetisch).
- Autonome samenwerking (swarming): Coördinatie en gezamenlijke acties van meerdere onbemande systemen boven, naast en onder water.
- Dual-use sensortechnologie: Vlaamse expertise in miniaturisatie en sensorfusion die inzetbaar is in zowel civiele toepassingen (bv. inspectiedrones) als maritieme defensie (UUVs).
- Manned-Unmanned Teaming: Integratie van bemande platforms (bv. fregatten) met USVs en UUVs voor gecombineerde maritieme operaties.
- Duurzame energie en aandrijving: Innovaties in batterij- en brandstofceltechnologie voor langere missieduur en grotere operationele autonomie.

Geautomatiseerde systemen & robotica

Geautomatiseerde systemen en robotica richten zich op het versterken van maritieme beveiliging en defensie door automatisering van detectie-, bewakings- en responsprocessen binnen en rond infrastructuur. Deze systemen werken continu of stand-by en treden automatisch in werking bij verdachte activiteit of sabotagepogingen.

De kern van dit domein ligt in de integratie van sensoren, beslissingslogica en communicatie in één geheel, waardoor menselijke tussenkomst geminimaliseerd wordt en reactiesnelheid sterk toeneemt. Geautomatiseerde systemen kunnen perimeterbewaking uitvoeren, verdachte bewegingen detecteren en een eerste respons opstarten. Ze zijn ontworpen om incidenten snel te isoleren en informatie real-time door te sturen naar hogere niveaus van commandovoering.

Specifiek voor onderwaterrobotica biedt dit domein de mogelijkheid om risicovolle, precieze taken uit te voeren op moeilijk bereikbare of vijandige locaties. Denk aan het inspecteren en identificeren van verdachte objecten onder water, of het neutraliseren van explosieven en mijnen op een gecontroleerde, veilige manier. Deze robotica is bij uitstek geschikt voor omgevingen waar manuele inzet te traag of te gevaarlijk zou zijn.

Naast detectie en respons kunnen dergelijke systemen ook ingezet worden voor post-incident repair en stabilisatietaken, zoals het herstellen van beschadigde sensoren, infrastructuur of communicatieverbindingen in moeilijk bereikbare zones.

Innovatiekansen:

- Geautomatiseerde responsmechanismen geïntegreerd in maritieme infrastructuur
- Onderwaterrobotica voor precisietaken zoals inspectie & detectie van vijandelijke objecten en gerichte neutralisatie van explosieven of mijnen in gecontroleerde operaties.
- Inzet van robotica in vijandige of onvoorspelbare omgevingen, waar manuele interventie te riskant is.

Communicatiesystemen en connectiviteit

Voor een goede maritieme beveiliging is het belangrijk dat alle systemen – in de lucht, op het water en onder water – veilig en betrouwbaar met elkaar kunnen communiceren. Ook het connecteren (bv. door het gebruik van dezelfde protocollen en op een uniforme wijze gegevens kunnen analyseren en interpreteren) is hier belangrijk. Drones in de lucht (UAV's) kunnen bijvoorbeeld tijdelijk dienen als doorgeefpunt, zodat informatie via een draadloos netwerk of satelliet direct wordt doorgestuurd naar een controlecentrum. Op het water kan 5G zorgen dat schepen en infrastructuur met elkaar in contact blijven. Onder water kunnen onderwaterdrones (UUV's) en vaste sensoren akoestische of optische signalen gebruiken om gegevens uit te wisselen.

Het is belangrijk in te zetten op redundante en storingsbestendige netwerken, die blijven werken bij pogingen tot spoofing en jamming. Ook zijn veilige koppelingen tussen systemen belangrijk, zodat bijvoorbeeld een UAV die een verdachte situatie waarneemt, die informatie direct kan doorsturen naar een onderwaterdrone die zich voorbereidt op actie. Er wordt ingezet op een vloeiend en beveiligd gegevensnetwerk, waarin alle systemen naadloos samenwerken – ongeacht waar ze zich bevinden.

Een bijkomende uitdaging is het ontwikkelen en toepassen van interoperabele protocollen en gemeenschappelijke standaarden. Alleen wanneer systemen dezelfde taal spreken, kan informatie uit verschillende netwerken en sensoren op een uniforme en betrouwbare manier worden weergegeven en geïnterpreteerd. Dit vergemakkelijkt niet alleen samenwerking maar verhoogt ook de efficiëntie en snelheid van besluitvorming.

Innovatiekansen:

- Nood aan veilige en interoperabele communicatie in 3 dimensies:
  - Lucht/oppervlak: robuuste, redundante netwerken (zoals 5G offshore, mesh-netwerken en satellietverbindingen) voor continue verbinding tussen drones, schepen en infrastructuur.
  - Onderwater: akoestische, optische of elektromagnetische communicatie met UUV's en vaste sensoren voor betrouwbare datadoorgifte in GPS-loze omgevingen.
  - Spoofing- en jamming-resistente communicatiesystemen die autonoom kunnen schakelen tussen verbindingstypes bij storing of vijandelijke verstoring.
  - Beveiligde interoperabiliteit tussen maritieme platforms, drones, sensornetwerken en controlecentra over alle dimensies heen.
  - Real-time datadeling tussen onbemande systemen en commandovoering, voor gecoördineerde acties bij detectie, verkenning en respons.
  - Ontwikkeling en toepassing van gemeenschappelijke standaarden en protocollen, zodat data uit uiteenlopende netwerken en sensoren op een uniforme en betrouwbare manier kan worden geïntegreerd en benut.

Data-analyse & artificiële intelligentie (AI)

AI-technologieën zijn essentieel om informatie uit verschillende bronnen – zoals luchtbeelden, radar, sonar en onderwatersensoren – snel te verwerken tot een samenhangend beeld van de situatie. Door deze grote hoeveelheden van data slim te combineren, kan AI afwijkende patronen herkennen die anders onopgemerkt zouden blijven. Denk aan het opmerken van ongebruikelijke bewegingen onder water kort nadat een verdachte drone in de buurt is geland.

Met behulp van predictieve algoritmes kan AI bovendien trends identificeren, zoals herhaalde vaarroutes rond gevoelige infrastructuur of subtiele veranderingen in onderwaterakoestiek die kunnen wijzen op mijnenplaatsing of sabotage.

AI ondersteunt operationele besluitvorming door gerichte analyses en aanbevelingen te geven, maar laat de uiteindelijke actie over aan menselijke of vooraf gedefinieerde commandolijnen.

Innovatiekansen:

- AI-gestuurde detectie van cyberdreigingen en afwijkend gedrag in maritieme netwerken, op basis van continue monitoring.
- Geavanceerde datafusie uit lucht-, zee- en onderwatersensoren voor een coherent, realtime situatiebeeld.
- AI-ondersteuning bij besluitvorming, waarbij systemen aanbevelingen doen op basis van patroonherkenning en risicobeoordeling – zonder autonoom in te grijpen.
- Predictieve AI-modellen die trends analyseren en en kunnen wijzen op risico's en incidenten.

Cyberbeveiliging

Moderne maritieme operaties zijn steeds sterker afhankelijk van digitale systemen voor navigatie, communicatie, detectie en coördinatie. Deze digitalisering vergroot de kwetsbaarheid voor cyberaanvallen die gericht zijn op het verstoren van datastromen, het overnemen van systemen of het manipuleren van sensorgegevens. Vooral autonome vaartuigen en verbonden infrastructuur lopen risico's bij verstoring of misleiding van hun software, verbindingen of besluitvormingsprocessen. Cyberbeveiliging is daarom een kernvoorwaarde geworden voor de veilige inzet van maritieme technologieën.
Daarbij is het essentieel om in te zetten op digitale redundantie en failover-architecturen die kritieke functies automatisch kunnen overnemen bij verstoring of manipulatie, zodat systemen operationeel blijven tijdens en na een aanval.

- Beveiliging van verbonden sensoren, drones en infrastructuur tegen manipulatie, sabotage of datalekken.
- Bescherming van kritieke systemen tegen cyberaanvallen die zich richten op communicatie, navigatie of besluitvorming.
- Detectie van digitale inbreuken in realtime, zowel aan boord van vaartuigen als in controlecentra.

Cyberveiligheid vormt een integraal onderdeel van maritieme beveiliging. Kritieke maritieme infrastructuren — havens, windparken, datakabels en schepen — zijn in toenemende mate digitale ecosystemen. De roadmap *Cyberveiligheid voor Defensie* benadrukt hoe cyberaanvallen en hybride oorlogsvoering directe impact hebben op zowel militaire operaties als civiele infrastructuur. Deze maritieme roadmap sluit daar naadloos bij aan: waar de cyberroadmap focust op generieke OT- en IT-beveiliging, vertaalt deze maritieme roadmap dat kader naar concrete toepassingen in het

Noordzeegebied en de Vlaamse havens. Meer concreet, het beschermen van het maritieme domein, zowel vanuit een civiel als dual-use perspectief, sluit nauw aan bij de pijlers FORTIFY (security-by-design) en SHIELD (operational security) van de roadmap Cyberveiligheid voor Defensie. Aanvullend focust de cybersecurity pijler CONTROL op specifieke cybersecurity technologie ter ondersteuning van cyberdefense operaties inclusief maritieme operaties.

Innovatiekansen:

- AI-gestuurde dreigingsdetectie: Automatische identificatie van cyberaanvallen via anomaliedetectie in netwerktrafiek en datastromen.
- Cybercontrol in commandostructuren: Integratie van cyberwaarschuwingen en automatische isolatie van aangetaste componenten binnen maritieme C2-processen.
- Cyber resilience van systemen: Verhoogde weerbaarheid van zowel autonome platformen als maritieme OT/IT tegen sabotage, spoofing en malware.
- Interoperabele beveiligingsarchitecturen: End-to-end bescherming van communicatie tussen drones, infrastructuur en commandocentra.
- Secure-by-design technologie: Ingebouwde hardware- en softwarebeveiliging vanaf de conceptfase bij drones, sensoren en platformen.
- Quantumveilige communicatie: Toepassing van post-quantum cryptografie in satelliet- en offshore netwerken.
- Threat intelligence sharing: Maritieme SOC's en havens als proeftuinen voor actieve informatie-uitwisseling over dreigingen.
- Digital twin security: Integratie van cybersecurity in maritieme digital twins om scenario's en risico's veilig te simuleren.

Samenwerking

Samenwerking tussen stakeholders is een essentiële pijler in de verdere uitbouw van het Vlaamse maritieme defensie-industrie. Gezien de grensoverschrijdende aard van de maritieme sector, vooral met betrekking tot offshore installaties en havens, is het van cruciaal belang om samenwerking te bevorderen tussen publieke en private actoren, internationale partners en maritieme veiligheidsexperts.

Deze samenwerking moet gericht zijn op het bevorderen van technologie-integratie, het verbeteren van coördinatie en het waarborgen van open data-uitwisseling. Hierdoor kunnen systemen naadloos op elkaar worden afgestemd, kunnen dreigingen sneller worden gedeeld, en kunnen responsoperaties effectiever worden uitgevoerd. Internationale samenwerking is ook essentieel voor het opzetten van gezamenlijke patrouilles en gemeenschappelijke noodresponsstrategieën.

CONCLUSIE

De Vlaamse Noordzee en havens groeien uit tot strategische knooppunten op het kruispunt van energievoorziening, digitale infrastructuur en internationale logistiek. Tegelijk neemt hun kwetsbaarheid toe in een context van toenemende geopolitieke spanningen en hybride dreigingen. Deze realiteit onderstreept de noodzaak van een structurele en toekomstgerichte aanpak van maritieme veiligheid en defensie.

Met het Impulsprogramma Veiligheid en Defensie zet de Vlaamse overheid een belangrijke stap naar de uitbouw van een robuuste, innovatieve en internationaal verankerde technologische en industriële defensiebasis.

Dit programma richt zich niet uitsluitend op de bescherming van kritieke maritieme infrastructuur zoals windparken, datakabels en havens, maar omvat ook bredere defensietoepassingen zoals naval combat, onderwaterverdediging en mine countermeasures (MCM) – domeinen waarin Vlaanderen reeds een erkende voortrekkersrol vervult.

De roadmap die hieruit voortvloeit biedt bedrijven, kennisinstellingen en overheden een concreet en geïntegreerd kader om gezamenlijk te werken rond sleuteltechnologieën zoals AI, autonome systemen, onderwaterrobotica, cybersecurity, sensorfusie en digitale besluitvorming. Door de combinatie van civiele en militaire toepassingen (dual-use innovatie) en door de versterking van publiek-private samenwerking ontstaat een dynamisch ecosysteem dat inspeelt op de strategische noden van vandaag én morgen.

Dit Impulsprogramma draagt bij aan de weerbaarheid van Vlaanderen en België, bevordert de Europese technologische autonomie, en versterkt onze rol als betrouwbare partner binnen NAVO en de Europese Unie. Deze maritieme roadmap vormt de basis waarop toekomstige projecten kunnen worden gebouwd – als hefboom voor innovatie, veiligheid en economische groei

Impulsprogramma Veiligheid & Defensie

Oriëntatieroadmap

Luchtvaart & Drones

Document opgesteld door Agoria-FLAG – Flemish Aerospace Group,
de cluster van de Vlaamse Luchtvaartindustrie, op vraag van WEWIS

Oktober 2025

Inhoudsopgave:

1 Inleiding

De snelle vooruitgang op gebied van luchtvaarttechnologie en onbemande- en autonome luchtvaarttechnologie in het bijzonder schept een continue uitdaging voor zowel de luchtvaartindustrie als het luchtruimbeheer (ATM – Air Traffic Management, UTM – Unmanned Traffic Management en C-UAS). Onbemande platformen – ook wel drones genoemd - veranderen niet alleen fundamenteel de manier waarop het luchtruim wordt benut, maar openen ook nieuwe economische kansen en toepassingen binnen zowel civiele als defensie gerelateerde sectoren.

Naarmate onbemande systemen steeds autonomer, performanter en beter geïntegreerd raken, groeit ook de complexiteit van het ecosysteem. Dit vraagt om heldere beleidsrichtlijnen, strategische samenwerking en een toekomstgerichte aanpak.

Daarbij dienen we steeds rekening te houden met het groeiende belang van een sterke, geïntegreerde Europese veiligheids- en defensie-industrie, zonder afbreuk te doen aan de nood tot samenwerking en coördinatie met de NAVO. We verwijzen hierbij naar de toespraak die Ursula von der Leyen – Voorzitter van de Europese Commissie - op 18 maart 2025 hield bij de Europese Commissie (in Kopenhagen), waarin zij de nadruk legde op de noodzaak voor Europa om lacunes in capaciteiten op te vullen en te investeren in defensietechnologieën zoals drones, kunstmatige intelligentie (AI), lucht- en raketverdediging : "*…we need to invest in air and missile defence, artillery systems, ammunition and missiles. And we have to learn the lessons from the battlefield … We have seen the importance of drones and counter-drone systems in Ukraine.* ***Europe needs to develop all types of unmanned systems and the advanced software and sensors behind them***."

Deze oriëntatie roadmap biedt een strategisch kader om de ontwikkeling van bemande en onbemande luchtvaarttechnologie in goede banen te leiden. Ze definieert technologische prioriteiten en noodzakelijke randvoorwaarden voor de uitbouw van een schaalbaar, veilig en veerkrachtig luchtvaart- en drone-ecosysteem in Vlaanderen. Door overheid, industrie en kennisinstellingen structureel met elkaar te verbinden - de gekende triple-helix - willen we innovatie versnellen, investeringen stimuleren en beleidsontwikkeling stroomlijnen.

Vlaanderen beschikt meerdere troeven om een voortrekkersrol op te nemen: een gunstige geografische ligging, sterke onderzoeks- en kennisinstellingen en een groeiend netwerk van technologiebedrijven. De weg vooruit vraagt gerichte actie: het opzetten van U-space-infrastructuur, het uitbouwen van testcapaciteit, het versterken van kritieke technologieën zoals AI, cyberveiligheid en autonome navigatie, en het verkleinen van de afhankelijkheid van niet-Europese componenten. Ook de relatie tussen industrie enerzijds en defensie en ordediensten anderzijds, dient verder uitgediept te worden.

Daarnaast zijn investeringen in start-ups, vaardigheden en arbeidsmarktontwikkeling essentieel om het technologische momentum vast te houden. Publiek vertrouwen en maatschappelijke draagkracht — ondersteund door transparant beleid en zichtbare toepassingen — zullen uiteindelijk bepalen of Vlaanderen en België hun positie kunnen versterken als sterkhouders in de Europese drone- en luchtvaartindustrie kunnen behouden.

2 Nieuwe ontwikkelingen en programma's

De oorlog in Oekraïne heeft het toepassingsgebied van drones ingrijpend verbreed en versneld. Waar drones vroeger vooral werden ingezet voor verkenning en observatie, tonen de gevechten in Oekraïne hoe veelzijdig deze technologie kan zijn. Drones worden nu gebruikt voor precisieaanvallen, logistieke ondersteuning, elektronische oorlogsvoering en zelfs als goedkope, snel inzetbare

wapensystemen. De conflictzone is daarmee een proeftuin geworden voor zowel militaire innovatie als tactische aanpassing, waardoor drones een onmisbaar onderdeel zijn geworden van moderne oorlogsvoering en strategische besluitvorming.

Naast de sterke uitbreiding van de toepassingsgebieden is ook de innovatiecyclus rond drones drastisch verkort: ontwerpen, testen en inzetten gebeurt vandaag binnen enkele weken in plaats van jaren. Hoewel verwacht wordt dat dit tempo in een post-oorlogsscenario enigszins zal afnemen, lijkt een terugkeer naar vroeger uitgesloten. Deze evolutie vormt een aanzienlijke uitdaging voor de traditioneel conservatieve luchtvaartindustrie, waar strikte test- en certificatieprocedures lange tijd het tempo van innovatie bepaalden. De snelle vooruitgang op het vlak van onbemande en autonome systemen brengt bovendien nieuwe vraagstukken met zich mee op het gebied van luchtvaartveiligheid, de integratie van deze systemen in het luchtruim, en civiele veiligheid in bredere zin.

Civiel-militaire integratie is een krachtige hefboom geworden, waarbij commerciële componenten, open-sourcesoftware en civiele industrieën snelle opschaling mogelijk maken. Ten slotte blijken drones operationeel zeer flexibel te zijn en worden ze ingezet voor uiteenlopende missies — van tactische inlichtingen-, surveillance- en verkennings (ISR) taken tot strategische diepe precisieslagen.

2.1 De ontwikkeling van 6de generatie gevechtsvliegtuigen

Momenteel worden wereldwijd verschillende programma's voor zesde generatie gevechtsvliegtuigen ontwikkeld, waaraan ook Europese landen actief deelnemen. Het Europese FCAS/NGWS-project (Future Combat Air System / Next Generation Weapon System [1]) richt zich op de ontwikkeling van een "*system of systems*" waarin bemande New Generation Fighters en onbemande Remote Carriers samenwerken binnen een geïntegreerde combat cloud. Daarnaast werkt het trilaterale Global Combat Air Programme (GCAP) [2] van het Verenigd Koninkrijk, Italië en Japan aan een vergelijkbare nieuwe generatie gevechtsvliegtuigen. Beide trajecten leggen de nadruk op de nauwe integratie van bemande en onbemande platforms, met gedeelde sensor-, effector- en command-&-controlcapaciteiten, die een hogere mate van interoperabiliteit en flexibiliteit mogelijk maken. Ook in Zweden werkt SAAB aan een 6de generatie opvolger voor de Gripen E/F. [3] In de Verenigde Staten loopt een parallel initiatief onder de naam NGAD (Next Generation Air Dominance)[4], dat eveneens inzet op een netwerkgerichte luchtgevechtsarchitectuur.

België neemt vandaag deel aan het NGWS/FCAS-programma met een observatorstatus[5], een positie die het land toelaat de technologische en industriële ontwikkelingen binnen het project van nabij op te volgen. Deze status vormt een strategische opstap naar volwaardige deelname aan het programma, naast de drie kernpartners Duitsland, Frankrijk en Spanje. Het uiteindelijke doel is om formeel toe te treden als partnerland, zodat Belgische industrie, kennisinstellingen en onderzoekscentra rechtstreeks kunnen bijdragen aan en profiteren van de ontwikkeling van dit zesde generatie luchtgevechtssysteem. Een volwaardige deelname zou niet alleen de Belgische defensie-industrie versterken, maar ook de technologische soevereiniteit van Europa ondersteunen en België positioneren als relevante speler binnen de toekomstige Europese luchtvaart- en defensie-ecosystemen.

---

[1] NGWS/FCAS : Future Combat Air System FCAS | Airbus
[2] GCAP BAE Systems : FCAS | Global Combat Air Programme | Air
[3] SAAB : While focusing on Gripen E, Saab is also looking at "What comes after next" - AGN
[4] NGAD : Next Generation Air Dominance Programme, US
[5] Observator status : Belgisch waarnemerschap in het NGWS/FCAS-programma | News.belgium

Met een verwachte operationele ingebruikname rond 2040–2045 staan deze programma's voor aanzienlijke politieke, financiële en technologische uitdagingen. Hun ontwikkeling vraagt om visionair leiderschap en een gezamenlijke inspanning om baanbrekende technologieën te realiseren op het vlak van geavanceerde sensoren, AI-ondersteunde besluitvorming, manned-unmanned teaming, stealth-capaciteiten, gerichte-energiewapens en hypersonische systemen.

De omvang en complexiteit van deze programma's onderstrepen het groeiende belang van internationale samenwerking en industriële partnerschappen om kosten te spreiden, kennis te bundelen en innovatie te versnellen. Voor de Vlaamse luchtvaartindustrie ligt hier een belangrijke uitdaging én kans: door actief bij te dragen aan de ontwikkeling van deze innovatieve, vaak disruptieve technologieën, kan Vlaanderen zich positioneren binnen de waardeketen van deze zesde generatie luchtvaartplatformen en zo een duurzame rol spelen in de toekomst van de Europese en mondiale defensie-industrie.

De Vlaamse luchtvaartindustrie erkent het strategische belang van deelname aan een Next-Generation Weapon System-programma (NGWS) en focust daarbij in het bijzonder op het NGWS/FCAS-programma, met actieve inspanningen om nauwere samenwerking aan te gaan met de verschillende primes en 'main partners'. Tegelijk blijft de sector realistisch over de huidige politieke uitdagingen en de complexe besluitvorming die dit programma kenmerken. Bijgevolg houdt de industrie bewust meerdere opties binnen handbereik, onder meer door zich te richten op alternatieve trajecten en technologieën die mogelijk sneller marktrijp zijn — zoals de ontwikkeling van Loyal Wingman-programma's. In dat kader ondersteunt de Vlaamse luchtvaart industrie actief de NGCAT-werkgroep, opgezet binnen de Agoria-structuren, evenals de DEFRA R&T-calls van het Koninklijk Hoger Instituut voor Defensie (KHID), die programma-agnostisch werken. Binnen deze initiatieven worden reeds meerdere projecten uitgevoerd of voorbereid, met als doel de Belgische positie te versterken binnen de toekomstige Europese en internationale waardeketens rond 6de generatie luchtgevecht platformen. .

2.2 Collaborative Combat Aircraft of Loyal Wingman

Zoals reeds aangegeven zijn 6de generatie gevechtsvliegtuig programma's opgebouwd rond een 'system-of-systems' [6] en 'combat-cloud' architectuur [7]. Essentieel binnen deze programma's zijn de "loyal wingman" of Collaborative Combat Aircraft. Dit zijn geavanceerde onbemande gevechtstoestellen die in samenwerking met bemande vliegtuigen kunnen opereren, en taken uitvoeren zoals elektronische oorlogvoering, luchtverdediging, decoy-operaties of doelgerichte aanvallen. Deze systemen vergroten het tactisch bereik van luchtmachtoperaties zonder extra risico voor menselijk personeel.

---

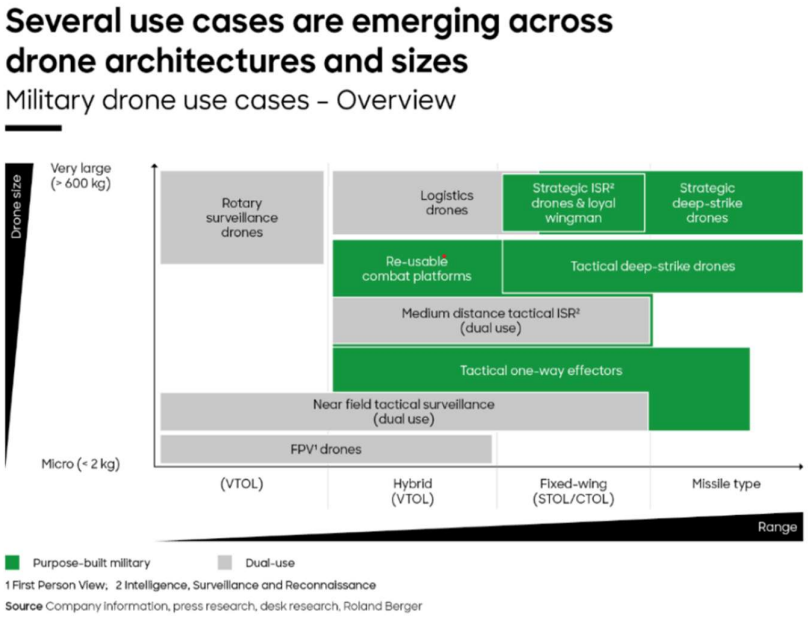
[6] Definitie System-of-Systems : Een System of Systems (SoS) kan worden omschreven als een verzameling van afzonderlijke deelsystemen die operationeel onafhankelijk zijn — elk systeem functioneert autonoom en vervult zijn eigen doelstelling. Hoewel deze systemen onafhankelijk worden beheerd en geografisch verspreid kunnen zijn, werken zij gezamenlijk samen om unieke functies uit te voeren die geen enkel individueel deelsysteem op zichzelf kan realiseren.

[7] Definitie combat-cloud: De Combat Cloud is een gedistribueerd gevechtsnetwerk dat bemande en onbemande platforms, sensoren en wapensystemen met elkaar verbindt — van het tactische tot het operationele niveau. Het systeem verzamelt en deelt uiteenlopende gegevens met minimale vertraging, om zo de "detecteer–beslis–handel"-cyclus aanzienlijk te versnellen.

De uitdagingen op het gebied van ontwikkeling en productie van deze loyal wingman-drones verlopen parallel aan die van bemande vliegtuigen. De inzet van deze nieuwe generatie 'Loyal Wingman' gaat echter gepaard met toenemende technologische en operationele complexiteit. Ze vereisen een hoge graad van digitalisering, sensorfusie, autonome besluitvorming en onderlinge communicatie. Deze onderlinge verwevenheid tussen platformen stelt zware eisen aan de command & control-architectuur (Manned – Unmanned Teaming, MUM-T), die tegelijk flexibel en schaalbaar moet zijn, maar ook robuust en fail-safe. Real-time coördinatie, prioriteitsbeheer, menselijke interventie en geautomatiseerde reacties moeten op een gecontroleerde manier samenkomen in één betrouwbaar systeem.

2.3 Schaalverbreding en -vergroting in defensie

Aan de andere kant van het spectrum ontstaan eveneens nieuwe rotary-wing en fixed-wing platformen en dit gaat gepaard met een duidelijke **schaalvergroting in het gebruik van drones**, zowel in kwantitatief als in kwalitatief opzicht. Waar onbemande luchtvaartuigen traditioneel vooral ingezet werden voor **ISR-opdrachten** (Intelligence, Surveillance & Reconnaissance), zien we nu een structurele verbreding richting **offensieve en tactische toepassingen**. Een belangrijk voorbeeld hiervan is het toenemend gebruik van '**loitering amunition**' - ook wel bekend als "kamikaze drones" - die kenmerken van drones en missielen combineren. Deze in staat zijn om zelfstandig boven of nabij het doelgebied te wachten en op het juiste moment een doelwit uit te schakelen.



Tekening 1: How military drones redefine defense in Europe, Roland Beger

In het huidige Defensie landschap wint het idee van een 'slimme, betaalbare massa' aan belang: in plaats van uitsluitend te investeren in dure, hoogtechnologische wapensystemen, zullen strijdkrachten in de toekomst vaker voor grote aantallen goedkope, flexibele en snel te produceren drones opteren. Dit hertekent de economische wetten van oorlogsvoering. Waar traditionele systemen vaak superieure prestaties bieden maar te kostbaar en langzaam te schalen zijn, vullen betaalbare drones die leemte door goede prestaties te leveren voor een fractie van de prijs en zo massale inzet mogelijk maken voor moderne afschrikking. Grote dronezwermen verhogen bovendien de effectiviteit van afschrikking — ze dwingen potentiële tegenstanders tot berekening — en dankzij modulaire payloads en software gestuurde architecturen kunnen ze snel van rol wisselen tussen verkenning, aanval en elektronische oorlogsvoering. Zo vormen ze de hoeveelheidscomponent die de kwaliteit van geavanceerde middelen zoals gevechtsvliegtuigen,

tanks en luchtverdediging versterkt, en dragen ze bij aan een meer gelaagde en veerkrachtige defensiestrategie. [8]

2.4 Verwachte toepassingen binnen defensie en civiel-militaire synergie

Hoewel drones van oorsprong sterk geassocieerd worden met militaire operaties, ontstaat er steeds meer overlap tussen civiele en militaire toepassingen, zeker op het vlak van 'situational awareness', perimeterbeveiliging en grensbewaking. In de toekomst zullen 'dual-use' drones — toestellen die zowel civiel als militair inzetbaar zijn — vaker ontwikkeld en ingezet worden. Denk bijvoorbeeld aan drones die in vredestijd gebruikt worden voor kritieke infrastructuurbewaking, en in crisistijd snel kunnen worden aangepast voor defensieve taken.

Op het vlak van territoriale en kritieke infrastructuurbescherming zal de samenwerking tussen civiele diensten, defensie en private actoren steeds intensiever worden. Drones zullen worden gebruikt voor patrouilles boven havens, luchthavens en energie-installaties, alsook voor het beveiligen van grootschalige evenementen. Dit vergt de ontwikkeling van modulaire drones met open architectuur en uitwisselbare payloads (camera's, sensoren, communicatieapparatuur), waardoor eenzelfde toestel flexibel kan worden ingezet voor uiteenlopende missies.

2.5 Drones als versterking van civiele veiligheid

Binnen het domein van civiele veiligheid zullen drones een steeds prominentere rol spelen. Politiediensten en hulpverleners gebruiken vandaag al drones voor verkeersmonitoring, menigtebeheer (crowd-control), ongeval-visualisatie en zoek- en reddingsoperaties. In de toekomst zal dit verder uitgebreid worden met real-time gegevensanalyse en live-beelden, gekoppeld aan centrale meldkamers. Drones zullen in staat zijn om zelfstandig ongeval locaties te benaderen, gevaar-situaties te analyseren en informatie door te sturen nog vóór de eerste interventieploegen ter plaatse zijn.

Er wordt ook gewerkt aan de inzet van drones met specifieke sensoren voor branddetectie in natuurgebieden, gaslekherkenning in stedelijke omgevingen, of het meten van luchtvervuiling in industrieclusters. Door integratie met smart city-platforms kunnen drones bovendien deel gaan uitmaken van permanente toezichtnetwerken, wat zal bijdragen aan snellere respons en betere coördinatie tussen hulpdiensten.

Voor deze toepassingen zal een combinatie van kleinere multi-rotor drones en grotere fixed-wing drones worden ingezet, elk afgestemd op specifieke operationele behoeften. Multi-rotor drones bieden de nodige wendbaarheid, stabiliteit en precisie voor operaties in stedelijke omgevingen of op moeilijk bereikbare locaties, zoals bij gebouwen, tunnels of rampgebieden. Ze zijn bij uitstek geschikt voor snelle respons, korte afstandsvluchten en real-time visuele ondersteuning.

Aanvullend worden fixed-wing drones gebruikt voor langere verkenningsvluchten, grensbewaking, bewaking van uitgestrekte natuur- of industriegebieden, en het uitvoeren van systematische patrouilles. Deze toestellen hebben een groter bereik, langere vliegtijd en kunnen zwaardere sensoren dragen. In de toekomst zullen beide platform types samenwerken binnen een geconnecteerd netwerk van lucht- en grondgebonden assets, waarin data centraal wordt verwerkt en gedeeld tussen meldkamers, commandocentra en interventieteams. Deze inter-operabele aanpak verhoogt de 'situational awareness' en verbetert de besluitvorming op alle niveaus van de veiligheidsketen.

[8] Artikel: Smart and affordable mass | Roland Berger

2.6 Naar een geïntegreerd ecosysteem

Zowel voor civiele veiligheid als voor defensie is het duidelijk dat de toekomst ligt in autonome, netwerk-gebaseerde drone-ecosystemen, waarbij toestellen met elkaar communiceren, zich coördineren via AI zelflerende algoritmes en geïntegreerd zijn in een overkoepelend 'command & control' systeem. Vlaanderen en België kunnen hierin een voortrekkersrol spelen.

De sleutel tot succes ligt in het ontwikkelen van een doordachte, gezamenlijke strategie die civiele innovatie en defensieve slagkracht met elkaar verbindt, inclusief de nodige aandacht voor ethiek, privacy en maatschappelijke acceptatie. Om het potentieel van deze schaalvergroting ten volle te benutten, zullen we niet alleen moeten investeren in technologie, maar ook in opleiding, doctrines, simulatiecapaciteit en interoperabiliteit met bondgenoten.

De rol van de industrie is cruciaal in het ontwikkelen van betrouwbare subsystemen, terwijl kennisinstellingen en testomgevingen de innovatiecapaciteit en veiligheidsgaranties mee moeten versterken. Kortom, de dronecapaciteit van morgen is niet alleen groter, maar ook slimmer, autonomer en meer verweven met alle domeinen van civiele veiligheid en moderne oorlogsvoering. **Artificiële Intelligentie** en **Cyberveiligheid** zijn niet langer randvoorwaarden, maar kerncomponenten. Aangezien deze drones vaak functioneren binnen een mesh-netwerk van sensoren, wapensystemen en dataverbindingen, zijn ze kwetsbaar voor vijandelijke inmenging, spoofing, jamming of digitale sabotage. Dit vraagt om ingebouwde redundantie, geëncrypteerde communicatie en actieve cyberdefensie op zowel hard- als softwarelaag. De controle over de digitale architectuur van deze systemen zal in de toekomst bepalend zijn voor operationeel succes en strategische autonomie. Een multidisciplinaire aanpak over de verschillende pijlers en technologie domeinen is cruciaal om deze uitdagingen het hoofd te bieden.

3 Het Vlaamse ecosysteem

3.1 Inleiding

Het Vlaamse luchtvaart- en drone-ecosysteem is een dynamisch en sterk gespecialiseerd netwerk van bedrijven en kennisinstellingen dat zich kenmerkt door een hoog technologisch niveau en een sterke focus op kwaliteit en techniciteit.

Vlaanderen telt een dicht KMO-landschap waarin talrijke innovatieve spelers actief zijn in uiteenlopende domeinen van de luchtvaart sector. De Vlaamse luchtvaartindustrie, opgebouwd rond enkele sterke internationale spelers met daaromheen een netwerk van kleine en middelgrote ondernemingen, is van nature sterk internationaal georiënteerd. Aangezien Vlaanderen (en België) geen grote OEM's (Original Equipment Manufacturers) telt, zijn onze bedrijven aangewezen op integratie binnen de uiterst competitieve internationale waardeketens van deze OEM's en hun diverse platformen. Dit heeft geleid tot een hoog competitieve industrie, die naast een sterke focus op onderzoek en ontwikkeling (O&O) ook uitblinkt in kostenefficiëntie, een modern productieapparaat en geoptimaliseerde productieprocessen.

Dankzij haar gespecialiseerde kennis en ervaring heeft de Vlaamse luchtvaart- en drone-industrie de voorbije jaren een stevige positie verworven binnen diverse internationale waardeketens. Ze neemt actief deel aan een reeks toonaangevende programma's, waaronder de F-16, A400M, F-35 en MQ-9B SkyGuardian.

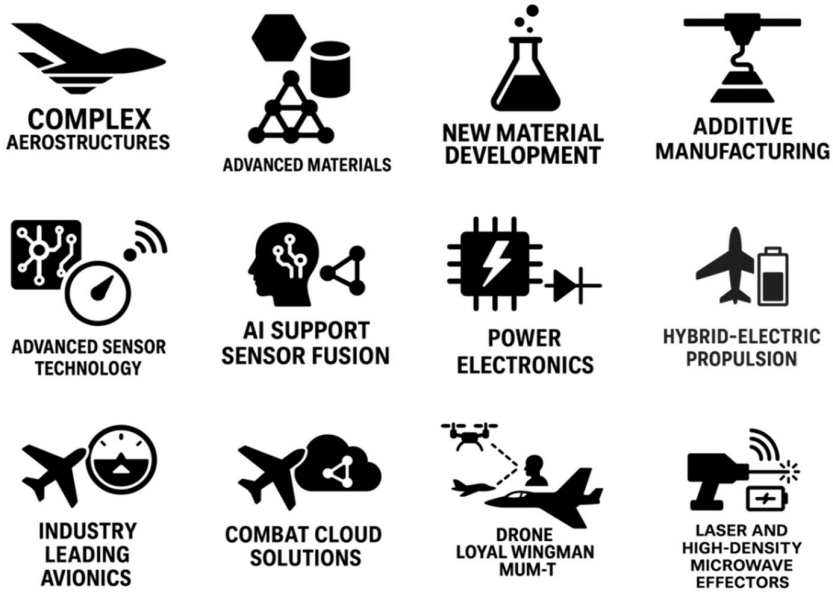
Wat het ecosysteem bijzonder maakt, is de complementariteit van de betrokken technologieaanbieders en de talrijke kennis- en onderzoeksinstellingen. Vlaanderen herbergt bedrijven die actief zijn in cruciale componenten, van structuurelementen en aandrijfsystemen tot digitalisatie, communicatietechnologie, navigatieoplossingen en geavanceerde sensoren. Deze diversiteit aan expertises vormt een sterke technologische basis waarop de competitieve luchtvaart- en drone-industrie kan steunen.

3.2 Vlaamse sterktes

Vlaamse innovatie richt zich niet enkel op het optimaliseren van bestaande systemen, maar ook op het verkennen van grensverleggende technologieën die zowel civiele inzetbaarheid en militaire capaciteiten fundamenteel kunnen transformeren.

Een van de speerpunten binnen deze technologische vooruitgang is **materiaalonderzoek en onderzoek naar nieuwe (hoog-preciese) productietechnieken**, waarbij wordt gewerkt aan lichtere, sterkere en duurzamere metaal- en composietstructuren, alsook hybride toepassingen.

Deze materialen dragen bij aan gewichtsreductie, stealth-capaciteiten en verhoogde operationele efficiëntie van zowel bemande als onbemande toestellen.



Tekening 2: Vlaamse Sterktes

Ook op vlak van **aerodynamica** vinden er geavanceerde simulaties en experimentele studies plaats, onder meer rond nieuwe vleugelconfiguraties en aandrijftechnologieën die prestaties verbeteren in uiteenlopende operationele omgevingen.

Vlaanderen beschikt over een brede expertise en jarenlange ervaring in het domein van **sensorontwikkeling**, een technologisch sleutelgebied met toepassingen in zowel de civiele als militaire sector. Dankzij een sterke combinatie van academisch onderzoek, hoogtechnologische bedrijven en interdisciplinaire samenwerking is de regio uitgegroeid tot een innovatie hub voor geavanceerde sensortechnologieën. Vlaamse spelers ontwikkelen en verfijnen sensoren die variëren van optische en infraroodtechnologie tot multi-spectrale en hyper-spectrale systemen, waarmee omgevingen en objecten met ongezien detailniveau kunnen worden waargenomen en geanalyseerd. Deze technologieën spelen een cruciale rol in surveillance, doelherkenning, navigatie en situationele bewustwording. Onderzoeksinstellingen zoals imec, VITO en verschillende Vlaamse universiteiten nemen hierbij een voortrekkersrol op, vaak in nauwe samenwerking met industriële partners die deze innovaties vertalen naar operationele toepassingen binnen luchtvaart, drones, ruimtevaart en defensie.

Een belangrijk aandachtspunt binnen het Vlaamse sensoronderzoek is het streven naar **miniaturisatie**, met als doel sensoren kleiner, lichter en energie-efficiënter te maken zonder aan prestaties in te boeten — een cruciale vereiste voor gebruik in drones en andere onbemande systemen waar ruimte en gewicht beperkt zijn. Tegelijkertijd wordt sterk ingezet op **kostenefficiëntie** om sensortechnologie schaalbaar en breed inzetbaar te maken, zowel binnen militaire als civiele domeinen. Vlaanderen onderscheidt zich daarbij niet alleen door technologische diepgang, maar ook door het vermogen om **volledige sensorketens** te ontwikkelen waarin data-acquisitie, dataverwerking en systeemintegratie naadloos worden gecombineerd. Deze systemische benadering maakt het mogelijk om sensoren optimaal te benutten binnen complexe operationele omgevingen, en versterkt Vlaanderen's positie als strategische innovatieregio in Europa.

Daarnaast speelt Vlaanderen een actieve rol in het ontwikkelen van technologieën rond **Manned-Unmanned Teaming (MUM-T)**, waarbij bemande gevechtsvliegtuigen en onbemande systemen zoals loyal wingman-drones gecoördineerd ingezet worden. Deze concepten vereisen verregaande interoperabiliteit, betrouwbare communicatiesystemen en een hoge mate van autonomie – domeinen waarin Vlaamse bedrijven en kennisinstellingen een sterke technologische basis hebben uitgebouwd. **Digitalisatie** vormt hier een rode draad: van AI-gestuurde besluitvorming en dataverwerking tot cyberbeveiliging en geïntegreerde softwareplatformen voor luchtvaartoperaties.

Opvallend is ook de **kruisbestuiving met de Vlaamse gaming- en simulatiesector**, die wereldwijd bekendstaat om haar creativiteit en technologische voorsprong. De expertise in real-time rendering, virtuele omgevingen en interactief ontwerp wordt steeds vaker toegepast in de luchtvaart- en drone industrie voor digitale tweelingen, simulatie, missieplanning, training en virtual prototyping.

Deze afgeleide technologieën verhogen de effectiviteit van opleidingen en bieden veilige, kostenbesparende manieren om complexe scenario's te testen en optimaliseren.

3.3 Uitdagingen

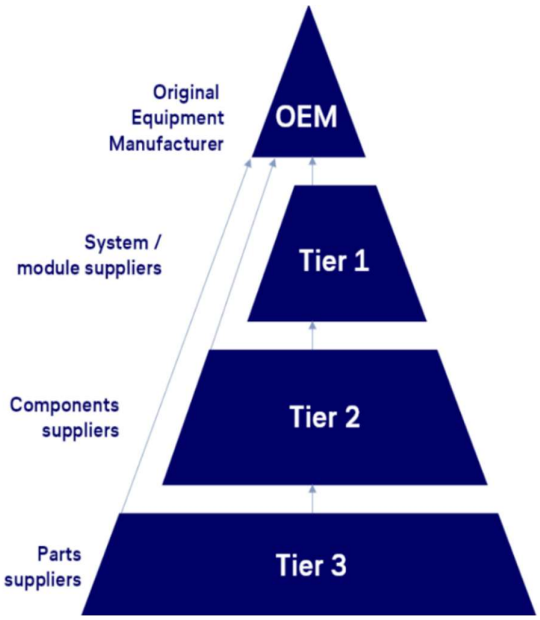
Hoewel het Vlaamse luchtvaart- en drone-ecosysteem zich kenmerkt door technologische excellentie en een sterke aanwezigheid van gespecialiseerde spelers, kampt het ook met enkele structurele uitdagingen. Een van de meest opvallende beperkingen is het gebrek aan systeemintegratoren en OEM's (Original Equipment Manufacturers). Daardoor ontbreekt een cruciale schakel in de waardeketen: spelers die de verschillende technologiecomponenten – van structuurelementen, sensoren en navigatie tot communicatie en aandrijving – samenbrengen tot volwaardige, operationele systemen. Deze leemte bemoeilijkt de opschaling, marktintroductie en internationale positionering van onze Vlaamse industrie en haar producten/diensten.

Tegelijkertijd wordt Vlaanderen geconfronteerd met toenemende internationale concurrentie. Grote buitenlandse spelers ontwikkelen geïntegreerde oplossingen aan een hoog tempo en domineren steeds meer markten en standaarden. Hierdoor wordt het moeilijker voor Vlaamse technologie-aanbieders om hun plek te verankeren in de internationale waardeketens, zeker wanneer zij afzonderlijk opereren of slechts componenten leveren. De afstand tot die globale waardeketens is voelbaar, en zonder voldoende zichtbaarheid en integratie wordt het risico groter dat Vlaamse innovatie onvoldoende wordt gevaloriseerd op het wereldtoneel.

De **waardeketen in de luchtvaartindustrie** is opgebouwd uit een gelaagd netwerk van producenten en toeleveranciers die elk een specifieke rol spelen in het ontwerp, de productie en het onderhoud van luchtvaartsystemen. Bovenaan staan de **OEM's (Original Equipment Manufacturers)**, zoals Airbus, Boeing of Dassault, die verantwoordelijk zijn voor het ontwerp, de integratie en eindassemblage van vliegtuigen of grote platformen.

Daaronder bevinden zich de **Tier 1-leveranciers**, vaak grote industriële spelers die complete subsystemen of belangrijke componenten leveren — zoals motoren, vleugelstructuren, landingsgestellen of avionica — en rechtstreeks samenwerken met de OEM.

De **Tier 2-leveranciers** produceren onderdelen of modules die deze subsystemen ondersteunen, zoals hydraulische systemen, sensoren of elektrische componenten.



Tekening 3 : Weergave van een luchtvaart waardeketen

De **Tier 3-leveranciers** leveren op hun beurt gespecialiseerde onderdelen, materialen of bewerkingen, bijvoorbeeld composietelementen, bevestigingsmiddelen of precisieonderdelen. Deze hiërarchische structuur maakt het mogelijk om complexe luchtvaartprojecten efficiënt te organiseren, waarbij innovatie, kwaliteit en betrouwbaarheid door de volledige keten heen essentieel zijn.

Om die positie te versterken, is intensievere interne samenwerking binnen het Vlaamse ecosysteem essentieel. De ontwikkeling en bouw van complexe (sub)systemen vraagt om gecoördineerde ketens van bedrijven en kennisinstellingen die complementaire technologieën en expertises bundelen. Door strategisch samen te werken rond integratieprojecten, kan Vlaanderen zich niet alleen technisch onderscheiden, maar ook operationeel sterker inkantelen in internationale programma's en consortia. Dit vereist gezamenlijke visie, durf tot schaalvergroting en ondersteuning vanuit beleid en industrie. Enkel zo kan Vlaanderen evolueren van een leverancier van hoogwaardige componenten naar een structurele partner in internationale luchtvaart- en dronetoepassingen.

3.4 Conclusie

Ondanks de structurele uitdaging biedt het ecosysteem een sterke basis voor groei, mits er wordt ingezet op meer samenwerking, open innovatie en waar mogelijk het aantrekken of ontwikkelen van systeem integratoren. Vlaanderen beschikt over het potentieel om een leidende rol te spelen in nichetoepassingen van dronetechnologie, mits dit ecosysteem verder wordt versterkt en strategisch uitgebouwd.

4 Innovatiekansen

4.1 Overzicht oriëntatie roadmap

	LUCHTVAART (MILITAIR) & DRONES					
Focuslaag	Sensoriek	Aandrijving & Autonomie (duurtijd operatie)	Manned-Unmanned Teaming (MUM-T) en strategische inzetbaarheid	Modulariteit	Stealth, hypersonica & andere eigenschappen	Kosten efficiëntie & schaalvergroting
Bouwsteen	Naast de continue vooruitgang in sensortechnologie ligt de focus eveneens op miniaturisatie en sensor fusion, ontwikkelingen die leiden tot slimmere, lichtere sensor pods en dragen bij tot een verhoogde autonomie en strategische inzetbaarheid	Vooruitgang in batterij technologie, energie management- en propulsie systemen moeten drones in staat stellen langer, efficiënter en stiller te vliegen, wat hun operationeel bereik en inzetbaarheid in uiteenlopende sectoren aanzienlijk vergroot.	Technologische ontwikkelingen op gebied van autonomie en strategische inzetbaarheid zullen drones transformeren tot intelligente systemen die zelfstandig complexe missies uitvoeren en flexibel kunnen worden ingezet in dynamische operationele omgevingen samen met bemande systemen.	Ontwikkeling van MOSA-architecturen (Modular Open Systems Architecture) leiden tot flexibele, snel aanpasbare 'platformen', MOSA architecturen faciliteren innovatie en multi-domein inzetbaarheid	Ontwikkeling van geavanceerde materialen en coatings in functie van verbeterede stealth-eigenschappen en performantere structurele prestaties van vliegtuigen en "Loyal Wingman" drone-toepassingen	Verdere kosten efficiëntie en schaalvergroting in de drone-industrie worden mogelijk gemaakt door technologische standaardisatie, modulaire ontwerpen, geautomatiseerde productieprocessen en bredere toepassing van dual-use componenten.

4.2 Sensoriek, miniaturisatie en sensorfusie

Thematische Doelstellingen

- **Hogere sensor resolutie en gevoeligheid**: waarneembaarheid van kleinere details , met betere prestaties bij slechts weer of lage lichtniveaus
- **Multifunctionele sensoren** die meerdere functies vervullen
- **AI-geïntegreerde sensoren met directe dataverwerking** (edge computing) ter vermindering van latency en verbetering van real-time besluitvorming

Het sensorisch domein evolueert razendsnel en vormt een essentiële pijler binnen de ontwikkeling van moderne luchtvaart- en dronetoepassingen. De industrie zet sterk in op geavanceerde sensortechnologieën die niet alleen de prestaties van individuele sensoren verbeteren, maar ook inzetten op miniaturisatie, sensor fusion en slimme dataverwerking. Deze evoluties leiden tot lichtere, compactere en energie-efficiëntere sensor pods, die perfect inzetbaar zijn op autonome of semi-autonome platformen en bijdragen aan een verhoogde strategische flexibiliteit.

Een belangrijke focus ligt op het verhogen van de sensorresolutie en gevoeligheid, zodat kleinere details beter waarneembaar worden – ook in moeilijke omstandigheden zoals slecht weer of lage lichtniveaus. Daarbij worden multifunctionele sensoren ontwikkeld die meerdere taken tegelijk kunnen uitvoeren, zoals het combineren van visuele waarneming, temperatuurmeting en navigatie-informatie in één geïntegreerd systeem.

- Kleinere, lichtere componenten, geavanceerde **micro-elektronica** (zoals MEMS – micro-electromechanical systems)
- **System-on-Chip** (SoC) waarbij verwerkingseenheden en sensoren worden geïntegreerd op één chip
- **Energiezuinige ontwerpen**
- **Geavanceerde, contextbewuste data-integratie**: Het combineren van data van meerdere sensortypes (bijv. GPS, IMU, visuele en infraroodbeelden) leidt tot robuustere en nauwkeurigere beslissingen, zelfs in omgevingen waar individuele sensoren falen
- **Real-time sensor fusion met AI en Machine learning-algoritmen** in functie van selectie en interpretatie van meest betrouwbare data bronnen

Deze benadering verlaagt het gewicht en de complexiteit van het totale systeem, terwijl de operationele capaciteiten toenemen.

Cruciaal in deze technologische vooruitgang is de integratie van AI en edge computing. AI-geïntegreerde sensoren zijn in staat om ruwe data lokaal te verwerken met minimale latency, wat toelaat om in real-time beslissingen te nemen zonder nood aan centrale verwerkingseenheden. Dit is bijzonder relevant in tactische of snel veranderende omgevingen waar reactietijd cruciaal is. Tegelijkertijd maken Vlaamse onderzoekers en bedrijven gebruik van geavanceerde micro-elektronica, zoals MEMS en System-on-Chip (SoC) technologieën, waarmee verwerkingseenheden en sensoren op één chip worden geïntegreerd, met grote voordelen op vlak van miniaturisatie en energieverbruik.

Tot slot wordt sterk ingezet op contextbewuste data-integratie: het combineren van data uit verschillende sensortypes zoals GPS, IMU, visuele camera's en infraroodsensoren. Dit verhoogt de betrouwbaarheid van beslissingsprocessen, zelfs wanneer individuele sensoren falen of verstoord worden. Dankzij real-time sensor fusion in combinatie met AI- en machine learning-algoritmen kunnen systemen autonoom de meest betrouwbare databronnen selecteren en interpreteren. Vlaanderen bevindt zich hiermee in een uitstekende positie om hoogwaardige sensortechnologieën te leveren voor complexe luchtvaart- en defensietoepassingen, met een sterke focus op intelligentie, robuustheid en schaalbaarheid.

4.3 Aandrijving en energiebeheer

Thematische Doelstellingen

- Hogere energiedichtheid dankzij ontwikkeling van **solid-state batterijen en lithium-metaal technologie** leidt tot langere vliegtijden en grotere actieradius.;
- **Sneller opladen en langere levensduur** dankzij nieuwe chemieën (zoals lithium-silicium) en laadstrategieën ter vermindering van degradatie en verbetering van snelladen zonder capaciteitsverlies
- **Veiligere batterij management systemen** door temperatuurcontrole, verbeterde behuizing en interne zelfdiagnose tegen thermische runaway
- **Slimme energieverdeling** dankzij AI en algoritmen voor real-time optimalisatie van energiegebruik (ifv vluchtfase, sensorgebruik en weersomstandigheden)

Het thema aandrijving en energiebeheer vormt een cruciale pijler in de verdere ontwikkeling van drones en geavanceerde luchtvaartsystemen. Nieuwe technologische doorbraken in batterijtechnologie, energiebeheer en hybride aandrijfsystemen stellen drones in staat langer, efficiënter en stiller te vliegen, wat hun operationeel bereik en inzetbaarheid in uiteenlopende sectoren – van defensie en inspectie tot logistiek en noodinterventie – aanzienlijk vergroot.

Een belangrijke evolutie is de opkomst van solid-state batterijen en lithium-metaal technologie, die zorgen voor een hogere energiedichtheid. Hierdoor kunnen drones grotere afstanden afleggen en langere vluchten uitvoeren zonder herladen. Tegelijk zorgen nieuwe materialen, zoals lithium-silicium, in combinatie met geavanceerde laadstrategieën voor sneller opladen en een langere levensduur van batterijen, zonder significant capaciteitsverlies. Dit verlaagt de onderhoudskosten en verhoogt de inzetbaarheid op het terrein.

Veiligheid blijft een belangrijke ontwerpprioriteit. Geavanceerde batterij management systemen combineren temperatuurcontrole, verbeterde behuizingen en interne zelfdiagnose om risico's zoals thermische runaway te minimaliseren. Daarnaast maakt de integratie van AI-gestuurde energieverdeling het mogelijk om het energieverbruik in real-time te optimaliseren, afhankelijk van vluchtfase, sensorgebruik en omgevingsomstandigheden.

- **Integratie van batterijen met hybride energiebronnen** met dynamisch schakelen tussen batterij, brandstofcel voor maximale efficiëntie
- Verdere optimalisatie van **direct-drive elektromotoren** met hoog rendement, lichtgewicht materialen en lage onderhoudsbehoefte
- **Hybride-elektrische en waterstofaandrijving** voor grotere autonomie

Hierdoor wordt het beschikbare vermogen efficiënter benut en kan de autonomie van het platform verder worden opgerekt.

Voor toepassingen met een hoge energiebehoefte wordt gewerkt aan hybride systemen, waarbij batterijen worden gecombineerd met andere energiebronnen zoals brandstofcellen. Deze systemen schakelen dynamisch tussen verschillende energiebronnen voor maximale efficiëntie en betrouwbaarheid. Tegelijk wordt ook ingezet op de verdere verfijning van direct-drive elektromotoren, die niet alleen efficiënter zijn maar ook lichter, onderhoudsarm en stiller functioneren dan klassieke motoren.

Voor grotere drones en eVTOLs (electric Vertical Take-Off and Landing systems) komen hybride-elektrische aandrijving en waterstoftechnologie in beeld. Deze systemen maken het mogelijk om langere afstanden af te leggen en complexere missies uit te voeren, met behoud van emissievrije of emissiearme prestaties. Vlaanderen heeft het potentieel om in deze niches een voortrekkersrol te spelen, mits verdere investeringen in materiaalonderzoek, systeemintegratie en slimme sturingsalgoritmen.

4.4 Manned-Unmanned Teaming

Thematische Doelstellingen

- **AI ondersteunde autonome besluitvorming** rond navigatie, doelherkenning, bedreigingsanalyse en beslissingsvorming
- **Machine Learning algoritmes** en swarming AI
- **LPI/LPG Communicatie-technologie** om de detecteerbaarheid van drones te beperken
- **Mesh netwerken en SATCOM** ter verbetering van communicatie in vijandige en complexe omgevingen
- **Vooruitgang in Human-Machine-Interface** (HMI) via spraak- en gebareninterfaces
- **AR/VR systemen** voor training en operationeel situationeel bewustzijn
- **Cybersecurity** laag met bescherming tegen hacking, spoofing en data manipulatie
- Nieuwe ontwikkelingen in **Elektronische Oorlogsvoering** (EW)

Het concept van Manned-Unmanned Teaming (MUM-T) vormt een van de meest strategische ontwikkelingen binnen de moderne luchtvaart- en defensietechnologie. Door bemande en onbemande systemen (zoals drones) naadloos te laten samenwerken, kunnen militaire en operationele capaciteiten aanzienlijk worden uitgebreid. In plaats van drones als losstaande sensoren of platforms in te zetten, worden ze geïntegreerd in gezamenlijke missiestructuren waarin ze autonoom opereren, maar wél in directe interactie met bemande systemen. Dit vraagt om verregaande technologische vernieuwing op vlak van autonomie, communicatie, interoperabiliteit en beveiliging.

Een essentieel fundament van deze evolutie is de toepassing van AI-ondersteunde autonome besluitvorming. Door gebruik te maken van kunstmatige intelligentie, kunnen drones zelfstandig navigeren, doelen detecteren, bedreigingen analyseren en zelfs in real-time beslissingen

nemen, zonder menselijke tussenkomst. Machine learning-algoritmen en swarming AI maken het bovendien mogelijk om meerdere onbemande systemen gecoördineerd en adaptief te laten samenwerken, wat het bereik en de impact van operaties aanzienlijk vergroot.

Om deze samenwerking efficiënt en veilig te laten verlopen, is robuuste en veilige communicatie onmisbaar. Vlaanderen ontwikkelt mee aan Low Probability of Intercept/Detection (LPI/LPD) communicatietechnologieën die de detecteerbaarheid van drones in vijandige omgevingen beperken. Daarnaast zorgen mesh-netwerken en SATCOM-oplossingen voor redundante en betrouwbare communicatie, zelfs in verstorende of vijandige omstandigheden. De compatibiliteit met bestaande commandostructuren en C4ISR-systemen (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) is hierbij cruciaal om een soepele integratie van bemande en onbemande systemen mogelijk te maken.

- Strategische inzet vereist **compatibiliteit met bestaande commandostructuren, sensor-netwerken en C4ISR-systemen**. (zie ook sensoriek en modulariteit)

Ook op het vlak van interactie met de menselijke operator zijn grote stappen gezet. Human-Machine Interfaces (HMI) evolueren richting natuurlijke communicatie via spraak- en gebarenherkenning, terwijl AR/VR-systemen worden ingezet voor realistische trainingsomgevingen en het versterken van het situationeel bewustzijn van piloten en operators.

Tegelijk wordt er sterk ingezet op cybersecurity, met beschermingslagen tegen hacking, spoofing en datamanipulatie, en op de integratie van technologieën uit de elektronische oorlogsvoering (EW) om verstoringen te detecteren en tegen te gaan.

Manned-unmanned teaming vereist dus een hoge graad van technologische maturiteit, interoperabiliteit en beveiliging, waarbij Vlaamse spelers zich kunnen onderscheiden in nichegebieden zoals autonome besluitvorming, veilige communicatie, sensorfusie en systeemintegratie. Mits verdere investeringen en samenwerking tussen KMO's, kennisinstellingen en defensieactoren, kan Vlaanderen hier een strategische rol opnemen in Europese en internationale samenwerkingsprogramma's.

4.5 Modulaire architecturen

Thematische Doelstellingen

- Stimuleren van een open ecosysteem waarin verschillende leveranciers modules kunnen aanbieden die compatibel zijn met bestaande platforms
- Toekomstbestendigheid en interoperabiliteit verhogen dankzij MOSA (Modular Open Systems Architecture) principes om flexibiliteit in ontwerp en samenwerking tussen verschillende partijen te waarborgen
- Modulair ontwerp van nieuwe platformen
- Ontwikkeling en gebruik van duidelijk gedefinieerde interfaces om 'vendor lock-in' te voorkomen
- Gebruik van Open Standaarden ter verbetering van de interoperabiliteit tussen verschillende systemen
- 'Loose Coupling' tussen de verschillende modules zodat modules uitwisselbaar en onafhankelijk zijn van elkaar waarbij de wijziging of uitval van één modules minimale impact heeft op de rest van het systeem

Modulariteit speelt een steeds belangrijkere rol in de ontwikkeling van geavanceerde luchtvaart- en dronesystemen. Door te werken met MOSA-architecturen (Modular Open Systems Architecture) kunnen platformen flexibeler en sneller worden aangepast aan veranderende operationele behoeften. Deze modulaire aanpak stimuleert innovatie doordat verschillende technologieën en componenten eenvoudig geïntegreerd kunnen worden, en maakt multi-domein inzetbaarheid mogelijk – essentieel in een omgeving waar systemen steeds vaker in combinatie met andere platformen en technologieën worden ingezet.

Een belangrijke pijler van MOSA is het creëren van een open ecosysteem, waarin diverse leveranciers hun modules aanbieden die compatibel zijn met bestaande systemen. Dit bevordert niet alleen de samenwerking tussen verschillende spelers, maar verhoogt ook de toekomstbestendigheid en interoperabiliteit van de platformen. Door het hanteren van MOSA-principes wordt flexibiliteit in ontwerp en ontwikkeling gewaarborgd, wat essentieel is om snel te kunnen inspelen op nieuwe technologische trends en operationele eisen.

Centraal in deze modulaire architectuur staat het modulair ontwerp van platformen, waarbij gebruik wordt gemaakt van duidelijk gedefinieerde interfaces. Deze interfaces voorkomen 'vendor lock-in', waardoor gebruikers niet gebonden zijn aan één enkele leverancier en makkelijk kunnen overschakelen of uitbreiden met nieuwe modules. Ook het gebruik van open standaarden draagt bij aan een betere interoperabiliteit tussen verschillende systemen en componenten, wat samenwerking en integratie vergemakkelijkt.

Daarnaast wordt gewerkt met het principe van 'loose coupling' tussen modules. Dit betekent dat de verschillende onderdelen van een systeem onafhankelijk van elkaar kunnen functioneren en uitwisselbaar zijn. Zo

heeft de wijziging, uitval of vervanging van één module slechts een minimale impact op de rest van het systeem. Deze aanpak verhoogt de robuustheid en onderhoudbaarheid van platforms aanzienlijk, en maakt het mogelijk om sneller en efficiënter nieuwe technologieën te implementeren zonder volledige herontwerpen.

Samengevat biedt modulariteit via MOSA-architecturen een krachtige basis voor de ontwikkeling van toekomstgerichte, flexibele en interoperabele dronesystemen en luchtvaart platformen, waarin innovatie en samenwerking tussen verschillende partijen centraal staan.

4.6 Geavanceerde materialen en aerodynamica

Thematische Doelstellingen

- Gewichtsreductie en prestatieverbetering door gebruik van lichtgewicht, hoogsterke materialen zoals composieten en geavanceerde legeringen
- Verhoogde duurzaamheid en levensduur dankzij ontwikkeling van materialen die beter bestand zijn tegen slijtage, corrosie en extreme weersomstandigheden, waardoor onderhoudsintervallen worden verlengd en impactbestendigheid verbeterd
- Verbeterde stealth door toepassing van coatings die radarabsorberende eigenschappen hebben en gebruik van thermisch camouflerende materialen die infrarooddetectie bemoeilijken
- Functionele coatings voor specifieke toepassingen zoals waterafstotende, vuil- en ijswerende coatings om operationele betrouwbaarheid te verbeteren en Anticorrosieve coatings voor inzet in maritieme of industriële omgevingen
- Materialen en coatings die de integratie van sensoren en communicatiesystemen bevorderen en versterken van structurele eigenschappen zonder afbreuk te doen aan elektromagnetische compatibiliteit.

De ontwikkeling van geavanceerde materialen en coatings speelt een cruciale rol in het verbeteren van zowel de structurele prestaties als de stealth-eigenschappen van moderne vliegtuigen en “Loyal Wingman” drone-toepassingen. Door het gebruik van extreem sterke, lichtgewicht materialen zoals composieten en geavanceerde legeringen, kan het totaalgewicht van platformen aanzienlijk worden verminderd zonder concessies te doen aan de structurele integriteit. Deze gewichtsreductie vertaalt zich direct in betere prestatieparameters zoals wendbaarheid, brandstofefficiëntie en actieradius.

Naast het verlagen van het gewicht ligt een sterke focus op het verhogen van de duurzaamheid en levensduur van materialen. Innovaties in materiaalkunde zorgen ervoor dat onderdelen beter bestand zijn tegen slijtage, corrosie en extreme weersomstandigheden. Dit leidt tot langere onderhoudsintervallen en een verbeterde impactbestendigheid, wat de operationele betrouwbaarheid en kostenefficiëntie ten goede komt.

Op het vlak van stealth zijn er aanzienlijke verbeteringen dankzij coatings met radar absorberende eigenschappen, die de zichtbaarheid van de platformen door radar verminderen. Daarnaast worden thermisch camouflerende materialen ingezet om detectie via infraroodsensoren te bemoeilijken, wat een strategisch voordeel biedt in vijandige omgevingen. Specifieke functionele coatings zoals waterafstotende, vuil- en ijswerende lagen verhogen de operationele betrouwbaarheid onder uiteenlopende omstandigheden, terwijl anticorrosieve coatings essentieel zijn voor toepassingen in maritieme of industriële omgevingen.

Een belangrijke technologische uitdaging is het ontwikkelen van materialen en coatings die de integratie van sensoren en communicatiesystemen ondersteunen zonder de elektromagnetische compatibiliteit te schaden. Dit vereist een zorgvuldige afstemming van materiaaleigenschappen, zodat deze systemen optimaal kunnen functioneren binnen het complexe ecosysteem van moderne drones en luchtvaartsystemen.

Samen dragen deze innovaties in materiaalkunde en aerodynamica bij aan drones en vliegtuigen die niet alleen lichter en sterker zijn, maar ook beter bestand tegen detectie en omgevingsinvloeden, wat hun strategische inzetbaarheid en operationele efficiëntie aanzienlijk verhoogt.

4.7 Kost efficiëntie en schaalbaarheid

Thematische Doelstellingen

- Standaardisatie en modulariteit : Bevorderen van gestandaardiseerde hardware- en softwarecomponenten en modulaire ontwerpen ter verbetering van uitwisselbaarheid en hergebruik van verschillende componenten mogelijk maken
- Geautomatiseerde en gedigitaliseerde productieprocessen (bv. 3D-printing, robotassemblage) om productiekosten te verlagen en consistente kwaliteit op schaal te garanderen en gebruik van digital-twins en simulatie software in ontwerp- en testfases om ontwikkelkosten te reduceren.
- Gebruik van dual-use technologieën en ontwerp van modulaire universele platform om ontwikkelkosten te verlagen en beschikbaarheid van onderdelen te verhogen
- Inzetten op technologieën en sensoren in functie van langere onderhoudsintervallen en automatische diagnosestelsels

De kostenefficiëntie en schaalbaarheid binnen de drone-industrie worden steeds meer gedreven door technologische vooruitgang op het gebied van standaardisatie, modulariteit en geautomatiseerde productieprocessen. Door te investeren in gestandaardiseerde hardware- en softwarecomponenten en het stimuleren van modulaire ontwerpen, wordt het eenvoudiger om componenten uit te wisselen en hergebruiken. Dit zorgt niet alleen voor lagere ontwikkelkosten, maar maakt ook een flexibeler productieproces mogelijk waarbij sneller kan worden ingespeeld op veranderende marktbehoeften.

Daarnaast speelt de implementatie van geautomatiseerde en gedigitaliseerde productieprocessen, zoals 3D-printing en robotassemblage, een belangrijke rol bij het verlagen van productiekosten en het garanderen van een consistente kwaliteit, ook bij grotere productievolumes. Het gebruik van digital twins en simulatiesoftware in ontwerp- en testfases draagt bij aan het reduceren van ontwikkeltijden en -kosten door virtueel testen en optimaliseren, waardoor fysieke prototypes en fouten tot een minimum worden beperkt.

Een bredere toepassing van dual-use technologieën en de ontwikkeling van universele platformen dragen eveneens bij aan een verlaging van ontwikkelkosten en verhogen de beschikbaarheid van onderdelen. Dit vergemakkelijkt de integratie van verschillende technologieën en maakt het mogelijk om dezelfde componenten in uiteenlopende toepassingen in te zetten. Tot slot zorgt digitale, geautomatiseerde real-time diagnosestelling voor een efficiëntere monitoring van operationele status en onderhoudsbehoeften, wat leidt tot lagere onderhoudskosten en een hogere beschikbaarheid van drones in het veld.

Deze gecombineerde aanpak van standaardisatie, modulariteit, automatisering en digitalisering vormt een solide basis voor kostenefficiënte opschaling en verhoogt de concurrentiekracht van de drone-industrie op internationaal vlak.

5 Conclusie

Dronetechnologie bevindt zich op een kantelpunt waarbij civiele innovatie en militaire toepassingen steeds dichter naar elkaar toe groeien. De brede waaier aan toepassingen — van infrastructuurinspectie en landbouw tot civiele veiligheid en militaire operaties — toont aan dat drones een structurele rol zullen opnemen in onze toekomstige luchtvaart-, veiligheids- en defensiesystemen. De trend naar toenemende autonomie, netwerk-gebaseerde samenwerking, AI-integratie en modulariteit maakt drones niet alleen slimmer, maar ook onmisbaar in het bredere ecosysteem van veiligheid en strategische capaciteit.

De ontwikkelingen rond zesde generatie gevechtsvliegtuigen en onbemande “loyal wingman”-platformen bieden reële kansen voor de Vlaamse luchtvaartindustrie. Ze creëren zowel op korte als lange termijn belangrijke mogelijkheden voor de ontwikkeling van nieuwe, disruptieve technologieën, die het innovatievermogen en de internationale positie van de sector verder kunnen versterken.

Het regionale ecosysteem beschikt over sterke troeven in nichetechnologieën zoals sensoren, materiaalonderzoek, high-precision manufacturing, AI, digitalisatie, 'Power Electronica', en Manned-Unmanned Teaming.

Tegelijkertijd zijn er structurele uitdagingen, zoals het ontbreken van systeemintegratoren en een versnipperde keten. Willen we deze technologie ook op schaal kunnen valoriseren en inzetten binnen Europese en internationale programma's, dan is een gecoördineerde strategie nodig waarin samenwerking, ketenregie (het streven naar ontwerp en productie van complexe (sub)systemen) en schaalvergroting centraal staan.

Door gericht te investeren in strategische samenwerking tussen industrie, kennisinstellingen en overheid, en in te zetten op geïntegreerde oplossingen met dual-use potentieel, kan Vlaanderen uitgroeien tot een toonaangevende speler binnen het snel evoluerende luchtvaart- en dronelandschap. De sleutel tot succes ligt in een toekomstgerichte visie waarin innovatie, veiligheid, autonomie en economische waarde samenkomen in één robuust, adaptief en internationaal verankerd ecosysteem.

Embracing technology
Embracing ambition

Impulsprogramma Veiligheid & Defensie

Oriëntatieroadmap

Counter-UAS

(Counter-Unmanned Aerial Systems)

Document opgesteld door Agoria-FLAG – Flemish Aerospace Group,
de cluster van de Vlaamse Luchtvaartindustrie, op vraag van WEWIS

Oktober 2025

Inhoudsopgave:

1 Inleiding

1.1 Snelle ontwikkelingen in de UAS industrie

Definitie: **UAS** (Unmanned Aerial Systems), beter bekend als drones, kunnen autonoom opereren of op afstand bestuurd worden, zonder dat er een piloot aan boord is. Het omvat het vliegtuig zelf, het grondcontrolesysteem en een datatransmissieverbinding die communicatie tussen de operator en de drone mogelijk maakt.

De afgelopen jaren is de aanwezigheid van UAS of 'drones' in het Europese luchtruim aanzienlijk toegenomen, waarbij UAS in verschillende sectoren voor diverse toepassingen worden gebruikt. Technologische ontwikkelingen, zoals de uitrol van 5G-netwerken en de integratie van kunstmatige intelligentie (AI), hebben hun mogelijkheden verder vergroot.

1.2 Civiele Context

De civiele toepassingen van drones kennen een snelle opmars, en worden sterk gedreven door voortdurende technologische innovaties. Geavanceerde sensoren, artificiële intelligentie en verbeterde communicatiesystemen maken toepassingen mogelijk in uiteenlopende domeinen zoals inspectie, monitoring, logistiek, landbouw en noodhulp. Deze evoluties zorgen niet alleen voor efficiëntere operaties, maar creëren ook nieuwe economische kansen én uitdagingen op het vlak van regelgeving, veiligheid en integratie in het luchtruim.

De Europese Unie heeft proactief maatregelen genomen door actieplannen uit te voeren en regelgevende kaders vast te stellen, wat cruciale eerste stappen zijn in het beperken van incidenten en ongevallen met UAS. Hierbij verwijzen we in eerste plaats naar volgende Europese verordeningen:

De **EU-verordening 2019/947**, die op 24 mei 2019 in werking is getreden, stelt de regels en procedures vast voor het gebruik van onbemande luchtvaartuigen (UAS) binnen de Europese Unie. Deze verordening maakt het mogelijk dat onbemande luchtvaartuigen, ongeacht hun massa, naast bemande luchtvaartuigen in hetzelfde luchtruim opereren, waarbij wordt gewaarborgd dat UAS-operaties even veilig zijn als bemande luchtvaart. De verordening heeft tot doel te zorgen voor een uniforme toepassing van regels en procedures voor exploitanten, met inbegrip van piloten op afstand, en houdt rekening met de specifieke kenmerken van UAS-operaties. [1]

De **EU uitvoeringsverordening 2021/664** van de Commissie, die op 22 april 2021 is vastgesteld, stelt een regelgevend kader vast voor U-space, dat is ontworpen om de veilige werking van onbemande luchtvaartuigen (UAS) in het luchtruim te waarborgen. Deze verordening bevat regels en procedures voor de integratie van UAS in het luchtvaartsysteem en de levering van U-space-diensten. Dit is van cruciaal belang voor het beheer van de risico's in het luchtruim die verband houden met UAS-operaties en is relevant voor de domeinen drones en luchtmobiliteit. [2]

Echter, naast de vele nuttige en legale toepassingen van drones, en ondanks de verschillende beleidsmaatregelen en regelgevende kaders maken ook criminele organisaties gebruik van deze technologie voor minder legitieme doeleinden. Dit heeft geleid tot toenemende bezorgdheid over mogelijk misbruik van drones voor illegale activiteiten zoals smokkel, spionage, het verstoren van diensten, en zelfs het transport van explosieven of gevaarlijke stoffen.

[1] EU-verordering 2019/947 : Implementing regulation - 2019/947 - EN - EUR-Lex
[2] **EU uitvoeringsverordening 2021/664:** Implementing regulation - 2021/664 - EN - EUR-Lex

Onlangs werden opnieuw meerdere drone-incidenten gemeld boven Scandinavische luchthavens. Deze voorvallen leidden onvermijdelijk tot een tijdelijke stillegging van de operaties, met zowel economische als imagoschade tot gevolg.[3]

Tekening 1: Financial Times, 29/09/2025

1.3 Militaire Context

De rol van UAS in moderne oorlogsvoering evolueert snel aangezien drones aanzienlijke voordelen bieden zoals dankzij de bediening op afstand, de kostenefficiëntie en minder risico voor menselijke piloten en militair personeel in het algemeen. UAS zijn een cruciaal onderdeel geworden van militaire operaties en worden zowel voor surveillance (ISR) als voor luchtaanvallen gebruikt. Naarmate hun mogelijkheden toenemen, vereisen ze steeds meer aandacht met betrekking tot veilige en beveiligde operaties binnen het militaire luchtruim. Recent nog werden er 15 drones waargenomen boven het militair domain Elsenborn [4]. Hoewel de herkomst van de drones onduidelijk blijft en er geen sprake is van een directe dreiging, zet dit incident de bewaking van militaire sites én het bredere C-UAS-debat opnieuw op scherp.

Bijgevolg wordt de noodzaak van doeltreffende C-UAS-systemen (Counter-Unmanned Aerial Systems) in een militaire context steeds urgenter door de snelle evolutie en proliferatie van drones, zowel bij statelijke als niet-statelijke actoren. Binnen de bewaking van vaste militaire installaties – zoals luchtmachtbasissen, munitiedepots of commandocentra – zijn vaste C-UAS-oplossingen essentieel om continue detectie, identificatie en neutralisatie van potentiële dreigingen te garanderen. Tegelijk is er behoefte aan mobiele systemen die snel inzetbaar zijn tijdens operaties in binnen- en buitenland, zodat troepen bescherming genieten bij tijdelijke kampementen, logistieke knooppunten of tijdens verplaatsingen. Tot slot groeit de vraag naar compacte, tactische C-UAS-capaciteiten op compagnies- en soldaatniveau, met name binnen special forces, waar situational awareness en onmiddellijke reactiemogelijkheden cruciaal zijn. Elk van deze niveaus vereist een eigen technologische benadering en integratie binnen de bredere militaire commandostructuur, zodat een gelaagde, adaptieve verdediging tegen vijandelijke drones kan worden gegarandeerd.

1.4 Nood aan veiligheidsmaatregelen

Bijgevolg is het, naarmate de dronetechnologie zich verder ontwikkelt, van cruciaal belang om robuuste veiligheidsmaatregelen te nemen om een veilig luchtruim te handhaven en kritieke infrastructuur te beschermen. [5]

Voor een land als België, met een relatief beperkte territoriale omvang en korte afstanden tussen militaire en kritieke civiele infrastructuur, is het logisch om na te denken over een geïntegreerde benadering van civiele en militaire belangen. Een dergelijke samenwerking kan bijdragen aan een doeltreffender beheer van C-UAS systemen, zowel voor interne veiligheid als voor militaire (externe) doeleinden.

[3] Denmark drone incidents expose European airspace vulnerabilities
[4] Vijftien drones waargenomen boven militair terrein Elsenborn: "Erg bizar incident" | VRT NWS: nieuws
[5] European Commission: Drones, counter drones and autonomous systems

Om de veiligheidsrisico's van drones aan te pakken, is een alomvattende aanpak nodig, waarbij technologieën voor detectie, identificatie, tracking en neutralisatie worden gecombineerd. We verwijzen naar een gecombineerde systeem ('system-of-systems') aanpak. Dit is essentieel voor het effectief en efficiënt inzetten van C-UAS-systemen. Dit houdt echter ook in dat commando- en controlemechanismen over meerdere betrokken diensten of instanties dienen afgestemd te worden, en dat de risico's op nevenschade zorgvuldig worden geëvalueerd en afgewogen – zowel bij de inzet van lethale als niet-lethale C-UAS effectoren.

Ook de Europese Commissie en het European Defence Fund erkennen de noodzaak voor een versnelde investering in C-UAS-systemen door de lidstaten. Binnen het SAFE-programma (Security Action for Europe) zijn C-UAS-systemen opgenomen in zowel categorie 1 als categorie 2, wat de lidstaten aanmoedigt om de uitrol van een Europees C-UAS-netwerk te versnellen. [6]

2 C-UAS en potentiële dreiging

2.1 Inleiding

De snelle toename van drone-activiteiten leidt tot een groeiend aantal incidenten, hoofdzakelijk veroorzaakt door technische storingen, menselijke fouten of een gebrek aan bewustzijn bij operators. Deze voorvallen kunnen ernstige gevolgen hebben, zoals verstoring van openbare ruimtes, schade aan kritieke infrastructuur en inbreuken op de privacy. Hoewel een groot deel van de incidenten het gevolg is van onwetend of roekeloos gedrag, groeit ook de bezorgdheid rond niet-coöperatieve drones die bewust buiten de regels opereren.

Slechts een klein deel van de gedetecteerde vluchten blijkt geautoriseerd, wat het belang onderstreept van robuuste detectie-, identificatie- en neutralisatiesystemen. Om de veiligheid van luchtruim, bevolking en strategische infrastructuur te waarborgen, is het essentieel te investeren in geïntegreerde technologieën die coöperatieve en niet-coöperatieve drones kunnen onderscheiden en adequaat kunnen reageren op potentiële dreigingen..

2.2 Belangrijkste drijfveren voor C-UAS in de civiele omgeving

Openbare veiligheid en nationale veiligheid: Drones kunnen worden gebruikt om grote openbare bijeenkomsten zoals concerten, sportevenementen, protesten of politieke bijeenkomsten te verstoren of aan te vallen, of om het luchtverkeer te verstoren, zoals blijkt uit het incident op Gatwick Airport in 2018.

Drones worden ingezet om smokkelwaar in gevangenissen te brengen en om bewaking uit te voeren in de buurt van gevoelige locaties.

De dreiging van bewapende of bewakingsdrones die worden gebruikt bij terroristische aanslagen of politiek gemotiveerde verstoringen vormt een groeiende zorg voor de nationale veiligheid.

Bescherming van kritieke infrastructuur: Belangrijke installaties zoals energiecentrales, overheidsgebouwen en transportknooppunten zijn kwetsbaar voor bewaking, interferentie of sabotage door drones. Vroegtijdige detectie en neutralisatie van ongeautoriseerde drones kan ernstige verstoringen van de dienstverlening en veiligheidsincidenten voorkomen.

[6] SAFE | Security Action for Europe - European Commission

Privacy: Civiele drones die zijn uitgerust met camera's met hoge resolutie kunnen de persoonlijke privacy schenden. C-UAS-oplossingen helpen bij de handhaving van wetten met betrekking tot luchtruimschending, waardoor de rechten en persoonlijke ruimte van burgers worden beschermd.

Evenementenbeveiliging: Grote openbare bijeenkomsten zoals concerten, sportevenementen en festivals worden steeds vaker het doelwit van drone-invasies. C-UAS-capaciteiten zorgen voor een veilig luchtruim boven deze evenementen en verminderen het risico op crashes of kwaadwillige aanvallen.

Luchtruimintegriteit: Drones die zonder toestemming vliegen in de buurt van gecontroleerd of druk luchtruim vormen een risico op botsingen met bemande vliegtuigen. Civiele C-UAS-systemen verbeteren de veiligheid van het nationale luchtruim door ondersteuning te bieden aan luchtverkeersbeheer en bewakingsinspanningen.

3.6 Belangrijkste drijfveren voor C-UAS in militaire omgevingen

Nu dronetechnologie een integraal onderdeel van moderne oorlogsvoering is geworden, worden strijdkrachten geconfronteerd met toenemende dreigingen van vijandige en ongeautoriseerde UAS. De volgende vijf domeinen vormen de belangrijkste drijfveren voor de inzet van C-UAS capaciteiten in militaire omgevingen:

Bescherming van strijdkrachten: Drones kunnen door tegenstanders worden gebruikt voor verkenning, het aanwijzen van doelen of directe aanvallen op personeel en middelen. Vooruitgeschoven operationele bases, konvooien en gevechtsposten zijn bijzonder kwetsbaar. C-UAS systemen bieden cruciale bescherming door inkomende dreigingen te detecteren, te volgen en te neutraliseren, waardoor soldaten en installaties worden beschermd.

Superioriteit op het slagveld en situationeel bewustzijn: Vijanden gebruiken drones om inlichtingen te verzamelen, troepenbewegingen te volgen en communicatie te verstoren. C-UAS-tools ontzeggen de vijand toegang tot het luchtruim, waardoor informatievoorsprong en operationele geheimhouding behouden blijven. Dit ondersteunt tactisch voordeel en het welslagen van missies.

Bescherming van strategische activa: hoogwaardige militaire activa – zoals commandocentra, radarstations, logistieke knooppunten en nucleaire faciliteiten – zijn belangrijke doelwitten voor dronesurveillance of sabotage. C-UAS-technologieën zijn essentieel om het luchtruim rond deze kritieke knooppunten te monitoren en te beveiligen, waardoor operationele paraatheid en strategische stabiliteit worden gewaarborgd.

Contra-insurgency en asymmetrische oorlogsvoering; Niet-statelijke actoren en irreguliere strijdkrachten maken steeds vaker gebruik van goedkope drones voor aanvallen, surveillance of psychologische oorlogsvoering. In conflictgebieden kunnen kleine drones explosieven vervoeren of doelwitgegevens verzamelen. C-UAS-systemen bieden schaalbare verdedigingsoplossingen om deze asymmetrische dreigingen te neutraliseren, met name in stedelijke of complexe terreinen.

Elektronische oorlogsvoering en geïntegreerde luchtverdediging: Drones kunnen deel uitmaken van bredere elektronische en hybride oorlogsvoeringstrategieën, waaronder het storen, misleiden of overweldigen van verdedigingssystemen. Door C-UAS te integreren in bredere luchtverdedigings- en EW-kaders wordt gezorgd voor gecoördineerde reacties op bedreigingen op meerdere domeinen, waardoor de algehele militaire veerkracht wordt vergroot.

C-UAS in militaire omgevingen gaat niet alleen over het beschermen van het luchtruim, maar ook over het behouden van operationeel voordeel, de overlevingskansen van troepen en het waarborgen van missies in steeds meer omstreden domeinen. Deze drijfveren onderstrepen de noodzaak van snelle ontwikkeling, implementatie en integratie van C-UAS in alle strijdkrachten.

3 C-UAS Systemen

3.1 Algemeen

Het tegengaan van UAS-dreiging is een uitdagende taak, zowel op militair als civiel gebied. Daarom is het belangrijk om alle beschikbare middelen in te zetten om deze taak te volbrengen.

De effectiviteit van C-UAS-operaties hangt af van een methodologie die een evenwicht biedt tussen preventieve en reactieve maatregelen. Preventieve maatregelen moeten in de eerste plaats gericht zijn op het afschrikken, onderdrukken of vermijden van de dreiging. Als deze maatregelen tekortschieten, zijn reactieve tegenmaatregelen nodig om de dreiging op te sporen, te beoordelen en te neutraliseren. De tijd die beschikbaar is om deze processen uit te voeren, is de belangrijkste factor die bepaalt of ze al dan niet slagen.

3.2 Geïntegreerde systemen

Een krachtig en effectief C-UAS systeem steunt op een robuuste **systeemarchitectuur** die **multi-sensorintegratie** en **multi-effectorintegratie** mogelijk maakt. Sensoren zoals radar, RF-detectoren, EO/IR-camera's, akoestische sensoren en transpondersignalen moeten naadloos samenwerken binnen een geïntegreerd systeem, dat in staat is om informatie te consolideren, dreigingen te analyseren en passende reacties te coördineren.

Even belangrijk is de koppeling aan meerdere neutralisatie technieken en effectoren, zoals elektronische verstoring, kinetische middelen of spoofing technieken, die flexibel en proportioneel kunnen worden ingezet afhankelijk van de aard van de dreiging.

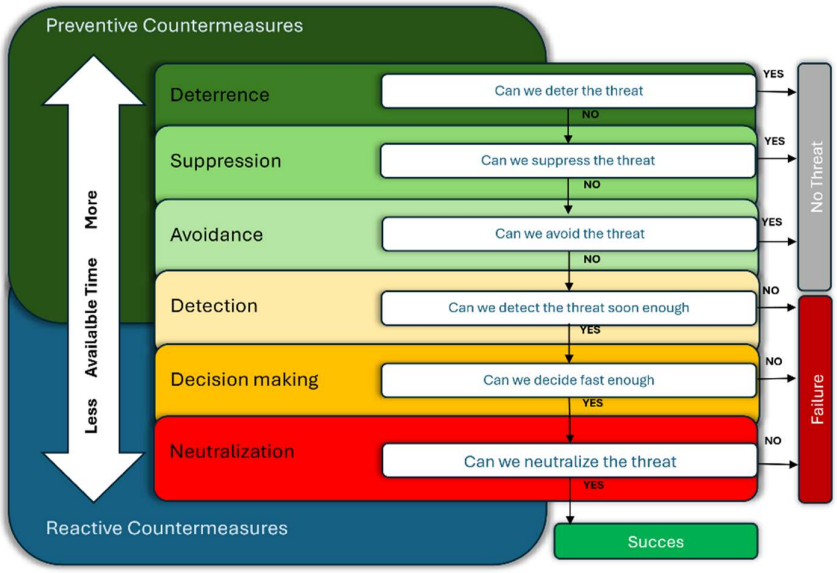
C-UAS systemen gaan ook verder dan alleen het tegengaan van dreigingen vanuit de lucht. Ze omvatten het aanpakken van kwetsbaarheden in het gehele onbemande systeem, dat niet alleen het luchtplatform omvat, maar ook belangrijke componenten zoals grondcontrolestations (zowel mobiel als stationair), radiocommunicatieverbindingen en menselijke operators.

Een volledig geïntegreerde, AI-gestuurde **C2 – Command & Control** oplossing vormt het hart van dit systeem en ondersteunt zowel geautomatiseerde als operator-gestuurde activatie van tegenmaatregelen. Het systeem moet in staat zijn om acties veilig te deconflicteren, juridische conformiteit te waarborgen (met name in civiele omgevingen), en een gecoördineerde werking tussen alle subsystemen te garanderen. Integratie met militaire of civiele commandonetwerken maakt het mogelijk om waarschuwingen snel te verspreiden en ondersteunende eenheden aan te sturen waar nodig.

3.3 C-UAS Methodologie

C-UAS methodologie verwijst naar de manier waarop het systeem wordt ingezet, geëxploiteerd en beheerd op het terrein. De meeste huidige C-UAS-systemen richten zich voornamelijk op de volgende taken: 'detecteren, identificeren, volgen en neutraliseren.

Zodra actieve neutralisatie maatregelen nodig zijn, wordt de snelheid van de besluitvorming doorslaggevend.



Tekening 2: C-UAS kill-chain & methodologie

De duidelijke omschrijving van de C-UAS inzetkaders en de vertaling ervan naar operationele methodologieën, tactische doctrines en algemene strategieën zijn van cruciaal belang voor de effectiviteit van de systemen.

Deze inzetkaders moeten het volledige spectrum van de C-UAS methologie en neutralisatie technieken omvatten in functie van een evenwichtige, evenredige reactie.

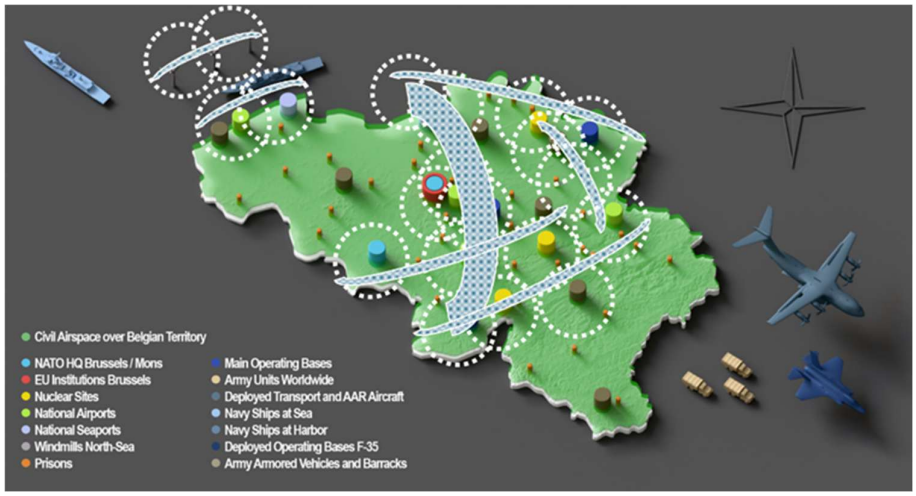
Deze gestructureerde aanpak moet een soepele coördinatie tussen het internationale, nationale, regionale en lokale niveau mogelijk maken, de samenwerking tussen civiele en militaire ANSPS bevorderen en efficiënte, verantwoordelijke kaders tussen hen tot stand brengen.

3.4 Gelaagde verdediging

De ontwikkeling en implementatie van een doordachte C-UAS methodologie voor alle potentiële civiele en militaire doelen in België legt de basis voor een uitgebreide, gelaagde veiligheid- en defensiestrategie, niet alleen in geografische zin, maar ook op het gebied van 'command en control'.

Geografische gelaagdheid : Het detecteren van dreigingen in een vroeg stadium, via strategisch gepositioneerde 'decectie, identificatie en tracking' systemen over het grondgebied, verhoogt de algehele paraatheid, maakt een snelle implementatie van tegenmaatregelen mogelijk en verbetert het vermogen van het land om op potentiële dreigingen te reageren. Het opsporen van dreigingen in een vroeg stadium versterkt niet alleen de verdedigingsmaatregelen, maar stelt ook aanvullende systemen in staat een cruciale rol te spelen bij het verbeteren van de algehele veerkracht.

Deze systemen kunnen zorgen voor cruciale redundantie, storingen compenseren, kwetsbaarheden verminderen en hiaten in de verdedigingslinies opvullen. Door aanvullende C-UAS-systemen in verschillende verdedigingslagen te integreren, wordt het algehele veiligheidskader robuuster, waardoor geen enkel storingspunt de effectiviteit van de reactie van het land op opkomende dreigingen in gevaar brengt.



Tekening 3: Geografische gelaagdheid

De noodzaak van een geografisch gelaagde verdediging werpt belangrijke vragen op bij de geplande EU Drone Wall[7] die de Europese Commissie wil realiseren. De asymmetrische dreiging die uitgaat van drones kan immers overal ontstaan en beperkt zich niet tot de oostelijke flank van de Europese Unie. Een effectieve verdediging vereist dan ook een flexibel en adaptief systeem dat over het volledige Europese grondgebied kan worden ingezet, afgestemd op uiteenlopende dreigingsniveaus en operationele contexten.

Gelaagde Commando & Controle (C2) structuren: Het concept van gelaagde verdediging moet niet alleen in geografische termen worden begrepen; het is ook van toepassing op gegevensbeheer en -uitwisseling en commando en controle, die op meerdere niveaus plaatsvinden.

De integratie van militaire en civiele gegevens verzekert een adequaat situationeel bewustzijn, waardoor snelle, daadkrachtige acties mogelijk zijn over de verschillende autoriteiten en diensten heen. Daarbij laten gedistribueerde commando en controle structuren toe om op lokaal niveau snel te ageren, alsook de escaleren naar bovenliggende niveau's in functie van het dreigingsniveau.

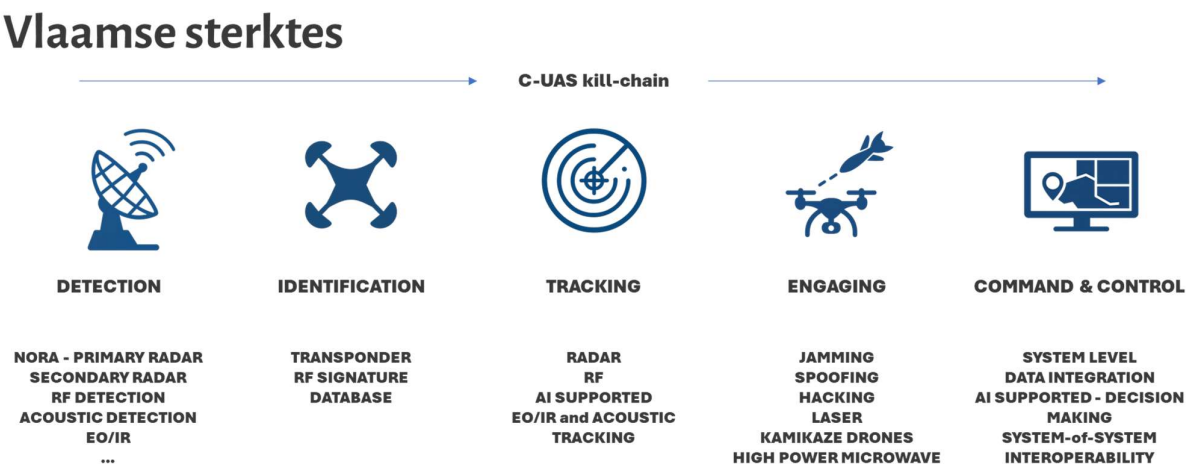
4 Stakeholder mapping – Vlaamse sterktes

4.1 Het Vlaamse C-UAS ecosystem

Hoewel de C-UAS industrie internationaal nog steeds beschouwd wordt als een ontluikende en sterk evoluerende markt, beschikt België – en Vlaanderen in het bijzonder – vandaag al over een in omvang weliswaar bescheiden, toch opmerkelijk sterk en technologisch geavanceerd C-UAS ecosysteem. De hoeveelheid aan gespecialiseerde bedrijven, academische instellingen en onderzoeksorganisaties in alle essentiële sub-domeinen van C-UAS is ronduit indrukwekkend. Onze bedrijven zijn actief is alle onderdelen van de C-UAS methodologie : **detectie**, **identificatie**, **tracking** en **neutralisatie**.

De Vlaamse C-UAS actoren hebben de voorbije jaren innovatieve technologieën ontwikkeld die bijdragen aan een brede waaier aan C-UAS-toepassingen, met zowel civiele als defensieve relevantie. Al dient gesteld dat hard-kill neutralisatie toepassingen (c.q. door middel van ondermeer ballistische

[7] EU moves forward with drone wall – POLITICO



Tekening 4: Vlaamse sterktes

effectoren) eerder in de zuidelijke landshelft ontwikkeld worden, en dat Vlaanderen zich in het verleden vooral heeft toegelegd op de ontwikkeling van oplossingen voor onder meer radar-, radiofrequentie- en visuele detectie, geavanceerde signaalverwerking, automatische tracking van verdachte objecten en systemen voor passieve neutralisatie van drones. Tevens merken we op dat er verschillende bedrijven zich ook richten op nieuwe lethale effector technologieën als laser en 'high-power microwave' (HPM). Wat dit ecosysteem extra bijzonder maakt, is de sterke rol van innovatieve kmo's. Deze bedrijven zijn vaak actief in zeer gespecialiseerde niche technologiedomeinen en leveren cruciale bouwstenen voor bredere systemen.

4.2 Opkomende technologie-domeinen in Vlaanderen

Naast de klassieke technologiedomeinen ontstaan in Vlaanderen steeds meer onderzoeks- en innovatietrajecten rond nieuwe, snel opkomende toepassingen en technologische gebieden.

Interceptor drones of Kamikaze drones: Een van de meest opvallende technologische ontwikkelingen binnen het C-UAS-domein is de opkomst van zogeheten hunter-killer drones. Deze autonome of semi-autonome platforms zijn specifiek ontworpen om andere drones op te sporen, te volgen en indien nodig uit te schakelen. Ze combineren sensoren voor detectie en tracking met ingebouwde neutralisatie-mechanismen, zoals netwerpermechanismen, kinetic impactors of elektronische verstoringssystemen. Hunter-killer drones zijn bijzonder geschikt voor bescherming van kritieke infrastructuur, mobiele eenheden of evenementenzones waar een snelle respons vereist is. Door hun mobiliteit en inzetbaarheid in zwak of niet afgedekte gebieden vullen ze bestaande vaste detectie- en effectorsystemen aan. Deze technologie bevindt zich nog in volle ontwikkeling, maar wordt wereldwijd erkend als een gamechanger in het operationeel beveiligen van luchtruim tegen ongewenste UAS-activiteiten.

Flexibele, gedistribueerde C2-systemen: Met de toename van het aantal sensoren, effectoren en inzetscenario's binnen C-UAS-operaties groeit de behoefte aan flexibele en gedistribueerde *Command & Control* (C2)-systemen. Deze systemen maken het mogelijk om data van verschillende bronnen — waaronder radar, RF-scanners, camera's en effectors — te verzamelen, te verwerken en te coördineren over meerdere locaties of entiteiten. In tegenstelling tot traditionele, gecentraliseerde C2-architecturen bieden gedistribueerde systemen een hogere robuustheid, schaalbaarheid en

responsiviteit. Dit is cruciaal in scenario's waarbij meerdere dreigingen zich gelijktijdig voordoen of waarin samenwerking tussen civiele en militaire eenheden vereist is.

Hoewel er momenteel nog geen Belgische of Vlaamse industriële speler bestaat die een volledig geïntegreerde C2-oplossing aanbiedt, wordt deze leemte (c.q. 'technology gap') snel kleiner. Verscheidene Vlaamse technologiebedrijven en kennisinstellingen zijn actief betrokken bij de ontwikkeling van modulaire, interoperabele C2-oplossingen die via open standaarden kunnen worden gekoppeld aan zowel bestaande beveiligingsnetwerken als NAVO-conforme systemen.

Geautomatiseerde bedreigingsanalyse : In een tijdperk van verhoogde dronesaturatie is het ondoenlijk om alle binnenkomende dreigingsinformatie manueel te verwerken. Daarom neemt het belang van systemen voor Geautomatiseerde bedreigingsanalyse en C2-ondersteuning sterk toe. Deze systemen maken gebruik van artificiële intelligentie, patroonherkenning en machine learning om snel en accuraat verdachte vluchten te classificeren, risico's in te schatten en aanbevelingen te formuleren voor passende responsacties. Ze ondersteunen de commandanten en operatoren in real-time door het aanleveren van contextuele beslissingsinformatie, inclusief scenario-afwegingen, risicoprofielen en inzetopties. In België en Vlaanderen wordt binnen verschillende onderzoeksprojecten gewerkt aan dergelijke AI-gedreven ondersteuningstools, die essentieel zijn om binnen complexe, multi-dreigingsomgevingen de situational awareness en reactiesnelheid aanzienlijk te verhogen.

4.3 Triple-helix

De snelle technologische ontwikkelingen en het toenemende dreigingsniveau onderstrepen de dringende noodzaak voor België en Vlaanderen om werk te maken van een robuuste en strategisch onderbouwde aanpak op het vlak van C-UAS. Dit is belangrijk met zowel het oog op de interne veiligheid en binnenlandse autonomie, als met het oog op de verdere versterking van dit hoogtechnologische en veelbelovende ecosysteem.

Met een duidelijke strategische focus, een sterke onderzoeksbasis en een ondernemend kmo-landschap is Vlaanderen goed gepositioneerd om een sleutelrol te blijven spelen in de Europese en internationale C-UAS-markt. Door gerichte investeringen, beleidsmatige ondersteuning en verdere versterking van publiek-private samenwerking kan dit ecosysteem uitgroeien tot een volwaardige aanbieder van geïntegreerde C-UAS-oplossingen. Een goed functionerend triple-helixmodel — de samenwerking tussen overheid, industrie en kennisinstellingen — is hierbij essentieel.

Een toekomstbestendig C-UAS-ecosysteem vergt meer dan losse initiatieven of gefragmenteerde projecten. Er is behoefte aan een gecoördineerde, samenhangende en strategische samenwerking tussen alle betrokken actoren. Dit houdt in dat bottom-up initiatieven van bedrijven en onderzoekscentra nauw moeten worden afgestemd op top-downbeleid en ondersteuning vanuit zowel civiele als militaire overheden. Zonder deze wederzijdse afstemming dreigt versnippering, en blijven schaalvergroting en markttoegang uit.

Daarnaast is het van cruciaal belang dat civiele en militaire autoriteiten actief samenwerken met de industrie aan de ontwikkeling van test- en evaluatie-infrastructuur. Dergelijke faciliteiten vormen immers een noodzakelijke schakel in het versnellen van technologische innovatie en de vertaling ervan naar operationele toepassingen en marktintroductie.

Kortom, een sterk verankerde triple-helixwerking is cruciaal voor de verdediging van onze strategische belangen in het C-UAS-domein. Maar mét een goed georganiseerde en gedragen samenwerking tussen overheid, industrie en kennisinstellingen ligt er een duidelijke opportuniteit om niet alleen bij te blijven, maar ook een voortrekkersrol te spelen in Europa.

5 Innovatiekansen

5.1 Orientatie Roadmap – Schematisch

Counter-UAS					
Focuslaag	Detectie	Identificatie	Tracking	Neutralisatie	Command & Control
Bouwsteen	Systemen die verschillende soorten drones — van consumentendrones tot meer gesofisticeerde, autonome platforms — kunnen detecteren, en kunnen ingezet worden in uiteenlopende operationele omgevingen	Identificatie vormt de brug tussen detectie en besluitvorming, en is cruciaal om te bepalen of een gedetecteerde drone legaal actief is of mogelijk een bedreiging vormt	Waar detectie het moment van waarneming markeert en identificatie duidelijkheid schept over het type of de intentie van een drone, stelt tracking ons in staat om de bewegingen van een toestel continu te volgen. Dit is essentieel om de dreiging in real-time te evalueren, effectors correct te positioneren, en incidenten tijdig te escaleren of de-escaleren	Geavanceerde neutralosatie technologieën die flexibel zijn en up-to date met de hybriede en snel evoluerende UAS dreiging	Geautomatiseerde bedreigingsanalyse en Command & Control ondersteuning

5.2 Toekomstige noden in UAS-detectie

Thematische Doelstellingen

- **Sensorfusie:** waarbij radar, radiofrequentiedetectie, elektro-optische/IR-camera's, akoestische sensoren en zelfs netwerksensoren (zoals mobiele telefonie- of Wi-Fi-sniffers) gecombineerd worden;
- **Adaptieve detectiesystemen.** die in staat zijn om te leren en zich aan te passen aan nieuwe dreigingsprofielen, onder andere via artificiële intelligentie en machine learning;

Naarmate het gebruik van drones blijft toenemen, groeit ook de nood aan geavanceerde detectiecapaciteiten binnen het C-UAS-domein. Detectie vormt de eerste en cruciale schakel in de detectie-identificatie-neutralisatieketen, en bepaalt in grote mate de effectiviteit van het volledige C-UAS-systeem. In de toekomst zal er een duidelijke nood zijn aan systemen die niet alleen verschillende soorten drones — van consumentendrones tot meer gesofisticeerde, autonome platforms — kunnen detecteren, maar ook in uiteenlopende operationele omgevingen kunnen functioneren: stedelijk, ruraal, maritiem en zelfs in conflictzones.

Evolutie naar multi-sensor integratie: Een belangrijke technologische trend is de toenemende integratie van verschillende detectietechnologieën in één systeem. Enkelvoudige detectiesystemen zoals radar of RF-scanners zijn vaak beperkt in bereik, nauwkeurigheid of bruikbaarheid in complexe omgevingen. De toekomst ligt in sensorfusie, waarbij radar, radiofrequentiedetectie, elektro-optische/IR-camera's, akoestische sensoren en zelfs netwerksensoren (zoals mobiele telefonie- of Wi-Fi-sniffers) gecombineerd worden. Door deze sensoren in real-time te laten samenwerken via slimme algoritmes, kan de nauwkeurigheid van

- **Gedistribueerde, netwerkgebaseerde detectiecapaciteiten** die grotere gebieden dekken met ingebouwde redundantie en dynamische operationele beeldvorming

detectie sterk worden verhoogd, worden valse positieven geminimaliseerd en wordt een beter tactisch overzicht gecreëerd.

Adaptiviteit en AI-ondersteunde detectie: Met de opkomst van autonome en zwak signaalgevende drones, zoals UAS met low observable profielen of die opereren buiten standaard frequentiebanden, wordt er een groeiende behoefte aan adaptieve detectiesystemen. Deze systemen moeten in staat zijn om te leren en zich aan te passen aan nieuwe dreigingsprofielen, onder andere via artificiële intelligentie en machine learning. AI-ondersteunde detectie maakt het mogelijk om patronen te herkennen, onbekende objecten te classificeren en contextuele anomalieën te detecteren — cruciale eigenschappen in een tijd waarin drones snel evolueren en steeds minder voorspelbaar worden ingezet.

Netwerk-gebaseerde en gedistribueerde detectie: In plaats van te vertrouwen op centrale systemen, zullen toekomstige C-UAS-oplossingen steeds vaker gebruikmaken van gedistribueerde, netwerkgebaseerde detectiecapaciteiten. Dit laat toe om dekking te bieden over grotere gebieden, redundantie in te bouwen en een dynamischer operationeel beeld te vormen. Zulke systemen kunnen ook mobiel zijn — denk aan snel inzetbare sensorkits op voertuigen, of tijdelijke installaties bij evenementen of op kritieke infrastructuren — en zo inspelen op de toenemende mobiliteit en onvoorspelbaarheid van dronebedreigingen.

5.3 Toekomstige evoluties op gebied van identificatie

Thematische Doelstellingen

- **Protocolgebaseerde identificatiesystemen,** met aandacht voor de uitdagingen rond interoperabiliteit, cybersecurity, en dekking in gebieden met zwakke connectiviteit, taktische en niet-cooperatieve omgevingen;
- **Elektronische transponders of ID-modules** met focus op op miniaturisatie, versleuteling van data en het mogelijk maken van dual-mode zenders (zowel actieve als passieve modi), zodat drones zich ook in complexere of verstoorde omgevingen betrouwbaar kunnen identificeren;
- **Visuele identificatie** met behulp van AI en beeldanalyse;

Identificatie vormt de brug tussen detectie en besluitvorming, en is cruciaal om te bepalen of een gedetecteerde drone legaal actief is of mogelijk een bedreiging vormt. In de toekomst zal het niet langer volstaan om een drone *te zien* of *te detecteren*; er zal ook snel moeten worden vastgesteld *wie* de operator is, *wat* het toestel doet, en of het zich aan de regels houdt.

Protocolgebaseerde identificatie en Remote ID: Een van de belangrijkste ontwikkelingen op korte termijn is de bredere uitrol en verfijning van protocolgebaseerde identificatiesystemen, met als bekend voorbeeld Remote ID. Dit systeem verplicht drones om tijdens de vlucht unieke identificatie-informatie uit te zenden via gestandaardiseerde communicatieprotocollen. Deze informatie kan door bevoegde instanties worden opgevangen en gebruikt om de operator, het toesteltype en de vluchtstatus te identificeren. Hoewel Remote ID op termijn in heel Europa verplicht wordt, blijven er uitdagingen rond interoperabiliteit, cybersecurity, en dekking in gebieden met zwakke connectiviteit. In de toekomst zal het belangrijk zijn dat deze systemen ook kunnen functioneren in tactische of non-coöperatieve omgevingen.

Transponders en elektronische ID-modules: Voor professioneel en gereguleerd droneverkeer zullen elektronische transponders of ID-modules een sleutelrol blijven spelen. Deze compacte modules zenden continu identificatie- en locatiegegevens uit, vergelijkbaar met ADS-B in de bemande luchtvaart. Technologische vooruitgang richt zich hier op miniaturisatie, versleuteling van data en het mogelijk maken van 'dual-mode' zenders (zowel actieve als passieve modi), zodat drones zich ook in complexere of verstoorde omgevingen betrouwbaar kunnen identificeren.

- **Radiofrequentie-signatuurherkenning,** waarbij drones worden geïdentificeerd op basis van unieke kenmerken in hun radiosignaal. Iedere drone zendt, vaak onbewust, een specifieke 'RF-vingerafdruk' uit, afhankelijk van de gebruikte elektronica, firmware en communicatieprotocollen.

In de toekomst zullen deze modules mogelijk verplicht worden voor vluchten in hogere risicocategorieën of in gecontroleerd luchtruim, zoals boven stedelijke gebieden of kritieke infrastructuur.

Visuele en elektro-optische identificatie: In omgevingen waar op radiofrequentie gebaseerde identificatiemiddelen niet beschikbaar zijn — bijvoorbeeld bij kwaadwillige of zelfgebouwde drones — wordt visuele identificatie steeds belangrijker. Geavanceerde camera- en sensoroplossingen maken het mogelijk om drones op afstand visueel te herkennen, met behulp van AI en beeldanalyse. Denk hierbij aan het automatisch herkennen van types, afmetingen, gedragspatronen of zelfs kleine merktekens op het toestel. De uitdaging ligt hier vooral in de prestaties bij slechte lichtomstandigheden, hoge snelheden en het onderscheiden van sterk op elkaar lijkende modellen.

RF-signatuurherkenning en gedragspatronen: Een andere veelbelovende technologie is radiofrequentie-signatuurherkenning, waarbij drones worden geïdentificeerd op basis van unieke kenmerken in hun radiosignaal. Iedere drone zendt, vaak onbewust, een specifieke 'RF-vingerafdruk' uit, afhankelijk van de gebruikte elektronica, firmware en communicatieprotocollen. Door deze patronen te analyseren en te vergelijken met gekende databanken, kunnen zelfs non-coöperatieve drones worden geïdentificeerd. In de toekomst zal deze techniek waarschijnlijk verder worden gecombineerd met gedragsanalyse, waarbij afwijkende vliegroutes, vluchtprofielen of respons op verstoringen extra indicaties geven over de aard en intentie van het toestel.

Naar een multimodale identificatie-aanpak: De complexiteit van het huidige en toekomstige UAS-landschap vereist een multimodale identificatie-aanpak, waarbij meerdere technologieën — protocol gebaseerd, RF-analyse, visuele herkenning en transponders — gecombineerd worden in één geïntegreerd systeem. Alleen zo kan men tot een hoge mate van betrouwbaarheid, snelheid en contextafhankelijke beoordeling komen. Vlaanderen beschikt vandaag reeds over sterke competenties in deze domeinen, maar blijvende investeringen in interoperabiliteit, standaardisatie en testinfrastructuur zullen nodig zijn om deze technologieën succesvol en schaalbaar te implementeren.

5.4 Tracking als essentiële schakel in C-UAS

Thematische Doelstellingen

- Triangulatie is één van de fundamentele trackingmethodes om nauwkeurige realtime positiebepaling te doen, dit vereist echter een netwerk van goed gesynchroniseerde detectiepunten, wat uitdagingen stelt in stedelijke of afgelegen gebieden;
- De vooruitgang in **pulse-Doppler radar, frequency-modulated continuous wave (FMCW) en multi-beam tracking** stelt systemen in staat om zowel de snelheid als de richting van drones nauwkeurig te bepalen, ook in omgevingen met veel visuele of elektromagnetische ruis;
- **Niet-rotatieve radararrays** (non-rotating radar arrays), zoals actieve elektronische gestuurde arrays (AESA). In tegenstelling tot traditionele, mechanisch draaiende radars kunnen deze systemen blijvend "staren" naar een object en zo een continue, hoge-resolutie opvolging garanderen;
- De toekomst van drone tracking ligt in **volledig geïntegreerde, autonome trackingmodules** die gebruikmaken van multi-sensorfusie, AI en real-time dreigingsanalyse. Zulke systemen combineren triangulatie, radar, visuele input en RF-analyse om een compleet en dynamisch luchtbeeld te genereren

Binnen een geïntegreerd C-UAS-systeem speelt drone tracking een cruciale rol. Waar detectie het moment van waarneming markeert en identificatie duidelijkheid schept over het type of de intentie van een drone, stelt tracking ons in staat om de bewegingen van een toestel continu te volgen. Dit is essentieel om de dreiging in real-time te evalueren, effectors correct te positioneren, en incidenten tijdig te escaleren of de-escaleren. Naarmate drones kleiner, sneller en autonomer worden, groeit de technologische complexiteit van trackingmethodes.

Triangulatie: ruimtelijke positionering via sensorfusie: Een van de fundamentele trackingmethodes is triangulatie, waarbij de positie van een drone wordt bepaald op basis van signalen die worden opgevangen door meerdere sensoren, verspreid over een gebied. Door het meten van verschillen in aankomsttijd of signaalsterkte tussen deze sensoren, kan het systeem de exacte positie en bewegingsrichting van een toestel berekenen. Deze techniek vereist echter een netwerk van goed gesynchroniseerde detectiepunten, wat uitdagingen stelt in stedelijke of afgelegen gebieden. Desondanks blijft triangulatie, zeker in RF-gebaseerde systemen, een kostenefficiënte en breed inzetbare methode die ook werkt bij passieve detectie van non-coöperatieve drones.

Radar blijft kerntechnologie voor dynamische tracking: Radartechnologie vormt nog steeds de ruggengraat van veel trackingoplossingen, met name in situaties waar RF-signalen ontbreken of onbetrouwbaar zijn. Moderne radarsystemen zijn in staat om zelfs kleine, snel bewegende drones te onderscheiden van vogels of andere objecten, dankzij hogere frequenties en geavanceerde signaalverwerking. De vooruitgang in pulse-Doppler radar, frequency-modulated continuous wave (FMCW) en multi-beam tracking stelt systemen in staat om zowel de snelheid als de richting van drones nauwkeurig te bepalen, ook in omgevingen met veel visuele of elektromagnetische ruis.

Niet-rotatieve radararrays en het "staren" naar drones: Een belangrijke technologische doorbraak binnen radartracking is de opkomst van niet-rotatieve radararrays (non-rotating radar arrays), zoals actieve elektronische gestuurde arrays (AESA). In tegenstelling tot traditionele, mechanisch draaiende radars kunnen deze systemen blijvend "staren" naar een object en zo een continue, hoge-resolutie opvolging garanderen. Dit maakt het mogelijk om drones zeer nauwkeurig te volgen, zelfs wanneer ze zich snel verplaatsen of complexe manoeuvres uitvoeren. Bovendien kunnen deze arrays meerdere doelen tegelijk volgen, snel overschakelen tussen sectoren en zijn ze minder onderhoudsgevoelig dan hun roterende tegenhangers. Deze technologie wordt als sleutelinnovatie beschouwd voor toekomstige high-performance C-UAS-oplossingen, zeker in combinatie met AI-gestuurde trackinglogica.

Geïntegreerde en autonome tracking: De toekomst van drone tracking ligt in volledig geïntegreerde, autonome trackingmodules die gebruikmaken van multi-sensorfusie, AI en real-time dreigingsanalyse. Zulke systemen combineren triangulatie, radar, visuele input en RF-analyse om een compleet en dynamisch luchtbeeld te genereren. Hierdoor kunnen beslissingen sneller en betrouwbaarder genomen worden, en kan men in

reële tijd inspelen op veranderende situaties. Voor Vlaanderen liggen hier kansen in de verdere ontwikkeling van innovatieve tracking-algoritmen, modulaire radaroplossingen en de integratie ervan in inter-operabele C2-systemen.

5.5 Evoluerende dreiging vraagt om geavanceerde neutralisatietechnologie

Thematische Doelstellingen

- Een van de meest veelbelovende en snel evoluerende technologieën zijn **hunter-killer drones**, zijnde autonome of semi-autonome toestellen fungeren als mobiele interceptoren die vijandige drones kunnen detecteren, achtervolgen en uitschakelen in real-time, Ze bieden een uitzonderlijke responsiviteit, precisie en reikwijdte, zeker in scenario's waar vaste systemen onvoldoende dekking bieden;
- De ontwikkeling en inzet van **high-power microwave (HPM)** technologie voor de neutralisatie van drones, systemen die krachtige microgolfpulsen uitzenden die de elektronica van drones kunnen verstoren of permanent uitschakelen, het grote voordeel van microgolfwapens is hun capaciteit om meerdere doelen tegelijk te treffen, wat ze bijzonder geschikt maakt tegen dronezwermen,
- **Combinatie van multi-target tracking, AI-gestuurde bedreigingsanalyse en parallelle neutralisatietechnieken** zoals HPM-systemen, hunter-killer drones in zwermconfiguratie, en zelfs toekomstige lasergebaseerde systemen

Met de groei van het dronegebruik neemt ook de complexiteit van de dreiging toe. Waar traditionele C-UAS-systemen zich vaak richtten op het uitschakelen van individuele, relatief eenvoudige drones, zien we vandaag een opkomst van gecoördineerde aanvallen door dronezwermen, autonome vluchten, en toestellen die gebruikmaken van stealth-technieken of onconventionele communicatiemethoden. Dit dwingt de industrie en overheden om hun neutralisatiemethoden te herdenken en te investeren in geavanceerdere, flexibele systemen.

Interceptor drones: mobiele neutralisatie in real-time: Een van de meest veelbelovende en snel evoluerende technologieën zijn interceptor drones. Deze autonome of semiautonome toestellen fungeren als mobiele interceptoren die vijandige drones kunnen detecteren, achtervolgen en uitschakelen in real-time. Ze kunnen uitgerust worden met diverse effectoren: van netwerpsystemen voor het fysiek vangen van drones, tot kinetische projectielen of verstoringsmodules. Omdat ze zelf mobiel zijn en opereren in dezelfde driedimensionale ruimte als hun doelwitten, bieden ze een uitzonderlijke responsiviteit, precisie en reikwijdte, zeker in scenario's waar vaste systemen onvoldoende dekking bieden. Hunter-killer drones zijn bij uitstek geschikt voor bescherming van kritieke infrastructuur, mobiele troepen en tijdelijke evenementenlocaties.

Microgolftechnologie: gerichte energie tegen elektronica: Een tweede belangrijke trend is de inzet van high-power microwave (HPM)-technologie voor de neutralisatie van drones. Deze systemen zenden krachtige microgolfpulsen uit die de elektronica van drones kunnen verstoren of permanent uitschakelen. Het grote voordeel van microgolfwapens is hun capaciteit om meerdere doelen tegelijk te treffen, wat ze bijzonder geschikt maakt tegen dronezwermen. Bovendien gebeurt de neutralisatie zonder fysiek contact of kinetisch effect, wat de kans op nevenschade beperkt. De technologie staat nog in ontwikkeling, maar wordt al getest in militaire contexten en als onderdeel van mobiele C-UAS-platformen. Belangrijke uitdagingen zijn de energiebehoefte, gerichte focus (om nevenschade te vermijden) en robuustheid tegen atmosferische invloeden.

Neutralisatie van dronezwermen: schaalbare en simultane respons: De opkomst van **drones die in zwermen opereren** — met gedeelde besturing of autonome coördinatie — vormt een van de grootste uitdagingen voor C-UAS-systemen. Klassieke effectors zoals jammers of netkanonnen zijn vaak onvoldoende schaalbaar of traag om meerdere doelen tegelijk aan te pakken. Nieuwe benaderingen combineren daarom **multi-target tracking**, AI-gestuurde bedreigingsanalyse en parallelle neutralisatietechnieken. HPM-systemen, interceptor drones in zwermconfiguratie, en zelfs toekomstige laser-gebaseerde systemen worden beschouwd als kerntechnologieën om deze bedreiging te counteren. Een effectief anti-

zwermsysteem zal bovendien afhankelijk zijn van een krachtige C2-architectuur die snel prioriteiten kan stellen, middelen toewijst en beslissingen automatiseert

5.6 Command & Control

Thematische Doelstellingen

- Systemen die maken gebruik van artificiële intelligentie, patroonherkenning en machine learning om snel en accuraat verdachte vluchten te classificeren, risico's in te schatten en aanbevelingen te formuleren voor passende responsacties. Ze ondersteunen de commandanten en operatoren in real-time door het aanleveren van contextuele beslissingsinformatie, inclusief scenario-afwegingen, risicoprofielen en inzetopties

Bedreigingsanalyse tool: Menselijke operators – zelfs wanneer zij zeer goed getraind zijn – kunnen niet consistent het tempo en het volume van asymmetrische drone-dreiging bijhouden in complexe omgevingen zoals stedelijke gebieden, luchthavens of gevechtszones. Automatisering en AI-gestuurde dreigingsevaluatie zijn dan ook geen luxe, maar essentiële vermenigvuldigers. Bovendien, naarmate drone-activiteit steeds frequenter voorkomt in het civiele luchtruim, groeit de noodzaak voor schaalbare, consistente en juridisch verdedigbare dreigingsbeoordelingen. Een robuust risicoanalyse-instrument voor dreigingen zorgt ervoor dat beveiligingsbeslissingen — zoals het inzetten van kinetische of elektronische tegenmaatregelen — gebaseerd zijn op duidelijke, transparante en controleerbare criteria. Dit verkleint het risico op onterechte onderscheppingen, nevenschade of juridische aansprakelijkheid.

Een goed ontworpen C-UAS bedreigingsanalyse tool vormt het brein van elk counter-UAS C2 systeem. Het vormt de basis voor proportionele, geïnformeerde en tijdige reacties op een dreigingslandschap dat zowel dynamisch als potentieel bedreigend is. Deze C-UAS bedreigingsanalyse tool mag dus terecht beschouwd worden als een essentieel onderdeel van moderne C-UAS systemen. Dergelijke tools bieden real-time situationeel bewustzijn, dynamische dreigingsscores en bruikbare beslissingsondersteuning aan operators en commandanten in zowel de militaire als de civiele sector.

- **Multi-sensor based**: Een modern risicoanalyse-instrument voor C-UAS (Counter-Unmanned Aircraft Systems) combineert de input van meerdere soorten sensoren met artificiële intelligentie om het dreigingsniveau van de gedetecteerde drones te classificeren op basis van intentie, gedrag, locatie, nabijheid van kritieke objecten en bekende dreigingspatronen.
- **Historische data:** Daarnaast moet het systeem live inlichtingen kunnen aftoetsen aan historische incidentgegevens en gedragsmodellen. Via machine learning past de tool zich continu aan op basis van nieuwe en veranderende drone-tactieken.
- **Machinesnelheid:** Cruciaal is dat het systeem op machinesnelheid moet kunnen opereren. Aangezien drones zich met hoge snelheid kunnen verplaatsen, vaak slechts kort in de lucht zijn en hun missie binnen enkele minuten of zelfs seconden kunnen uitvoeren, betekent elke vertraging in de dreigingsanalyse een directe toename van het risico op missie-uitval, fysieke schade of juridische fouten.

Command & Control: De ontwikkeling begint met een grondig begrip van de operationele vereisten en de dreigingsomgevingen. Dit vereist nauwe samenwerking met eindgebruikers (zoals strijdkrachten, luchthavenbeveiliging, politie) om het volgende vast te stellen:

- **Dreigingstypen** (bijv. hobbydrones, zwermen, vastevleugeldrones)
- **Eisen aan responstijd**
- **Rules of Engagement** (regels voor inzet van tegenmaatregelen)
- **Behoefte aan integratie** met bestaande systemen (bijv. radar, nationale luchtverkeersbewaking)

Op basis hiervan wordt een **Concept of Operations (CONOPS)** opgesteld, dat beschrijft hoe het C2-systeem zal functioneren onder verschillende dreigingsscenario's (bijv. perimeterinbraak, bescherming van kritieke infrastructuur).

Integrated Air Picture (IAP): Een betrouwbare, overzichtelijke **'Integrated Air Picture'** is van cruciaal belang binnen een robuuste C2-oplossing voor C-UAS, omdat het de brug vormt tussen complexe sensorinvoer en menselijke besluitvorming. Een effectieve IAP integreert gegevens van uiteenlopende bronnen — zoals radar, RF-detectoren, EO/IR-camera's, akoestische sensoren en ADS-B-/transpondersignalen — in een sensorfusie-engine die de ruwe data consolideert tot één overzichtelijk luchtbeeld. Door het elimineren van valse meldingen en het verhogen van de betrouwbaarheid van dreigingsherkenning, ontstaat een operationeel beeld waarop operators kunnen vertrouwen.

De **human-machine interface (HMI)** speelt hierin een sleutelrol. Deze moet het luchtbeeld in real-time weergeven via een intuïtieve 2D- of 3D-kaart, waarbij potentiële dreigingen worden gemarkeerd met kleur gecodeerde risiconiveaus. Het systeem moet meerdere doelen gelijktijdig kunnen volgen, waarschuwingen genereren en context specifieke aanbevelingen doen. Omdat drones zich snel ontwikkelen en inzetten in zowel civiele als militaire omgevingen, moet de IAP flexibel zijn afgestemd op het gebruiksdoel — gebruiksvriendelijk en toegankelijk voor civiele veiligheidsteams, en tactisch gedetailleerd voor militaire commandanten.

Een krachtige IAP stelt operators in staat om snel inzicht te krijgen in een veranderende dreigingssituatie en adequaat te reageren — wat het verschil kan maken tussen een succesvolle interceptie en een gemiste dreiging.

Activatie van neutralisatie middelen en effectoren: Een volledig geïntegreerde, AI-gestuurde C2-oplossing maakt zowel geautomatiseerde als handmatige activering van tegenmaatregelen mogelijk.

Het C2-systeem moet acties veilig op elkaar afstemmen (deconflicteren), het wettelijk en juridisch kader respecteren (vooral in civiele omgevingen), en zorgen voor een correcte coördinatie tussen systemen. Daarnaast kan het systeem worden geïntegreerd met commandonetwerken van politie of defensie om waarschuwingen door te geven en ondersteuningseenheden in te schakelen.

6 Conclusie

Waar drones aanvankelijk vooral werden ingezet voor commerciële en recreatieve doeleinden, zijn ze vandaag uitgegroeid tot strategische actoren binnen een steeds complexer luchtruim. Deze evolutie brengt onmiskenbare voordelen met zich mee — efficiëntie, innovatie en nieuwe economische mogelijkheden — maar creëert tegelijk aanzienlijke veiligheidsuitdagingen. De stijgende incidentiegraad, het toenemende aantal niet-coöperatieve vluchten en de opkomst van drones als potentieel wapensysteem maken duidelijk dat een geïntegreerde benadering van detectie, identificatie en neutralisatie onontbeerlijk is.

In de civiele context ligt de nadruk op het beschermen van burgers, infrastructuur en luchtruimintegriteit. Het groeiende aantal incidenten boven luchthavens, stedelijke gebieden en kritieke installaties toont aan dat bestaande veiligheidskaders ontoereikend zijn. C-UAS-systemen vormen een cruciale schakel in het verzekeren van openbare veiligheid en operationele continuïteit.

In de militaire context is de rol van drones fundamenteel veranderd: van observatieplatforms tot tactische wapensystemen. De asymmetrische aard van de UAS-dreiging vraagt om een flexibele systemen die vaste installaties, mobiele eenheden en individuele militairen beschermen.

Deze systemen moeten flexibel inzetbaar zijn, interoperabel met luchtverkeersbeheersystemen en afgestemd op zowel preventieve als reactieve maatregelen. Door investeringen in slimme sensoren, AI-gestuurde analyses en gestandaardiseerde communicatieprotocollen kan de luchtveiligheid op een toekomstbestendige manier worden versterkt. De geografische gelaagdheid moet worden ondersteund door een robuuste commandostructuur die data, besluitvorming en actie in real time verbindt.

België en Vlaanderen bevinden zich in een unieke positie om hierin een voortrekkersrol te spelen. Dankzij een sterk technologisch ecosysteem, innovatieve kmo's en toonaangevende kennisinstellingen beschikt Vlaanderen over de bouwstenen om geïntegreerde C-UAS-oplossingen te ontwikkelen en te exporteren. Door de samenwerking tussen overheid, industrie en onderzoek te versterken - volgens het triple-helixmodel - kan dit ecosysteem uitgroeien tot een strategische pijler van zowel nationale veiligheid als economische groei. Een gecoördineerde, langetermijnaanpak die civiele en militaire belangen verenigt, zal niet enkel bijdragen aan een veiliger luchtruim, maar Vlaanderen ook positioneren als een sleutelspeler in de Europese C-UAS-innovatieagenda.

Impulsprogramma Defensie

Oriëntatieroadmap

AI for Defence

Authored by Imec

on the request of the

Departement Werk, Economie,

Wetenschap, Innovatie &

Sociale Economie

October 2025

Contents

A Vision & Context on AI for Defence

"AI & Defence, in an EU and NATO context "

Artificial intelligence (AI) has become omnipresent in today's world, and it is foreseen that its importance will only grow in the future. Over the last years we have seen a wide adoption of AI across various domains and applications, penetrating the entire spectrum of society, economy and government. One can thereby think of a plethora of specific use cases and wider domains being impacted. Examples are (semi)-autonomous driving and mobility, healthcare (e.g., medical imaging), business optimization, government interactions with citizens, optimized process logistics, agricultural precision activities and so on. The wide applicability of the potential of AI also leads to a direct understanding of the impact that it can offer to defence and security. Indeed, many of today's civil AI applications are also relevant from a defence and security point of view. Additionally, there are defence specific use cases, being driven by the specific context of Defence and military operations (Haldorai et al., 2024). Today's regional conflicts, with a global impact, such as the ongoing Ukraine-Russia war as well as the conflicts in the Middle East demonstrate the relevancy and importance of AI being used in various (e.g., target recognition, de-mining) situations. One can thus fairly conclude that **AI, in its wide context, is strongly impacting defence, and should hence be adopted across the various layers of a defence ecosystem – both from governmental and economic points of view, while being embedded in the international context.**

AI can be considered as an enabling technology strongly related to other technologies and domains: It is not a standalone technology, but it is intertwined with specific use cases and applications that set boundary conditions, have specific objectives and data limitations and constraints. Furthermore, AI has become an umbrella term for a broad range of different families of algorithms and techniques. Additionally, AI algorithms not only rely on application parameters but are also dependent on other technologies such as compute infrastructure, sensor systems, and communication backbones. These interdependencies must be acknowledged and understood within a military context, which is why the Roadmap also incorporates references to this broader ecosystem through the four proposed "Focus Elements" and their corresponding "Building Blocks" described in this document.

Despite the potential and success stories of AI, one should not be blind to risks that are coupled to this technology such as bias, errors, and the lack of transparency. The above-mentioned challenges only grow stronger in a security context where any vulnerability will be exploited. On top, additional constraints and complexities arise from this specific context: Can we trust open-source models? How to define bias, error and transparency in a military context compared to a civil context, and what is the impact of applying a civil-military perspective on those concepts? How can data infrastructures – strongly required for optimally functioning AI –, both from a hardware and software point of view, be designed in a context of rising transatlantic questions, thus strengthening European sovereignty?

To provide defence and security actors with the required AI capabilities, and solve the aforementioned challenges, there is a clear need for innovation and triple helix collaboration across military specialists, industry and knowledge centers. However, **the broadness of AI, and**

the challenging context, force us to be selective in the areas where Flanders can create significant impact or where there is a need for national autonomy.

However, similar to other (security) technologies, Europe lags behind compared to the US and China in terms of innovation, in particular when it comes to defence – as also indicated by the Draghi Report. This is not different for AI and its related infrastructure (Draghi, 2024). It must nevertheless be recognized and underlined that the European Commission, together with the Member States, is taking action both from a policy development and implementation point of view. Initiatives include the European AI Continent Action Plan (European Commission, 2025a), and the recent Apply AI Strategy (European Commission, 2025b), leading to the set-up of – for example – European AI Factories, related Antennas, and AI Gigafactories. Nevertheless, it should also be underlined that **continuous support for innovation and infrastructure will be required**.

Whereas in the past a dual-use perspective was applied whereby innovation from a military perspective would influence innovation in the civil world, the perspective is now being turned around. Indeed, many solutions to technological and innovative defence issues come from civilian non-traditional defence industry players (dual use) and are also cost-effective. **It is from this point of view that the Flemish government, via its administration is working towards the following goal: "*Promote, stimulate and support security and defence industry and innovation in Flanders which contributes to the Flemish, Belgian, European and transatlantic technological and industrial defence base.*"**, to contribute positively from Flanders to a geopolitically turbulent context, with a view to strengthening Flemish players in this domain. In this way, we strengthen innovation and our industry in Flanders (in line with the Flemish Coalition Agreement), ensuring a more competitive region.

The implementation of this goal runs via the so-called "Impulsprogramma Veiligheid en Defensie", mobilizing resources for a decisive policy focused on innovation and industry, working both horizontally and vertically. If we want to strengthen the defence industry in Flanders and boost defence innovation, a long-term strategy is needed. The Impulse Program articulates this long-term strategy, translating how the freed-up resources will be used, through which governance and how this aligns and connects to the federal, European and international initiatives and value chains. There is also a focus on better aligning current policy with today's defence challenges.

Within this Impulse Program, several domains have been selected:

- Horizontally speaking:
    - EDTs (Enabling Digital Technologies) – AI, autonomy, biotech and hypersonics
    - Cybersecurity
    - Energy, environment and geo-intelligence
- Vertically speaking:
    - Aviation & (C-)UAVs ((Combat) Unmanned Aerial Vehicles)
    - Space
    - Maritime

For each of those domains a first analysis of the economic landscape in Flanders has been conducted, and a roadmap has been designed based on existing needs matched with the potential contribution from a Flemish economical ecosystem.

This document presents the Ecosystem and Roadmap for AI, and continues as follows: Firstly, the ecosystem analysis and results are presented, followed by the roadmap which consists of four focus elements and 14 dedicated building blocks.

Flemish AI – Defence Ecosystem

As indicated in the previous section, this exercise consists of three interrelated elements, whereby **mapping the existing Flemish private AI ecosystem was the first element to be undertaken to understand the ecosystem**. This section describes firstly the methodological approach applied, and, secondly, the main lessons learned from this existing ecosystem. Given the orientation on the intersection between AI on the one hand, and security & defence activities on the other hand, it resulted in a solid basis of understanding the private actors active on this intersection. Nevertheless, it should be emphasized that, besides present companies active in the security & defence domain, there is also the wider potential of AI companies active in civil-oriented domains.

Methodology & categorisation of the Flemish industrial AI ecosystem

A first step in the ecosystem mapping was defining a solid categorisation that would encompass both the complexity of the concept of AI, thereby considering the various supporting elements it can offer, its technical complexity, and the current identified challenges and needs. For the first element, we relied on the solid expertise available within Imec. For the second element, a first needs assessment was made based on existing literature, including the European Defence Fund opportunities and funded calls.

In total **we have defined six categories to cluster the various expertise domains of the Flemish industrial base:**

1. **Decision support, models, data science, ML**: Companies focussing on a range of high-level software services and functionalities, including but not solely referring to the use and development of AI-driven predictive and prescriptive models, data science technologies and solutions, and machine learning (ML) techniques to support decision-making. Those companies can for example offer tools to support more informed, data-driven decisions.
2. **AI compute**: Companies that focus on the different aspects and functionalities to optimize the workloads of various AI and software on underlying hardware and infrastructure. This can both be from a hardware perspective (e.g., ASIC design, Graphics Processing Unit (GPU)) or software perspective (deployment, training, running of models). Similar, the scale and size can vary from single-chip, edge equipment to larger (cloud) infrastructure.
3. **AI for Communication**: Companies that focus on (intelligent) radio spectrum and telecommunication related activities, particularly for communication, monitoring, and localization across various wired and wireless technologies.
4. **Intelligent sensing**: Companies that work on (parts of) the pipeline for intelligent perception using all kinds of sensors. This starts from algorithms for low-level sensor processing, sensor fusion, up to the (possible) independent software layers and AI algorithms for perception tasks.
5. **Simulations**: Companies focussing on everything related to simulations and digital twins for various purposes including, synthetic data generation, large-scale modelling (e.g., wargames) etc.

6. **Human-AI interaction**: Companies focussing on improving Human-Machine interaction using AI and related technologies. Examples are XR technologies, and chatbots/NLP.

Those six categories where then applied to several identified overview documents and the list of companies active in the field of AI and/or active in the field of security & defence. A detailed listing of the analysed documents can be found in Annex 1 of this Roadmap. Note that topics such as robotics can span across multiple categories. As such, the companies engaged in these areas can be listed under several categories.

Finally, it is important to highlight that **this exercise was conducted in April and May 2025**. The ecosystem of AI-related companies in Flanders is actively evolving and the overall list should therefore be maintained and considered a first starting point. Nevertheless, the overview of the lessons learned is valid and provides insights in the main strengths, as well as weaknesses, of the currently existing AI ecosystem.

Results of the Flemish industrial AI ecosystem analyses

This Section provides an overview of the key lessons on the AI – defence & security ecosystem currently present in Flanders.

First an overview of the information collected is provided, followed by a number of conclusions to be drawn from those results.

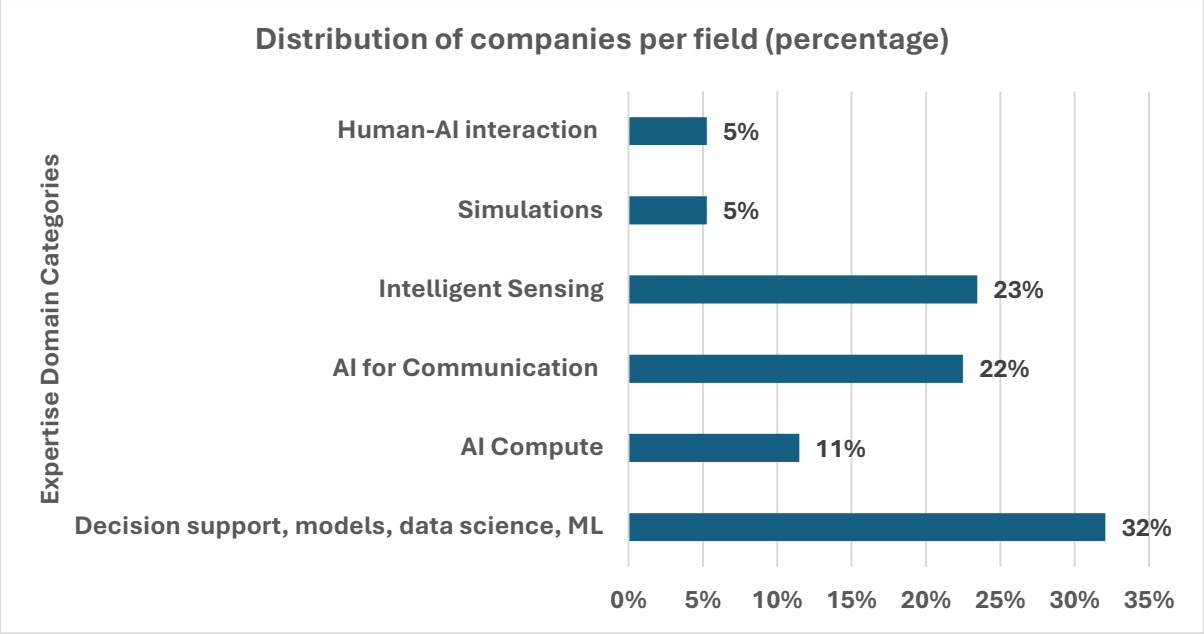
In total, 227 companies have been identified within the Flemish region. If the Brussels area is also included[1], the number increases to 270 companies. Based on the above perspective on the defence/security-AI label, and only referring to companies based in the Flemish region, we see the following numbers:

1. EDF Brokerage Event participation / AGORIA BDSi participation / participation to know defence project: 83 companies
2. A public connection to defence / security, but not part of the previous category: 5 companies
3. Related to AI, but no connection to defence / security: 139 companies

Looking into the **connection towards the AI domain** in which those companies are active, and again only for companies located in the Flemish region, gives the following view:

1. Decision support, models, data science, ML: 67 companies
2. Intelligent Sensing: 49 companies
3. AI for Communication: 47 companies
4. AI Compute: 24 companies
5. Simulations: 11 companies
6. Human-AI interaction: 11 companies

[1] Given the close proximity of Brussels and the fact that several companies have a seat in Brussels, it was decided to include this information as well.



Furthermore, around 18 companies could not be linked to a specific AI element, and around half of the companies was also connected to (a) secondary domain(s) (domains listed above). This last element can be understood as a sign of the variation available in the market.

Key Lessons Learned

The following insights can be drawn from this ecosystem activity mapping:

1. **While a solid group of companies is already today active on the intersection between defence / security and AI, more than half of the companies is not yet – publicly – active in the field, demonstrating the strong potential for growth**. Whether or not there is an interest of those companies in the domain of security and defence, remains to be seen. This is also confirmed by a recent publication by Agoria and De Tijd.
2. Secondly, overall, the **Flemish industrial ecosystem has already a solid basis of AI-driven companies, contributing to various application domains. Thereby, it should also be recognized that there is a strong research & development network in Flanders, consisting of both Strategic Research Centre's (Strategische Onderzoekscentra), universities and higher education institutions contributing to the progress of AI**, in collaboration with the Flemish industry, from a fundamental to a development & deployment level. Among others, the Flanders AI Research Programme is constributing to this.
3. Thirdly, the **potential for cross-regional collaboration should not be underestimated**. Such collaboration – involving actors from Flanders, Brussels and Wallonia – could pave the way for stronger, more aligned partnerships and a shared strategic perspective in the field.
4. Fourthly, **many of the identified companies are SMEs, start-ups and scale-ups – while this can be considered a hindering factor in the European ecosystem, which is applying a system of system approach, those SMEs, start-ups and scale-ups are to be recognized for their strong innovation potential and agility.**

5. Fifthly, while the overview is a solid mix of companies active in several domains, it should be noted that the **overall majority is active in three categories (in decreasing order): (1) decision support, models, data science, ML, (2) intelligent sensing, and (3) AI for communication.**

A Flemish AI – Defence Roadmap

This roadmap is the result of combining the above mapping of the Flemish AI ecosystem and its industrial and innovative capabilities, with an extensive study of defence needs (conducted through both desk research and interviews with key Defence stakeholders). This dual foundation reflects requirements at both the national, European and transatlantic levels.

The roadmap is structured around four mutually reinforcing and complementary focus domains: AI Sensing, AI Compute, AI for Communication, and AI for Operational Support. The first three domains are guided by a systems-of-systems logic and a strategic orientation, directly aligned with strong and clearly identified needs at national, EU, and NATO levels, and industrial and innovation capabilities. The fourth domain responds to concrete operational needs, and again also industrial and innovation capabilities, and is closely linked to the preparation and strengthening of the national defence ecosystem.

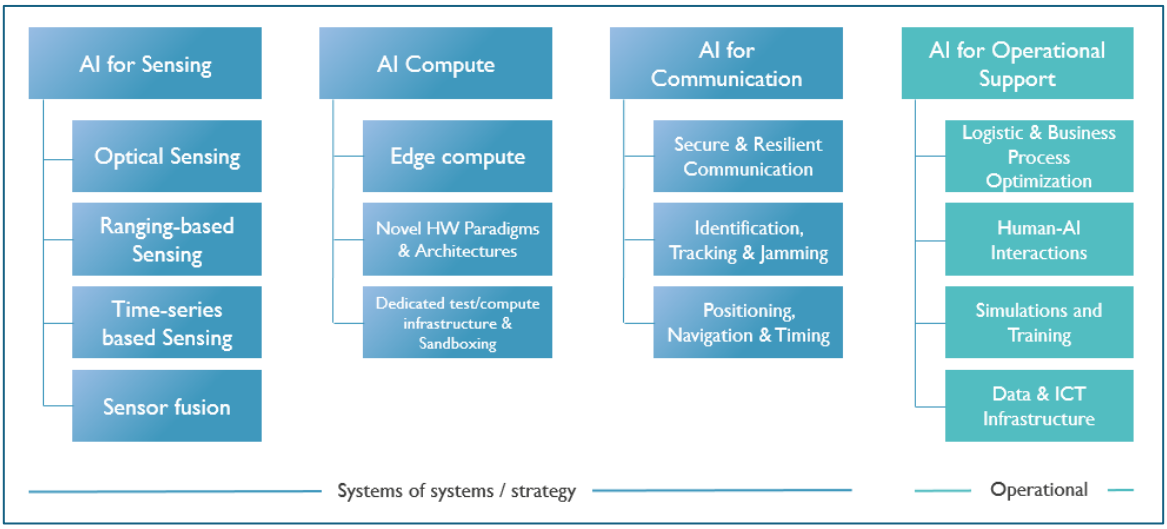


Figure 1 – Overview of focus domains and building blocks

The crucial element among those four focus domains is the central interaction that is required between the software and hardware. Further strengthening the interaction, and thus the co-design across the software and hardware, is required both from a technical point of view (e.g., reducing energy consumption, increasing efficiency), and from a digital sovereignty perspective. Indeed, digital sovereignty is the power to shape Europe's digital destiny – secure and with a higher level of self-determination and control. This interaction is reflected across all four domains, and in the different building blocks.

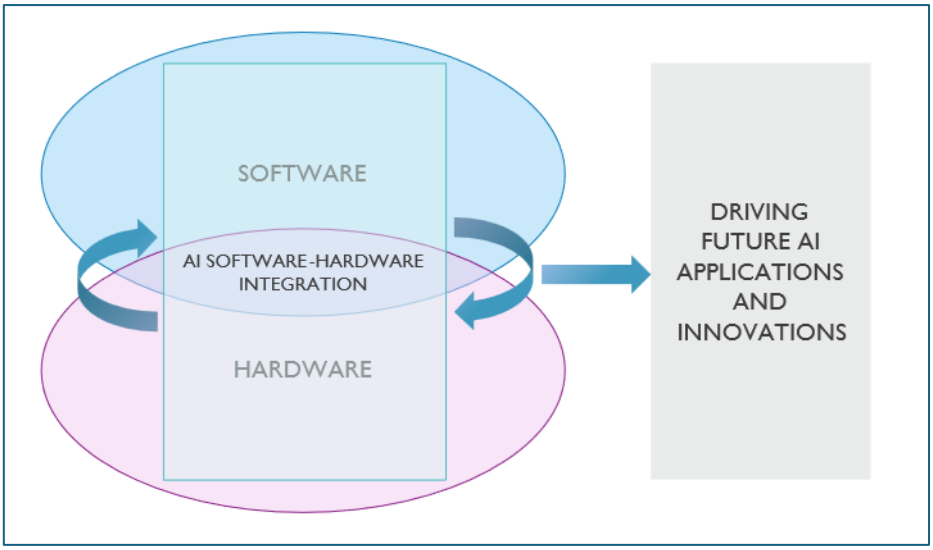


Figure 2 – AI Software – Hardware Integration, driving future AI applications and innovations

Furthermore, and besides the hardware-software interaction that runs through the different domains and building blocks, a fundamental interaction is required across the different domains to offer and develop future AI applications. For instance, when thinking about robotics, one can notice immediately the different interactions required between the domains: sensing, compute capacity and communication from a technical side, operational connection to bring in robotics as a fundamental support element in defence context. Another example are large language models, model-driven AI and hybrid AI applications, which require both an optimised compute capacity, data input which can be delivered via sensing, and integration into AI application context optimised via human-AI interactions and offered to training and working environments.

The Flemish industrial and innovative ecosystem is well placed to contribute to all four domains, with strong potential to engage directly with the Operational Support domain, while parts of the ecosystem are also ready to support the more technology-driven first three domains, and with strong cross-domain interactions.

Within each Pillar, several Building Blocks have been defined, following a complementary logic. All are described hereunder, with an explanation, a defined goal, technologically oriented examples and a set of application elements.

Focus 1: AI Sensing

Enable real-time, context-aware surveillance

A critical component in all defence and security systems is the capability to observe a specific environment. Such environments can vary a lot in size, complexity, involved actors, terrain, conditions, etc. Robust and reliable sensing is key for both manned and autonomous systems, and applications can be found across all the various defence components. Typically, sensing technologies are integrated into various systems that exist in all kinds of

formfactors (e.g., from drones and satellites, to hand-held monocular). Note that we focus here on physical surveillance, complementing the digital surveillance of the Cybersecurity roadmap.

To process the captured information, increasingly, AI-based algorithms are employed for tasks such as object detection and tracking, image segmentation, or action recognition. The need for intelligent sensor processing will only grow as more data streams and sensors become available. However, today, the different and ever-changing environments give headaches to pretrained algorithms. There are also stringent requirements in terms of accuracy, latency, efficiency, resource consumption, trustworthiness, etc. To meet the requirements, AI algorithms need to be closely coupled and integrated with the sensor(s) and the complete processing pipeline.

While there are already quite a few AI-based algorithms, such as in the computer vision domain, important technical challenges remain such as accuracy, robustness to various environmental conditions (e.g., bad weather) and disturbances (e.g., light reflections). Coupled with there are (potentially) limited data and changing contexts or tasks. Additionally, explainability methods need to be further developed to increase system trust, safety and interpretability, which is essential in a context where adversaries will want to trick or sabotage the systems.

This close coupling between algorithms and sensing pipelines is reflected in the following building blocks that focus on **3 different kinds of sensing modalities and sensor fusion**. The above-mentioned challenges recur across all building blocks.

Building Block 1.1: Optical sensing

Image-based sensors – such as RGB, thermal, infrared (short wave and long wave), and hyperspectral cameras – play a crucial role across a wide spectrum of defence and security applications. These sensors are **used in both short-range systems** (e.g., standard surveillance cameras for perimeter monitoring or night-vision visors) **and long-range platforms** (e.g., hyperspectral imaging in satellites or naval vessels). These sensors enable critical capabilities like detecting threats in low-visibility conditions, identifying targets at distance, and even supporting medical diagnostics on the battlefield.

In operational environments, there is a growing need for contextual awareness, not just pattern recognition. To increase efficiency, and lower costs of some of those cameras, there is a **need for further integration of the sensor with the processing**. AI-based methods can help with that by, for instance, playing a role in assessing performance of current camera performance and actively steer its operation. Finally, on the longer term, there is also an **interest in completely novel sensors with improved capabilities and efficiency**: for instance, quantum-based sensing, or extremely low power/passive systems.

Examples: RGB, thermal, infrared, hyperspectral cameras

Example applications: Satellite imaging, night vision and medical diagnostics

Building Block 1.2: Ranging-based sensing

Complementing the previous category are **ranged-based sensors** such as LIDAR, RADAR, SONAR, or other acoustic systems. These systems are **vital in situational awareness and threat**

detection, such as detecting aerial threats, monitoring underwater activity (e.g., submarines or underwater infrastructure), and securing critical infrastructure through perimeter surveillance. Unlike optical sensors, the data they generate (often in the form of sparse, lower-resolution point clouds) require highly robust and efficient AI-based processing to ensure accurate interpretation in complex environments. Challenges such as signal interference, physical propagation effects, and the variability between active and passive sensing modes all affect the reliability of detection algorithms. **AI plays a key role in making these systems more adaptive and capable of identifying anomalies under dynamic conditions.** In defence contexts, there's also growing interest in joint sensing and communication radio frequency technologies as this can provide additional information (e.g., for underwater data cables or the existing mobile and wi-fi commercial networks). This links with Focus area 3. Towards the future, sensors that operate at higher or varying frequences can be of interest. Focus should also be on integration of sensing and intelligence capabilities, increased efficiency and operation, and disruptive technologies like quantum-based sensors (e.g., quantum radar). One of the stand-out use cases is the detection of aerial threats.

Examples: Radar, LiDAR, sonar, acoustic systems

Example applications: Aerial threat detection, underwater monitoring, infrastructure surveillance

Building Block 1.3: Time-series based sensing (incl. health & biosensors)

A completely different type of sensors are the **time-based sensors that typically produce a series of measurement at given timestamps**. This can, among others, be in the context of measurement of vibrations or pressure (e.g., to check correct operation of machines or vehicles), environmental sensing (e.g., temperature readings or measurements for the presence of substances), or monitoring of the human body (e.g., heart rate). Note that we exclude sensors that fall in the above categories. **To process these information streams, AI algorithms are employed to detect patterns and anomalies and forecast future measurements and events.** For instance, in the context of individual soldier monitoring, it can be used to assess physical conditions and avoid specific injuries. Further development is needed and requires co-design of AI with sensing systems to ensure the captured data supports accurate, context-aware analysis. Furthermore, complementing algorithms are needed that detect anomalies as soon as possible, while limiting the number of false positives. This would require the detection and understanding of causal relationships between different measurements and variables.

Examples: Time-stamped sensor data such as vibrations, pressure, temperature, human heart rate, individual soldier monitoring

Example applications: Equipment diagnostics, environmental sensing, human performance tracking

Building Block 1.4: Sensor fusion

As it is impossible that a single sensor can offer near perfection accuracy for various tasks across different conditions, an important building block is needed that can fuse the data coming from various sensors into a single information stream that forms the basis of complete contextual awareness. Today there are two dominant approaches to achieve this: early and late fusion. As the name suggests, early fusion will bring all data directly together once it comes out of the sensors and feed that into AI networks. In contrast, in a late fusion approach, the data from each sensor is processed independently and the detections of individual sensors are merged. First efforts exist that try to combine the best of both worlds, but further R&D is definitely needed to make this more accurate, efficient and scalable. Moreover, fusing different sensors modalities is often far from trivial due to various technical aspects like different data outputs, dimensionalities (e.g., 2D versus 3D) and spatial/temporal resolutions. Also, is it difficult to easily calibrate or synchronize different sensors. Offering this (real-time) alignment of the operation of the connected sensors, and thus going beyond mere data fusion, would further increase the system-level accuracy and efficiency. These truly sensor fused system, could benefit all perception use cases across the various defence components.

Examples: Combined data of multiple sensors

Example applications: Threat detection, navigation and situational awareness

Focus 2: AI Compute

Enable flexible, efficient and secure AI systems that can adapt to rapidly changing conditions across hardware environments

It is well-known that the AI breakthroughs of the last decade have been made possible by the abundant availability of data and compute power. The popular Large Language Models are the latest exponent of this race of adding increasing amounts of GPUs and data. However, at the same time the variety of AI models is also increasing, as typically each model is made for a specific task. This heterogeneity will only further grow when AI moves even closer to the physical world (cf. physical and agentic AI). **To further increase performance, and to continue to meet the demands of algorithms, there is a need for increased flexibility on the hardware level.**

This challenge becomes even more important in a military context, where flexibility is of utmost importance. AI models will typically need to be adapted to rapidly changing conditions. As such, the impact on the underlying compute system can also vary significantly. As AI is being integrated throughout various systems with varying limitations and formfactors, the need for flexibility at a hardware level becomes ever larger. One of the key requirements is the number of resources, in the form of computational (e.g., memory) constraints or energy consumption. Especially the latter is an important one in, for instance, extreme contexts like in space or underwater where resources are scarce, or in situations where a device or system should operate passively. Furthermore, the global geopolitical context requires a growing

technological sovereignty, whereby more flexible perspectives on the software – hardware integration are needed. This requires also further developments on the software-side, i.e. by mapping the algorithms and AI workload optimally on the hardware. This is reflected in the three building blocks below.

Building Block 2.1: Edge compute

As AI algorithms are increasingly integrated in all other systems, they also need to respect the stringent requirements of those systems and the context where they operate in. When considering all kinds of UAVs, robots, satellites, or surveillance equipment, limited physical space, battery capacity, and other resources are available. However, in all these systems local intelligence is required that can perform tasks such as the processing of sensor information, fast decision making, navigation and engine control, communication, etc. This means that the E/E (electrical/Electronic) architecture of such systems need to be optimized as much as possible, including the impact of computational workloads. From a hardware perspective, we can consider the design and development of specific (modular) chips (e.g., ASIC, Neuromorphic, Chiplet approaches…) that can operate more efficiently in these contexts. In parallel, novel AI algorithms should be designed that optimally use those specific chips. While awaiting novel hardware, techniques can be employed to limit the size of AI models (cf. the impact of DeepSeek) and limit resource consumption (e.g., brain-inspired algorithms). Additionally, we can also evaluate at system-level, which components need to be active at specific moments in time (e.g., perhaps an AI model can be put to sleep during some periods). Finally, we remark that reducing resource usage has many other advantages as well: it can lower the change of detection of such systems, lower the (operational) cost of systems and reduce ecological footprints.

Examples: Robotics, model compression algorithms, brain-inspired algorithms, AI-for-IoT, embedded microprocessors (from Nvidia, NXP, AMD etc.)

Example applications: Autonomous systems, battlefield monitoring, AGVs & drones, swarm systems

Building Block 2.2: Novel hardware paradigms & AI architectures

As AI systems become more sophisticated, the demand for computational resources has grown dramatically. This surge is driven by several interrelated factors, including the increasing volume and diversity of training data, the lengthening of training cycles, the exponential growth in model size, and the growing heterogeneity of AI workloads. First, to achieve broader generalization and multimodal capabilities, modern AI models are trained on vast and varied datasets that include not only text, but also images, code, video, audio, and sensor data. **This expansion necessitates not only more GPU and storage capacity but also greater bandwidth and more intensive preprocessing pipelines.** The infrastructure required to manage and prepare such data is itself a significant driver of compute demand.

Second, and in parallel, the **time required to train state-of-the-art models has increased substantially.** Training a model can now take weeks or even months, utilizing thousands of high-performance GPUs or TPUs operating in parallel. This problem only grows with the relentless growth in AI model size.

Compounding these challenges is the increasing heterogeneity of AI workloads – a factor being highly present also in the defence domain. Indeed, the **AI defence ecosystem now includes a wide range of compute-intensive activities: fine-tuning models for specific defence applications, running real-time inference at scale, deploying models on edge devices with limited resources, and orchestrating complex pipelines that combine multiple models and modalities.** Each of these workloads has distinct compute, memory, and latency requirements, making infrastructure optimization far more complex. This heterogeneity strains existing hardware and software stacks and demands more flexible, adaptive compute architectures.

Furthermore, also the **AI compute supply side is facing serious challenges as the global supply of high-performance GPUs is struggling to keep pace with demand**. This is due in part to the sheer scale of compute required by modern AI workloads, but also to constraints in the semiconductor supply chain. Going beyond geopolitics, there is also a more fundamental issue: **GPUs themselves are approaching architectural and physical limits**.

Addressing the above identified issues at both the demand and supply side, is taking place via solutions being explored at both the hardware and software side, as well the intersection between them, evolving towards new hardware paradigms and AI architectures: explorations towards specialized AI accelerators, chiplet architectures – whereby the requirements are being split over different chiplets instead of a monolithic chip – , optical and neuromorphic computing, and quantum computing. Evolving towards this perspective, allows the configuration of hardware that can follow-up on the fast evolutions on the software side of AI, which is a crucial factor in modern security and defence situations.

Examples: AI accelerators, neuromorphic compute, quantum compute

Example applications: Autonomous systems, secure communications, cyber defence

Building Block 2.3: Dedicated compute/test infrastructure & sandboxing

A final building block, complementing the edge compute and novel hardware paradigms & AI architectures, is the further **establishment and development of dedicated test/compute infrastructures as well as sandboxing facilities, specifically dedicated to AI, as well as the interaction between AI and the related hardware.** This building block thus encompasses three complementary perspectives.

Firstly, as indicated above, **compute capacity has been – and is expected to be – a crucial factor in further spurring the evolutions of the AI. Therefore, further advancements in making compute capacity available are needed for both the development of AI systems, but also to keep the AI systems running and functioning in the most optimal conditions.** Ongoing investments to increase compute capacity and making this available for the innovation ecosystems are therefore highly relevant, and to be further developed. However, given the specific critical elements of a defence situation, attention might be devoted to new perspective on how compute capacity can be made operational in times of crisis situations – reflecting thereby on energy supply and availability, disconnections from large compute centers, mobility of compute infrastructures and distributed approaches ensuring a compute availability-risk awareness and handling.

Secondly, concerning the testing environment, this is a crucial element as the **AI systems are complex, dynamic and can – in certain instances – behave in an unpredictable way in real-world situations. Especially in the context of defence, which is driven by unpredictable and rare situations, dedicated attention is needed for testing environments.** Having thorough testing is needed to ensure reliability, security and fairness, thus preventing outcomes considered as problematic. Thus, the availability of testing environments is strongly needed from an actual functioning and ethical perspective, which encompasses both an economic and societal point of view.

Thirdly, concerning sandboxing, the EU AI Acts refers to sandboxing, and in particular AI regulatory sandboxes as follows: "provide for a controlled environment that fosters innovation and facilitates the development, training, testing and validation of innovative AI systems for a limited time before their being placed on the market or put into service pursuant to a specific sandbox plan agreed between the providers or prospective providers and the competent authority." (AI Act, 2024). From a Flemish judicial point of view, AI regulatory sandboxes are considered to fall under the so-called "experimental regulations" (Dutch: "experimenteerregelgeving"), which focuses on introducing new rules to test policy effects (Diependaele, 2024). While the set-up and implementation of sandboxes for AI is still ongoing, the expected added value refers to the fact it allows for rigorous testing in relation to issues such as security vulnerabilities, unpredictable behavior, bias etc., which is especially relevant for a domain such as defence.

However, in relation to AI innovation in the defence domain, a **further understanding of how also a "fewer rules zone"** (Dutch: "regelluwe zones", which allow for temporarily disapplying existing regulations (Diependaele, 2024))**, would be beneficial to be further established – thereby taking a perspective on how AI can be applied in times of severe national crises situations.**

Examples: Portable data centers, defence AI sandbox, AI Factory

Example applications: AI Factory (Antenna), Testbed Infrastructures (e.g. City Labs, Wireless Teslabs)

Focus 3: AI for Communication

Ensure secure, reliable and AI-enhanced communication to support coordination, decision-making and resilience in operations

A third critical element for the security and defence domain is communication. In the context of defence, communication refers to the secure and reliable exchange of information between military personnel, units, command centres, and systems to coordinate operations, share intelligence, issue orders, and maintain situational awareness. This includes voice, data, and video transmissions across various platforms such as radios, satellite links, networks, and digital messaging systems. Effective communication in defence ensures timely decision-making, synchronization of forces, and rapid response to dynamic battlefield conditions while protecting sensitive information from interception or

disruption by adversaries. Within the defence and security context, AI can, for example, enhance secure data transmission by identifying potential threats or breaches in communication networks, ensuring that information flows efficiently and safely during operations. Overall, AI for communication strengthens connectivity and coordination, which are vital in complex and high-pressure situations.

Three building blocks were identified and are further elaborated hereunder. We also want to highlight that this topics links strongly with the cybersecurity roadmap for topics such as encryption of communications signals.

Building Block 3.1: Secure & resilient communication

In security and defence contexts communication is key in various conditions. Hence communication infrastructure or transmissions are a prime candidate form disruptions and attacks. Wired cables can be cut, wireless signals can be jammed or spoofed, while endpoints and infrastructure can be destroyed. Note that not all disruption is deliberate as (natural) disaster can destroy communication towers and equipment, and channels can be overloaded easily when bandwidth is limited (e.g., in rural areas). **AI algorithms can help in optimally using the available spectrum or assign different priorities.** The importance of such intelligent operations grows even stronger when regular communication is out or severely disrupted. Furthermore, **especially if there is no centralized infrastructure, there is need for ad-hoc and mesh networks that can serve as best-effort communication option.** Various communication technologies are of interest, including satellite communications or extremely low power transmissions that are hard to detect. Software-defined radios are powerful devices that, when coupled to intelligent algorithms, could play a major role in all of the above. Finally, it is of course also **key that communication signals are encrypted, and back-end infrastructure is protected** as well. As such this topic ties into the Cybersecurity roadmap.

Examples: Ad-hoc and mesh networks, software-defined radios linked to intelligent algorithms, AI algorithms for priority assignment

Example applications: Communication disruption handling, extreme terrain communication

Building Block 3.2: Identification, tracking & jamming

This area is linked to the previous one in terms of technologies under consideration, but the objective is different, and to some extent even the opposite. Given the importance of communication, **having the capacity of disrupting adversarial signals is powerful**. A first challenge is to detect and identify those signals, especially in contexts where there are also many legit communications. For instance, in the context of hybrid or urban warfare, and to detect criminal or espionage activities. Also, explosive devices or drones can send or receive communications that should be intercepted. After detection and identification, communication signals can be used to track objects or persons. A final step can be jamming of those signals. However, note that if you jam a signal, the adversary also will typically realize that. In certain scenarios it might be better to spoof signals. **Next to AI algorithms, also hardware developments (such as directed antenna's) can play a role in this context.** Finally, this topic (especially the identification & tracking part) also ties in into the AI sensing topic (building block 1.2 on Ranging-based sensing) around the topic of joint sensing & communication.

Examples: AI algorithms, ad-hoc and mesh networks, software-defined radios linked to intelligent algorithms

Example applications: Explosive device and drone detection, and disturbance of flight routes

Building Block 3.3: Positioning, Navigation & Timing

Next to secure communication, **an important capability is reliable navigation and positioning**. There are some recent examples that highlight the importance of this topic: For instance, from Ukraine, we have learned that drone communication and localization is jammed in the last kilometres before arriving on target. This sparked the interest of (re-)using fiber optic cables. Also, in the Baltics region, GPS signals of (commercial) planers are often disrupted or spoofed. Hence it is clear that **reliance on only satellite positioning systems is insufficient. Localization using other wireless signals can be explored, in combination with visual navigation** (e.g., using AI detection of landmarks). Hence this links with topics from the other two areas. Next to outdoor navigation, **indoor or urban navigation is still a challenge, especially in previously unknow areas**. Localization and recognition of teammates in such conditions could potentially save lives (e.g., friendly fire, evacuations, …). Here, technologies such as Bluetooth (low energy) and Ultra-Wide band can be of interest.

Examples: AI algorithms for visual analysis, Bluetooth, ultra-wide band

Example applications: AI based localization, combining wireless and visual navigation

Focus 4: AI for Operational Support

Enable and ensure efficient & effective defence and military operations

A fourth focus element is the relevancy of AI for the provision of operational support. Indeed, operational activities remain a critical element in ensuring the efficient and effective functioning of an integrated defence and security system, within a single nation but also across borders, in various constellations and collaborations. AI can help to reinforce collaboration, to support decision-making and analysis, to increase the overall responsiveness etc. of various operational activities. **Given that operational support is cutting throughout the various layers of a defence & security systems, a close attention for the human-AI interaction is thereby also required.**

Already today, AI can be a highly supportive element for the provision of operational support, functioning on a wider continuum of application domains and degrees to which AI is actively applied in the human-AI relationship for decision-making. Further advancements in the technology are expected to even more impact this focus area.

Four building blocks were identified and are further elaborated hereunder:

- **Logistic and business process optimization and decision support**
- **Human-AI interactions**
- **Simulation and training**
- **ICT Infrastructure & Data**

From a technological perspective on AI in relation to this focus area, one can think of data simulations and digital twins, synthetic data generation, large-scale modelling, XR / VR / AR technologies, chatbots, natural language processing and large/small language models, software services etc.

Building Block 4.1: Logistics and business optimization & decision support

Modern military operations face growing complexity in both logistics and decision-making. For instance, coordinating routes, schedules, personnel, and equipment across diverse missions requires balancing multiple priorities, such as cost, speed, and risk, under constantly changing conditions. Other examples can be found in daily administration, procurement, scenario building, inter-team/department information exchange, and overall decision-making. **To meet these challenges, advanced technologies like machine learning and AI are playing an increasingly vital role.**

These algorithms help improve logistics by forecasting demand, managing inventories, and dynamically adjusting supply routes based on real-time data such as terrain, weather, or mission updates. They ensure that critical resources reach the right place at the right time, reducing both shortages and waste. ML and AI also support smarter resource allocation by matching personnel, vehicles, and equipment to mission needs more effectively.

Beyond logistics, these technologies strengthen broader business and operational functions. Automating the analysis of large volumes of unstructured information –such as reports, emails, or sensor data – helps teams access key insights faster and reduces administrative burden. In procurement, AI-powered tools can analyse past contracts to improve cost estimates and keep budgets on track. When it comes to maintaining complex equipment, predictive models can anticipate failures before they occur, cutting downtime and operational costs.

By embedding AI, including ML, across logistics and decision-making processes, defence activities and operations can operate with greater speed, precision, and resilience, transforming data into a strategic advantage and ensuring readiness in an increasingly dynamic and demanding environment.

Examples: Advanced analytical approaches, metaheuristics, mathematical modelling, data sharing technologies

Example applications: Real-time logistics, staff matching to vehicles & equipment, equipment maintenance, improved cost estimations and decision making

Building Block 4.2: Human-AI interactions

The growing complexity of modern warfare entails an increase in ways in which humans and AI systems communicate, collaborate and influence each other. Human-AI interaction

techniques are vital to ensure AI systems are intuitive, transparent and trustworthy. These systems support complex, high-stakes decision making so it is important that human operators can quickly understand and act on AI recommendations.

To foster meaningful human-AI collaboration, it is essential that systems communicate in ways users can understand and trust. Interfaces that show how AI reaches its conclusions - without overwhelming the user – can support better judgment, especially in high-pressure or time-sensitive settings. Transparent, explainable systems allow users to verify outputs rather than blindly accept them, helping prevent misuse and over-reliance. At the same time, thoughtful interface design can reduce mental effort, making interactions more intuitive and responsive to users' real-world demands. Simplicity, accessibility, and clarity are critical, not only for usability but also for safety and ethical accountability.

Examples: Interface developments, explainable algorithms, black-box unraveling

Example applications: Battlefield Management Systems, Training environments for logistics, Human-supervised UAVs

Building Block 4.3: Simulations and training

AI has a crucial role in military personnel training by enabling personalized, adaptive, and highly immersive simulation experiences. AI algorithms can analyze individual performance data to tailor training programs that target specific skill gaps and learning speeds, ensuring optimal development. Leveraging AI-powered Virtual Reality (VR), Augmented Reality (AR) and Extended Reality (XR) technologies as well as digital twin simulations of real-world, training environments can simulate complex, dynamic combat scenarios with high fidelity, including varied terrains, weather conditions, and realistic adversary behaviors. AI systems will dynamically adjust these scenarios in real-time based on trainee decisions, providing continuous challenge and immediate feedback to enhance decision-making and situational awareness.

Furthermore, AI-driven cognitive models can replicate stress and unpredictability, helping military personnel to develop resilience under pressure. Detailed performance analytics powered by AI will enable objective assessment and after-action reviews, identifying strengths and areas for improvement. By enabling scalable, resource-efficient remote training, AI combined with VR/AR reduces logistical burdens and costs associated with traditional exercises.

Examples: AR, VR, XR technologies for training military personnel, digital twin simulations of crisis and battlefield environments, AI algorithms supporting digital twin & AR/VR/XR environments

Example applications: Training of field surgery, practica of maintenance of complex systems, operational/mission training

Building Block 4.4: Data & ICT Infrastructure

Focus 2: AI Compute, *Building Block 2.3* refers to dedicated compute/test infrastructure and sandboxing. This is related to this Building Block from an operational point of view, and refers specifically to the **data availability and sharing for both hardware and software**. In the various defence branches, such as land, sea, air, space and cyber, the military activities strongly rely on data and its availability – which can, in turn, then also be applied in the context of AI. Especially for operational activities, **a close connection towards the data is required, also given the extreme operational conditions**. Furthermore, **making data more easily accessible, but strongly protected, strengthens the possibilities for AI developments and applications**. A solid data backbone allows for active cross-border military collaboration, from a European and international point of view. **Further evolutions in the field of the overall ICT infrastructure for data are thus to be explored**, whereby both decentralized (e.g. data space evolutions) and cloud approaches come forward. Across this thema, special attention should also be given to increased data, ICT and algorithmic sovereignty at a European level.

Examples: Cloud and data centers, data sharing technologies

Example applications: Any type of application to be support by data availability in any type of situation.

Conclusion

This Orientationroadmap provides a starting point for strengthening the relationship between the defence and security ecosystem on the one hand, and the Flemish industrial based AI-ecosystem. It is the results of an intensive analysis of the Flemish industrial ecosystem active in the field of AI and defence/security, and an identification of needs existing in a national, European and transatlantic (NATO) defence context.

This document, and related exercise is, as indicated in the introduction **embedded in a wider exercise "Impulsprogramma Veiligheid en Defensie", which aims to "*promote, stimulate and support security and defence industry and innovation in Flanders which contributes to the Flemish, Belgian, European and transatlantic technological and industrial defence base*".** As such it can function as a starting point for Flanders to contribute positively, from the Flemish region to a geopolitically turbulent context, with a view to strengthening Flemish players in this domain.

It can be noted that the needs, to be tackled via the focus areas, are connected to the classification of the Flemish industrial AI ecosystem. Indeed, based on the conducted exercise, one can be argued that **the Flemish industrial AI ecosystem has a relevant potential to contribute to the identified needs, especially via a wide group of actors via AI for Operational Support, and via a more specialized group within the ecosystem also to the three other focus areas.** Crucial will be the system of systems logic however, whereby the Flemish industrial AI ecosystem, which consists mainly of smaller and high-specialized actors within the field, focuses on building regional, national and international connections, to further position itself within the European and NATO-oriented landscape.

References

AGORIA, 2025a

AGORIA, 2025b

AI Act, 2024

De Tijd, 2025

Diependaele, 2024

Draghi, 2024

European Commission, 2025a

European Commission, 2025b

European Commission, 2025c

Flemish Peace Institute, 2022

Haldorai et al., 2024

imec istart, s.d.

Leuven Mindgate, s.d.

Mamediieva, 2025

VARIO, 2024

Wireless Community, s.d.

Annexes

Annex 1

The following listings and documents with a specific focus on security & defence were analysed:

1. **AGORIA Belgian Security & Defence Industry**: An overview of the AGORIA members and other companies and stakeholders with a specific interest in Security or Defence technology (AGORIA, 2025).
2. **European Defence Fund (EDF) Brokerage Event participants**: Overview of all participants (at company level) of the latest European Defence Fund Brokerage Event (European Commission, 2025c).
3. **VARIO Advisory Report 38**: Opportunities and needs for the Flemish defence industry and -innovation (VARIO, 2024).
4. **Flemish Peace Institute 2022 Report**: De defensiegerelateerde industrie in Vlaanderen: doorlichting van een sector op scherp (Flemish Peace Institute, 2022).
5. Various **newspaper articles** of Flemish newspapers

The following listing and documents with a specific focus on AI and technology were analysed:

1. **Flanders AI Forum 2024**: An overview of the active contributors to the Flanders AI Forum 2024.
2. **Imec istart**: Companies active in the istart support mechanism system (imec istart, s.d.).
3. **Leuven Mindgate**: Members of Leuven Mindgate (Leuven Mindgate, s.d.)
4. **Wireless Community**: A network of partners working on wireless and communications technologies active in Flanders (Wireless Community, s.d.)
5. **The Beacon community**: Innovation hub that brings together tech companies, to foster collaboration in AI, IoT and smart-city solutions in Antwerp. (The Beacon, s.d.)

Finally, extra companies were identified via **existing (imec) security & space related collaborations**, **direct personal contacts** and **ongoing non-defence & security related (EU-funded) projects**.

Each of the identified companies was screened via the public available information, whereby the following data was collected:

1. AI connection (first and secondary order, whereby secondary order could entail various elements),
2. public indication of a defence & security connection (e.g. via a domain labelling, a direct project reference),
3. a concise conceptual description of the focus, location (in Flanders or Brussels) and
4. a website (when available).

Finally, for each company, a defence/security-AI label was provided linking to the following: (1) EDF Brokerage Event participation / AGORIA BSDi participation / participation to know defence project, (2) a public connection to defence / security, but not part of the previous category and (3) related to AI, but no connection to defence / security.

Cyberveiligheid voor defensie

Versterking van militaire cyberweerbaarheid en bescherming van kritieke infrastructuur via Vlaamse technologische innovatie en internationale samenwerking.

Cyber Security Vlaanderen

howest hogeschool

KU LEUVEN

Visie en context

De **geopolitieke context** wordt steeds complexer met toenemende spanningen tussen grootmachten, hybride oorlogsvoering en een explosie aan **cyberaanvallen die zowel militaire doelwitten als kritieke economische en maatschappelijke sectoren treffen**. Cyberaanvallen op energie-infrastructuur, satellietcommunicatie, havens, gezondheidszorg en defensie-netwerken tonen aan dat de digitale dimensie van conflicten niet langer een ondersteunend domein is, maar een frontlijn op zich. Dit heeft ertoe geleid dat in vele krijgsmachten wereldwijd een vierde component, cyberdefensie, naast land-, lucht- en zeemacht wordt uitgebouwd. Deze cybercomponent is onlosmakelijk verbonden met cybersecuritymaatregelen en -acties in vitale sectoren, aangezien de grenzen tussen militaire, economische en civiele infrastructuur in het digitale domein steeds meer vervagen. Het groeiend aantal aanvallen met geopolitieke impact – van grootschalige DDoS-campagnes tot aanvallen op kritieke OT-systemen – maakt duidelijk dat **een geïntegreerde en grootschalige aanpak noodzakelijk is**.

De **economische en maatschappelijke impact van cybersecuritydreigingen is indrukwekkend** en onderstreept de urgentie van een krachtige verdediging. Wereldwijd zullen de kosten van cybercrime naar verwachting oplopen tot maar liefst 8 biljoen euro in 2024, en volgens voorspellingen zelfs tot 20 biljoen euro in 2027. Voor individuele organisaties kunnen datalekken gemiddeld meer dan 4 miljoen euro kosten. De beruchte Petya-aanval (ook NotPetya genoemd) veroorzaakte verliezen die opliepen tot meer dan 8,5 miljard euro op wereldvlak, met zware impact voor onder andere Maersk en Merck. Hoewel cijfers specifiek voor militaire contexten zeldzamer zijn, benadrukken deze enorme bedragen hoe cyberaanvallen niet louter financiële schade veroorzaken, maar diep doordringen in logistieke, operationele en strategische lagen — zeker tijdens geopolitieke crisissen.

Deze prioriteiten zijn reeds duidelijk benoemd in diverse beleidsdocumenten. Op internationaal vlak leggen de NAVO Cyber Defence Policy en de Digital Transformation Vision 2030 de nadruk op cyber-resilience, AI-integratie en de nauwe samenwerking met industrie en kennisinstellingen. De Europese Unie heeft met de Cybersecurity Strategy for the Digital Decade, het Cyber Defence Policy Framework en het EU Space Strategy for Security & Defence een stevig beleidskader neergezet waarin het Europees Cybersecurity Competence Centre, PESCO-projecten en de NIS2-richtlijn als sleutelelementen fungeren. Op nationaal vlak maken het Belgische Defensieplan STAR 2023–2030 en het Vlaamse Beleidsplan Digitalisering en Innovatie de weg vrij voor een versterkte cyberweerbaarheid, dual-use technologie en hechte samenwerking tussen bedrijven, overheid en kennisinstellingen.

Tegelijkertijd **neemt de kwetsbaarheid toe door de unieke positie van Vlaanderen in de Europese en mondiale economie**. Als logistieke draaischijf met zeehavens van wereldniveau, een open en hooggeconnecteerde digitale economie, een sterk ontwikkelde maakindustrie en gespecialiseerde clusters in lucht- en ruimtevaart, energie en biomedische technologie vormt Vlaanderen een aantrekkelijk doelwit voor statelijke actoren en georganiseerde cybercriminaliteit. Het hoge digitaliseringsniveau en de verwevenheid met internationale waardeketens vergroten de potentiële impact van cyberaanvallen op zowel de economie als de

samenleving. Net deze kwetsbaarheid maakt van cybersecurity **niet alleen een veiligheidsnoodzaak, maar ook een strategische groeikans**: investeringen in geavanceerde cyberdefensie kunnen Vlaanderen positioneren als een Europese voortrekker in digitale soevereiniteit en als leverancier van hoogwaardige beveiligingsoplossingen aan kritieke sectoren wereldwijd.

Voor Vlaanderen liggen hier unieke geopolitieke en economische kansen. Met een internationaal erkend onderzoekslandschap rond cybersecurity, een performant hightech en maakindustrie-ecosysteem en strategische clusters in onder meer lucht- en ruimtevaart en maritieme infrastructuur kan Vlaanderen een voortrekkersrol spelen in de ontwikkeling van niche-oplossingen voor cyberdefensie. Dat kan gaan van cybersecurity-by-design in defensie- en ruimtevaarttechnologie tot de integratie van hardwarebeveiliging en high-end communicatieoplossingen in militaire toepassingen. Ook de uitbouw van cyberranges en testfaciliteiten, evenals de ontwikkeling van dual-use technologie die zowel defensie- als civiele sectoren versterkt, zijn domeinen waarin Vlaamse bedrijven zich kunnen onderscheiden en exportmarkten kunnen aanboren binnen de EU en NAVO.

Om deze opportuniteiten te verzilveren is specialisatie en focus noodzakelijk. Enkel door de krachten van publieke, private en academische actoren te bundelen, **via een sterke mobilisatie van het Vlaamse ecosysteem en met Europese schaalvergroting**, kan Vlaanderen duurzame impact creëren. Slimme specialisatie in domeinen zoals AI-ondersteunde cyberbeveiliging, lucht- en ruimtevaarttechnologie, OT- en netwerkbeveiliging in de maakindustrie en de bescherming maar ook activatie van medische data en militaire gezondheidsinfrastructuur vergt een lange termijnstrategie waarin innovatie, economische groei en geopolitieke slagkracht hand in hand gaan.

Het militaire cybersecuritylandschap evolueert snel en omvat een brede waaier aan technologieën en capaciteiten, gaande van security-by-design voor software, hardware en communicatie, tot cyber operations voor inlichtingen, situation awareness, command & control en red/blue teaming. Door deze domeinen te verbinden met de bestaande sterktes van Vlaamse bedrijven en kennisinstellingen kan een geïntegreerde aanpak ontstaan die niet alleen de weerbaarheid van defensie en kritieke sectoren versterkt, maar ook een nieuwe industriële groeimotor vormt in het tijdperk van digitale soevereiniteit en strategische autonomie voor Vlaanderen en Europa.

Vanuit deze sterktes van de Vlaamse cybersecuritysector en de geïdentificeerde noden van nationale en internationale defensie wordt vervolgens een visuele roadmap ontwikkeld met duidelijke focusgebieden en thematische doelstellingen. Deze roadmap kans dienen als inspiratie of richtlijn om investeringen, onderzoek en industriële innovatie te bundelen in een gecoördineerde strategie die Vlaanderen en Europa positioneert als voortrekkers in cyberdefensie en digitale veiligheid.

Vlaamse sterktes in Cyberveiligheid

Vlaanderen heeft in de voorbije vier decennia een wereldreputatie opgebouwd in cybersecurity. Zo is er een heel sterke internationale track record rond het cybersecurity onderzoek, met een brede waaier van expertise gaande van cryptografie en veilige software ontwikkeling tot systeem- en hardwarebeveiliging. Daarnaast is Vlaanderen gekenmerkt door een solide industrieel weefsel rond cybersecurity, geënt op de internationale pioniersrol van Ubizen[1] rond de eeuwisseling.

Op basis van een brede screening van publiek beschikbare bronnen werden meer dan 170 bedrijven in de cybersecurity sector geïdentificeerd in Vlaanderen, waarvan meer dan 70% hun hoofdvestiging in Vlaanderen heeft. Hun kernactiviteiten werden in kaart gebracht, en deze worden weergegeven in onderstaande tabel. Hierbij zijn cybersecurity bedrijven vaak actief in meerdere van de geïdentificeerde subdomeinen.

Cybersecurity subdomein	**# bedrijven**
Application Security	19
Awareness	13
Cloud security	19
Cryptography	2
Endpoint security	29
GRC: Governance, Risk and Compliance	35
Identity and Access Management	26
Infrastructure security	11
Network security	50
OT security	24
Privacy	17
Security monitoring	62
Security testing	38
Security training and simulation	34

Hierbij valt een sterke representatie van de Vlaamse industrie in het bouwen en versterken van veilige applicaties en systemen (FORTIFY), alsook het verzekeren van de operationele beveiliging van de infrastructuur en hun toepassingen (SHIELD). Deze twee pijlers zijn vanzelfsprekend belangrijk in de civiele context, maar zijn ook cruciaal in de beveiliging van kritische infrastructuur en defensie.

[1] Het internetbeveiligingsbedrijfs Ubizen werd destijds onder de naam NetVision opgericht door Stijn Bijnens als spinoff van de KU Leuven. Het groeide uit tot marktleider in internetbeveiliging in Europa en werd integraal onderdeel van Verizon Business. Vele oud-medewerkers zijn tot op vandaag nog steeds actief in de cybersecurity industrie in Vlaanderen.

Zo is er brede expertise en dienstverlening aanwezig voor de ontwikkeling van veilige (en privacy-vriendelijke) software, gaande van *threat modeling* technieken, veilige code ontwikkeling en uitgebreide security testing. Zo wordt bijvoorbeeld in deze context het leiderschap van het OWASP SAMM (S*oftware Assurance Maturity Model*) project vanuit Vlaanderen aangestuurd, en is er een hele wereldwijde community opgebouwd rond dit maturiteitsmodel.

Qua operationele beveiliging van infrastructuur en hun toepassingen heeft Vlaanderen een brede set van dienstverleners, met uitgebreide expertise in het eindpunt beveiliging, het beveiligen van netwerk en OT omgevingen, en het monitoren en beheren van beveiliging.

Vlaanderen heeft internationaal een ijzersterke reputatie wat betreft cybersecurity onderzoek en heeft ook de nodige kritische massa opgebouwd, mede dankzij het Vlaams Onderzoeks-programma Cybersecurity. De track record van meer dan 40 jaar cybersecurity onderzoek omvat onder andere tal van cryptografische innovaties zoals de ontwikkeling van het AES algoritme en meer recent de bijdrages aan post-quantum cryptografie en confidential computing, de pioniersrol in software security en de vele attack/defense onderzoeksbijdragen aan systeembeveiliging – denk maar aan Wifi beveiliging en Trusted Execution Environments (zoals SGX). Vanuit die onderzoekssterktes is Vlaanderen dan ook heel geschikt om de beveiligingsuitdagingen van morgen aan te gaan, en emerging beveiligingstechnologie te ontwikkelen voor kritische infrastructuur en defensie, zoals post-quantum cryptografie, cybersecurity voor AI-gebaseerde systemen, sovereign clouddiensten en veilige communicatie-netwerken van de toekomst.

Vlaanderen beschikt ook over een groeiend ecosysteem van startups en scale-ups in cybersecurity, en biedt meerdere innovatieve security diensten aan wereldwijd, zoals recent nog gedemonstreerd op de grootste cybersecurity beurs ter wereld, RSAC.

Cybersecurity roadmap

Cyberveiligheid voor Defensie

FORTIFY Security-by-Design	SHIELD Operational Security	SURGE Emerging Security Technology	CONTROL Cyber Operations Technologies
Security and resilience built-in for software- and hardware-based defense technology	*Operational security for defense and critical infrastructure*	*Develop and integrate emerging security technology*	*Technology to support and enable Cyber Operations*
• Software Security • Hardware Security • Cyberdefense Modeling and Simulation • Cyber Immune System Design	• Active Threat Intelligence • Cloud and Infrastructure Security • OT and Network Security • End-point Security • Security monitoring and management	• Post-Quantum Cryptography • Cybersecurity for AI • Sovereign Cloud • Secure & Resilient Communication	• Cyberspace intelligence, Surveillance and Reconnaissance (CyISR) • Cyber Defense Situation Awareness • Red teaming • Command-and-Control services

Fortify-Shield-Surge-Control

In een wereld waarin geopolitieke spanningen en digitale dreigingen elkaar versterken, wordt cyberdefensie een strategische pijler voor zowel nationale veiligheid als industriële innovatie. Het Vlaamse Defensieplan speelt hierop in door de sterktes van de Vlaamse industrie – zoals high-tech maakbedrijven, cybersecurity-scale-ups, digitale infrastructuurspelers en kennisinstellingen – te koppelen aan de toenemende noden van nationale en internationale defensiepartners (NAVO, EU, Belgische Defensie). Deze kruisbestuiving creëert een unieke kans om technologie en expertise te valoriseren, waarbij Vlaanderen zich kan positioneren als een betrouwbare leverancier van geavanceerde cyberdefensie oplossingen, ingebed in een breder ecosysteem van beleid, onderzoek en industriële ontwikkeling.

Binnen deze visie worden vier strategische pijlers uitgewerkt die elk een reeks thematische doelstellingen en innovatiekansen omvatten: **FORTIFY** (security-by-design: veilige software, robuuste hardware, en beveilingsarchitecturen vanaf de ontwerpfase), **SHIELD** (operational security: bescherming van netwerken, infrastructuur en operaties), **SURGE** (emerging security technology: securing AI, quantum, autonome systemen en next-gen cryptografie) en **CONTROL** (cyber operations technologies: situation awareness, command-and-control en actieve verdediging). Samen vormen zij de bouwstenen van een toekomstgerichte cyberverdediging waarin Vlaamse bedrijven, gesteund door kennisinstellingen en beleidskaders, innovatieve oplossingen kunnen ontwikkelen die zowel aan de Belgische als aan de internationale defensienoden voldoen.

Binnen zowel FORTIFY en SHIELD wordt er in Vlaanderen vertrokken vanuit een sterke maturiteit en ervaring, opgebouwd in een civiele context, waarbij er een duidelijk potentieel is om dit verder te ontwikkelen en te vermarkten in een context van dual use, kritische sectoren en defensie. SURGE biedt gerichte innovatiekansen aan om samen met de onderzoeksexpertise in Vlaanderen toekomstgerichte oplossingen voor een defensiecontext te creëren. Binnen het CONTROL luik kan ons industrieel weefsel zich nieuwe capaciteiten eigen maken en ontwikkelen, die specifiek gericht zijn op defensieve en offensieve militaire cyberoperaties.

FORTIFY - Security-by-Design

FORTIFY: Security and resilience built-in for software- and hardware-based defense technology

Ook in een defensie context betekent Security-by-Design dat beveiliging en veerkracht niet achteraf worden toegevoegd, maar vanaf de eerste conceptfase integraal worden ingebouwd in software-, communicatie- en hardwarecomponenten die worden gebruikt in defensiesystemen en kritieke infrastructuur. Dit is essentieel omdat militaire technologie vaak opereert in hoog-risico-omgevingen waar cyberaanvallen, elektronische oorlogsvoering en supply chain-dreigingen continu aanwezig zijn. Door Security-by-Design te hanteren, wordt elke laag – van microchip en firmware tot communicatieprotocollen en operationele software – ontworpen met intrinsieke beveiligingsmechanismen, waardoor de aanvalsoppervlakte drastisch wordt verkleind en systemen beter bestand zijn tegen zero-day exploits, hybride oorlogsvoering en insider threats.

Het is voor Vlaanderen strategisch belangrijk om in te zetten op Security by Design of Security & Resilience Built-in binnen defensie- en kritieke infrastructuurtechnologie, omdat deze aanpak de basis vormt voor veiligheid, betrouwbaarheid en interoperabiliteit van toekomstige militaire en civiele systemen. Door te focussen op Software Security, Hardware Security, Cyberdefense Modeling & Simulation en Cyber Immune System Design kunnen Vlaamse bedrijven oplossingen ontwikkelen die voldoen aan NAVO-, EU- en nationale veiligheidsnormen, en tegelijk de groeiende vraag naar cyberveilige digitale transformatie in defensie, maritieme en energie-infrastructuur bedienen. De combinatie van deze domeinen creëert een geïntegreerde beveiligingsarchitectuur waarbij hardware en software vanaf de conceptfase weerbaar worden ontworpen, communicatiekanalen intrinsiek beschermd zijn, en simulatieplatformen en AI-gedreven “immune systems” proactieve detectie en respons mogelijk maken.

De thematische doelstellingen versterken elkaar in een logische fasering/roadmap: eerst wordt robuuste hardware- en softwarebeveiliging geborgd als fundament, waarna op architectuur en infrastructuur niveau wordt ingezet op modelering en simulatie enerzijds, en autonome detectie en herstel anderzijds. Voor Vlaamse bedrijven betekent dit kansen om high-tech niches te ontwikkelen zoals chip-level security, quantum-safe communicatie, AI-gedreven simulatie-omgevingen en self-healing cyberdefenseplatformen. Deze roadmap creëert exportpotentieel naar Europese defensieprogramma’s (EDF, PESCO), versterkt lokale toeleveringsketens en positioneert Vlaanderen als innovatieve hub in de Europese veiligheids- en defensie-economie.

Software Security

Software Security binnen cybersecurity richt zich in een militaire context op het beschermen van kritieke softwaretoepassingen tegen kwetsbaarheden, malware, sabotage en cyberaanvallen. Voor bedrijven die actief zijn in defensie betekent dit het ontwikkelen van veilige software vanaf de ontwerpfase (security by design), inclusief threat modeling, software beveiligingsarchitecturen, veilige codeerpraktijken, geautomatiseerde vulnerability-scans en het toepassen van technieken zoals zero-trust architecturen en code-signing. Dit is essentieel voor militaire systemen zoals command-and-control-platformen, drones, communicatie-

infrastructuur en wapenbeheersystemen, waar een succesvolle aanval directe impact kan hebben op operationele veiligheid en nationale verdediging.

Zowel binnen defensie als binnen kritische sectoren is software security cruciaal om cyberaanvallen van statelijke actoren, sabotagepogingen en supply chain-risico's te minimaliseren. Vlaamse bedrijven kunnen hierop inspelen door oplossingen te ontwikkelen rond veilige softwareontwikkeling, AI-gedreven dreigingsdetectie en real-time monitoring van kritieke applicaties. Voorbeelden zijn samenwerking tussen Vlaamse cybersecurity-startups, onderzoekers en defensiebedrijven voor geautomatiseerde code-analyse of voor het bouwen van geharde softwareplatformen voor maritieme en luchtvaarttoepassingen. Dit creëert niet alleen strategische autonomie maar ook exportkansen richting NAVO en EU-defensieprojecten.

Innovatiekansen[2]

- Software security expertise: Toepassen van de kennis in secure software development en software maturiteit in defensie- en kritieke infrastructuurprojecten.
- Automated Vulnerability Detection: Tools voor software verificatie en real-time code-analyse kunnen vanuit Vlaanderen internationaal worden ingezet.
- Digital Twin Security Testing: Integratie van cybersecurity in digitale tweelingen van militaire systemen maakt veilige simulaties en training mogelijk.
- Supply Chain Security Platforms: Software voor het monitoren en verifiëren van toeleveringsketens kan vanuit Vlaanderen worden geëxporteerd naar Europese defensiepartners.

Hardware Security

IT- en OT-componenten zoals servers, communicatiesystemen, sensoren, cryptografische modules en edge-devices tegen sabotage, spionage en ongeautoriseerde toegang. Voor bedrijven in de defensiesector betekent dit het ontwikkelen en integreren van technologieën zoals hardware-gebaseerde root-of-trust, secure boot, fysieke anti-tampering, Trusted Platform Modules (TPM), Hardware Security Modules (HSM) en Supply Chain Security voor microchips en embedded systemen. Deze maatregelen zijn cruciaal om te garanderen dat militaire communicatienetwerken, drones, radar- en wapensystemen niet worden gecompromitteerd door vijandelijke actoren of insider threats.

Voor defensie is dit belangrijk omdat hardware vaak de laatste verdedigingslinie vormt tegen cyberaanvallen en fysieke sabotage, en omdat digitale soevereiniteit afhangt van betrouwbare en veilige elektronica. Voor Vlaamse bedrijven biedt dit kansen in high-tech domeinen zoals hardware beveiliging, IoT-beveiliging, edge computing en cryptografie. Concreet kan Vlaanderen inspelen op Europese defensieprojecten rond secure supply chains, cyberfysieke beveiliging van

[2] Niet-exhaustieve lijst van innovatiekansen.

drones en maritieme systemen en militaire datacenters met hardwarematige isolatie (zoals Intel SGX of AMD SEV). Dit creëert economische opportuniteiten voor KMO's en onderzoeksinstellingen om nieuwe producten, testlabs en certificeringsdiensten te ontwikkelen.

Innovatiekansen[2]

- Secure hardware supply chain – Ontwikkeling van tools en processen voor traceerbare en authentieke componenten in defensie-toepassingen.
- Hardware-gebaseerde root-of-trust – Vlaamse high-tech bedrijven kunnen cryptografische modules en HSM-technologie ontwikkelen voor militair gebruik.
- Fysieke anti-tampering oplossingen – Ontwerp van sensoren en coatings die fysieke manipulatie van kritieke hardware detecteren en voorkomen.
- Edge-security voor IoT en drones – Beveiligde hardwareplatformen voor autonome systemen in maritieme en luchtvaarttoepassingen.
- Test- en certificeringslabs – Vlaanderen kan zich profileren als Europees centrum voor hardwarebeveiligingsaudits en militaire compliance-normen.

Cyberdefense Modeling and Simulation

Cyberdefense Modeling and Simulation binnen cybersecurity omvat het gebruik van geavanceerde simulatieplatformen en digitale tweelingen om cyberaanvallen, verdedigingstactieken en bedrijfscontinuïteitsscenario's te testen in een realistische maar gecontroleerde omgeving. In een militaire context stelt dit bedrijven in staat om security testing, incident response en resilience-strategieën door te voeren zonder reële systemen in gevaar te brengen. Het ondersteunt bovendien het trainen van personeel, het modelleren van kritieke infrastructuren en het uitvoeren van "what-if" analyses rond cyberdreigingen, zodat zowel operationele technologie (OT) als IT-netwerken voorbereid zijn op grootschalige en complexe aanvallen.

Voor defensie biedt deze aanpak enorme voordelen: ze versnelt de ontwikkeling van robuuste beveiligingsarchitecturen, ondersteunt militaire besluitvorming met data-gedreven inzichten en reduceert downtime- en herstelkosten bij incidenten. Voor Vlaamse bedrijven opent dit opportuniteiten in domeinen zoals AI-gestuurde simulatie-tools, digitale tweelingtechnologie en cloud-gebaseerde testomgevingen. Denk aan KMO's die een cyberrange ontwikkelt voor maritieme logistiek, of die zelflerende modellen bouwen voor OT-netwerkverdediging. Zulke oplossingen sluiten aan bij internationale defensiebehoeften en bieden toegang tot NAVO- en EU-programma's.

Innovatiekansen[2]

- Digitale tweelingen van kritieke infrastructuur – Bedrijven in haven- en energiesector kunnen digitale kopieën van systemen maken voor veilig testen en training.
- Cloud-gebaseerde cyberranges – Vlaamse cloud- en securitybedrijven kunnen schaalbare oefenplatformen aanbieden voor militaire en industriële partners.

- Resilience- en herstelstrategieën – Consultancy-bedrijven kunnen geavanceerde business continuity plannen ontwikkelen gebaseerd op simulatie-data.
- OT- en IoT-beveiligingstesten – kmo's met focus op industriële automatisering kunnen testomgevingen bouwen voor fabrieken, energie en maritieme toepassingen.
- Cybersecurity-training en serious gaming – Vlaamse edtech-spelers kunnen gamified trainingsmodules ontwikkelen voor defensie en industrie.
- Cyber Range & simulatieplatformen: Opleiding en testinfrastructuur bouwen voor NAVO-partners in samenwerking met Vlaamse kennisinstellingen.

Cyber Immune System Design

Cyber Immune System Design binnen de NAVO-cybersecuritycontext verwijst naar een defensieve architectuur die geïnspireerd is op het menselijk immuunsysteem. Het gaat verder dan klassieke firewalls en detectiesystemen: het moet niet alleen evoluerende cyberaanvallen detecteren en afweren, maar ook zichzelf herstellen en adaptief reageren op inbreuken om de continuïteit van militaire operaties te waarborgen. Belangrijke concepten zoals Zero Trust Architectures en Data-Centric Security worden geïntegreerd: gegevens worden centraal beveiligd, ongeacht de infrastructuur of gebruiker, met geavanceerde classificatie- en labelmechanismen die veilige en gecontroleerde informatie-uitwisseling mogelijk maken tussen militaire systemen en bedrijven.

Voor defensie is dit cruciaal om cyberweerbaarheid te versterken tegen hybride dreigingen en supply chain-aanvallen. Voor Vlaamse bedrijven ontstaan economische opportuniteiten in domeinen zoals geavanceerde anomaliedetectie, toekomstgerichte encryptietechnologie, en secure cloud-omgevingen voor NAVO- en EU-partners. Denk aan samenwerkingen rond self-healing netwerken, data labeling voor beveiligde informatie-uitwisseling, en cyberfysieke beveiliging van kritieke infrastructuur in de haven- en energiesector.

Innovatiekansen[2]

- Zelfherstellende systemen en netwerken: Inzetten van cybersecurity expertise voor real-time detectie en automatische mitigatie van aanvallen.
- Zero Trust implementaties in OT/IT-convergentie: Toepassen in havenlogistiek en maritieme infrastructuur voor verhoogde cyberweerbaarheid.
- Data labeling & classificatie tools: Ontwikkeling van veilige informatie-uitwisseling tussen NAVO- en civiele partners.
- Cyber-resilient hardwareontwikkeling: Vlaamse crypto en hardware security expertise benutten voor HSM's en encryptiechips met militaire certificering.

SHIELD - Operational Security

SHIELD: Operational security for defense and critical infrastructure

Operational Security (OpSec) voor defensie en kritieke infrastructuur is cruciaal om de continuïteit, veerkracht en veiligheid van strategische systemen te waarborgen. Moderne dreigingen – zoals cyberaanvallen op energie- en communicatienetwerken, disruptie van transport- en maritieme systemen, en aanvallen op militaire commandonetten – zijn vaak hybride van aard en combineren cyber, elektronische oorlogsvoering en fysieke sabotagetechnieken. Het beschermen van deze vitale infrastructuur vereist een geïntegreerde aanpak van zowel IT- als OT-beveiliging, inclusief detectie- en responsmechanismen, geavanceerde versleuteling, netwerksegmentatie, en redundantie. Voor een Vlaams defensieplan vormt dit een essentiële bouwsteen om Belgische en NAVO-doelstellingen te ondersteunen en om interoperabiliteit met Europese partners te verzekeren.

Voor Vlaanderen biedt de uitbouw van Operational Security aanzienlijke economische en innovatieopportuniteiten. De regio beschikt over een sterke industriële basis in mechatronica, telecom, maritieme technologie en cybersecurityonderzoek. Door gerichte samenwerking tussen kmo's en kennisinstellingen, en de ontwikkeling van Europese defensietechnologie, kan Vlaanderen een sleutelpositie innemen in de groeiende markt voor cyber- en OT-beveiliging. Bovendien opent een geïntegreerd Vlaams defensieplan de deur naar Europese fondsen (zoals EDF, DEP en Horizon Europe) en versterkt het de lokale werkgelegenheid in hoogtechnologische sectoren, terwijl het tegelijkertijd de digitale en fysieke soevereiniteit van België en Europa versterkt.

Het is voor Vlaanderen van strategisch belang om binnen Operational Security (OpSec) voor defensie en kritieke infrastructuur te focussen op Active Threat Intelligence, Cloud & Infrastructure Security, OT & Network Security, End-point Security en Security Monitoring & Management. Deze thema's zijn complementair: Active Threat Intelligence vormt de kern voor het proactief identificeren en neutraliseren van dreigingen; Cloud & Infrastructure Security waarborgt de bescherming van gedistribueerde en hybride IT-omgevingen; OT & Network Security beschermt industriële systemen en communicatienetwerken tegen sabotage of spionage; End-point Security beveiligt de toegangspunten van gebruikers en sensoren; en Security Monitoring & Management integreert alle gegevens en incidenten in een centrale detectie- en responscapaciteit. Samen creëren deze lagen een robuuste en gecoördineerde beveiligingsarchitectuur die essentieel is voor defensie, energie, transport en andere kritieke sectoren.

Active Threat Intelligence

Active Threat Intelligence in een militaire cybersecuritycontext omvat het proactief verzamelen, analyseren en interpreteren van gegevens over potentiële en actuele cyberdreigingen. Bedrijven die actief zijn in kritieke infrastructuur, defensietechnologie en digitale diensten kunnen hierdoor aanvallen vroegtijdig detecteren, aanvallers identificeren en hun tactieken begrijpen. Dit gaat verder dan passieve monitoring: het combineert real-time dreigingsinformatie, AI-gestuurde

analyse en samenwerking met internationale defensienetwerken om bedrijven weerbaar te maken tegen steeds complexere cyberaanvallen. Een belangrijk onderdeel hierin is ook het bestrijden van cyberdisinformatie en misinformatie, omdat vijandige actoren steeds vaker digitale campagnes gebruiken om besluitvorming te verstoren, publieke opinie te manipuleren of militaire en industriële doelwitten te destabiliseren. Hierdoor wordt dreigingsinformatie niet alleen technisch, maar ook strategisch en communicatief van groot belang.

Voor defensie is Active Threat Intelligence cruciaal omdat het niet alleen de nationale veiligheid versterkt, maar ook nieuwe economische opportuniteiten opent voor Vlaamse bedrijven. Door hun sterktes in AI en data-analyse, cybersecurity-onderzoek en kritieke infrastructuur (Blue Energy, havens, offshore wind) kunnen Vlaamse ondernemingen geavanceerde oplossingen ontwikkelen voor real-time dreigingsdetectie, automatische incidentrespons en dreigingssimulaties. Denk bijvoorbeeld aan AI-modellen die zero-day aanvallen voorspellen of Security Operations Centers (SOC's) die dreigingsinformatie delen met defensie, industrie en onderzoeksinstellingen. Dit kan leiden tot exportproducten voor NAVO-landen, samenwerking in Europese defensieprojecten zoals EDIDP, DEP en Horizon Europe.

Innovatiekansen[2]

- Opportuniteiten rond threat intelligence gathering en sharing, voor het beveiligen van het economisch weefsel in Vlaanderen, de kritische infrastructuur alsook de defensie infrastructuur.
- AI-gestuurde dreigingsdetectie en –voorspelling: Vlaamse cybersecurity expertise kan ingezet worden om zero-day aanvallen en geavanceerde dreigingen sneller te identificeren en te voorspellen.
- Cyberdisinformatie-analyse en weerbaarheid: Door kennis in data-analyse en taaltechnologie kan Vlaanderen tools ontwikkelen die desinformatiecampagnes vroegtijdig detecteren en neutraliseren.
- Security Operations Centers (SOC) as a Service: Vlaamse cybersecuritybedrijven kunnen geïntegreerde en meer geavanceerde SOC-diensten leveren aan kmo's in kritische sectoren, defensiepartners en overheden binnen België en Europa.
- Cyber Threat Intelligence Sharing Platforms: Innovatieve platformen voor real-time informatie-uitwisseling versterken de samenwerking tussen defensie, industrie en onderzoeksinstellingen.
- OT- en IoT-beveiliging: Vlaanderen kan door zijn sterke industriële en haveninfrastructuur oplossingen ontwikkelen voor de beveiliging van operationele technologie en slimme sensornetwerken.

Cloud and Infrastructure Security

Cloud and Infrastructure Security in een militaire context richt zich op het beveiligen van private, hybride en multi-cloudomgevingen waarin kritieke defensiegegevens en -applicaties draaien. Dit omvat Identity and Access Management (IAM) voor strikte toegangscontrole, virtualisatie- en containertechnologieën om workloads te isoleren en flexibel te beheren, en hardware-gebaseerde isolatie zoals Intel SGX of TDX voor het beschermen van gevoelige data, zelfs

wanneer systemen of hypervisors worden gecompromitteerd. Voor bedrijven in de defensiesector betekent dit het opzetten van zero-trust architecturen, versleutelde communicatie, en robuuste monitoring die zowel fysieke als virtuele infrastructuur dekt.

Het belang voor defensie is groot: betrouwbare en veilige cloud- en infrastructuuroplossingen zijn cruciaal voor het verwerken van real-time operationele data, AI-toepassingen, en internationale samenwerking binnen EU- en NAVO-kaders. Vlaamse bedrijven kunnen hierop inspelen door oplossingen te ontwikkelen zoals secure edge-computing nodes voor militaire drones, gecertificeerde soevereine clouds voor gevoelige informatie, of geïntegreerde IAM-platformen voor militaire toeleveringsketens.

Innovatiekansen[2]

- Soevereine en militaire cloudoplossingen – Vlaamse IT- en cybersecuritybedrijven kunnen eigen Europese cloudinfrastructuren ontwikkelen met focus op NAVO- en EU-compliance, wat digitale soevereiniteit versterkt.
- Geavanceerde IAM-platformen – Bedrijven kunnen innovatieve identity- en accessmanagementsystemen bouwen met multi-factor authenticatie en zero-trust principes, cruciaal voor militaire supply chains.
- Hardware-assisted security – Vlaamse high-tech spelers en chipbedrijven kunnen inzetten op SGX/TDX-gebaseerde isolatie en secure enclaves voor defensieapplicaties, gekoppeld aan Europese semiconductor-initiatieven.
- Virtualisatie- en containerbeveiliging – Cloud-native security oplossingen kunnen worden ontwikkeld om hybride en containeromgevingen in militaire datacenters en op het slagveld veilig te beheren.
- Edge computing voor defensietoepassingen – Vlaamse bedrijven kunnen veilige edge-nodes leveren voor AI toepassingen, drones en autonome voertuigen in tactische omgevingen.
- Versleutelde communicatie en dataopslag – Innovaties in kwantumveilige encryptie en data-slicing technologieën kunnen bijdragen aan robuuste militaire communicatiekanalen en dataopslag.
- Compliance- en risicobeheerplatformen – Vlaamse softwarebedrijven kunnen tools ontwikkelen die defensie helpen bij naleving van EU/NAVO-normen en automatische risico-assessment.
- Integratie met OT- en IoT-beveiliging – Door cloud security te koppelen aan operationele technologie en IoT in defensie-installaties kunnen Vlaamse bedrijven totaaloplossingen aanbieden voor kritieke infrastructuur.

OT and Network Security

OT- en netwerkbeveiliging zijn cruciaal voor inzetbaarheid en veerkracht van moderne krijgsmachten en bescherming van kritieke infrastructuur. Sensoren, voertuigen, wapens, logistiek en basisinfrastructuur draaien op ICS/SCADA, edge-compute en (semi-)gesloten netwerken die vaak decennia meegaan en moeilijk patchbaar zijn. Zonder microsegmentatie, zero trust voor OT, strikte identiteits- en sleutelbeheerprocessen, en snelle detectie/herstel

(EDR/NDR/IDS) kan één verstoring – sabotage, supply-chain-malware of misconfiguratie – operaties lamleggen, van havens tot radarposten. OT-security is daarmee niet alleen "compliance" (NIS2/IEC 62443), maar een operationele force multiplier: hogere beschikbaarheid, kortere MTTR en beter mission assurance.

Voor Vlaanderen liggen hier directe kansen: sterke embedded/ASIC/micro-elektronica en fotonica, industriële automatisering, maritieme en havengerelateerde OT, telco/netwerk-expertise, en cyberranges/digital-twin-kennis. Vlaamse KMO's kunnen waarde leveren in veilige veldgateways, protocol-firewalls, anomaly detection op industriële protocollen, supply-chain-assurance, ruggedized crypto/PKI, cross-domain solutions, en C-UAS-sensorfusie. Door aan te sluiten op Europese noden—veerkrachtige kritieke infrastructuur, interoperabiliteit met NAVO/EU-standaarden, en dual-use innovatie—kunnen bedrijven via o.a. EDF en (N)ATO-ecosystemen sneller schalen.

Innovatiekansen[2]

- Bescherming van kritieke infrastructuur (havens, luchtmachtbasissen, radarinstallaties) tegen cyber- en hybride aanvallen.
- NIS2, EU Cyber Resilience Act en NAVO Cyber Defence Pledge leggen nadruk op industriële netwerken en militaire logistiek.
- Haven- en maritieme OT-expertise (Port of Antwerp, Zeebrugge) → living labs voor dual-use beveiligingsoplossingen.
- Vlaamse KMO's in industriële automatisering en SCADA/ICS bieden nicheproducten voor segmentatie, anomaly detection en veilige remote access.
- Innovatie in ruggedized edge-apparatuur en secure gateways.
- Digitale twins voor OT-omgevingen.

End-point Security

End-point Security vormt een cruciale verdedigingslijn tegen cyberdreigingen door alle eindgebruikersapparaten – zoals laptops, mobiele toestellen, sensoren en industriële controle-eenheden – te beschermen tegen aanvallen en misbruik. In een militaire context omvat dit ook de beveiliging van draagbare commandosystemen, veldsensoren, drones en andere kritieke operationele apparatuur, waarbij zero-trusttoegang, versleutelde communicatie en real-time gedragsanalyse essentieel zijn om vijandige infiltratie of sabotage te voorkomen. Dit zorgt ervoor dat zowel IT- als OT-omgevingen van defensie robuust en veerkrachtig blijven, ook in tactische omstandigheden.

Voor Vlaanderen is dit belangrijk omdat een sterke end-point security niet alleen de nationale en Europese defensiebelangen beschermt, maar ook aanzienlijke economische opportuniteiten creëert. Vlaamse bedrijven kunnen innovatieve oplossingen ontwikkelen rond geavanceerde detectietechnologie, AI-gestuurde cyberdefensie en beveiliging van kritieke infrastructuur, die zowel in militaire als civiele domeinen inzetbaar zijn. Dit versterkt de Vlaamse positie binnen Europese defensie- en NAVO-programma's en opent exportmarkten voor hoogwaardige beveiligingstechnologie, wat bijdraagt aan economische groei en technologische soevereiniteit.

Innovatiekansen[2]

- Automatische dreigingsdetectie en –respons: Ontwikkeling van geavanceerde modellen voor anomaliedetectie op tactische eindpunten en geautomatiseerde incidentrespons.
- Zero-Trust en identiteitsbeheer: Integratie van zero-trustprincipes en gedecentraliseerde identiteitsoplossingen voor militaire eindpunten.
- Bescherming van OT- en IoT-eindpunten: Beveiliging van sensoren, drones en veldapparatuur in hybride IT/OT-omgevingen tegen cyberaanvallen.
- Versleutelde communicatie en data-soevereiniteit: Ontwikkeling van robuuste encryptieoplossingen voor mobiele en tactische militaire systemen.

Security monitoring and management

Security monitoring and management in een militaire cybersecuritycontext voor bedrijven omvat het continu bewaken, analyseren en beheren van alle digitale infrastructuren om dreigingen en anomalieën tijdig te detecteren en te neutraliseren.

Het gaat verder dan klassieke beveiliging en omvat governance, risk management en compliance: duidelijke processen en verantwoordelijkheden, risicogebaseerde beslissingen en rapportering richting defensie- en bedrijfsleiding. Dit vereist integratie van SIEM-oplossingen (Security Information and Event Management), SOAR-platformen (Security Orchestration, Automation & Response) en threat intelligence feeds, zodat bedrijven en militaire partners in real-time inzicht hebben in incidenten, kwetsbaarheden en risico's, met de mogelijkheid tot geautomatiseerde respons en forensische analyse.

Voor defensie is dit cruciaal om kritieke infrastructuren en militaire supply chains te beschermen tegen cyberaanvallen en hybride dreigingen, maar ook om te voldoen aan strenge governance-, riskmanagement- en compliance-eisen (GRC). Vlaamse bedrijven kunnen hierop inspelen door oplossingen te ontwikkelen voor geïntegreerde GRC-platformen die risicoanalyses, incidentrapportage en naleving van Europese en NAVO-normen (bv. NIS2, ISO 27001, EU Cyber Resilience Act) combineren. Concrete opportuniteiten liggen in automatisering van compliance-audits, risicogestuurde security monitoring voor kritieke infrastructuur zoals havens of energiecentrales, en AI-ondersteunde dashboards die defensie en bedrijfsleiders real-time inzicht geven in cyberrisico's en -incidenten. Vlaamse spelers kunnen zich zo positioneren als strategische partners voor Europese defensieprogramma's door niet enkel technologie, maar ook beheers- en governanceprocessen te leveren die interoperabel zijn binnen EU- en NAVO-context.

Innovatiekansen[2]

- Automatische dreigingsdetectie en –respons: Toepassen van security expertise in de ontwikkeling van geavanceerde modellen voor geautomatiseerde risico- en anomaliedetectie die voldoen aan EU- en NAVO-standaarden.
- Geïntegreerde GRC-platformen: KMO's in softwareontwikkeling kunnen oplossingen creëren die governance, risk en compliance combineren in één platform, afgestemd op NIS2- en ISO-normen.

- OT- en kritieke infrastructuurbeveiliging: Met de Vlaamse expertise in haven- en energiesectoren kunnen gespecialiseerde securityoplossingen voor industriële netwerken worden ontwikkeld, inclusief risicobeheersing.
- CyberGovernance-as-a-Service: Vlaamse cloud- en IT-bedrijven kunnen managed security services aanbieden die risicobeheer, monitoring en compliance integreren voor defensie en kritieke infrastructuren.

SURGE - Emerging Security Technology

SURGE: Develop and integrate emerging security technology

We identificeren een aantal belangrijke opkomende trends en technologieën binnen cybersecurity, waarvan we verwachten dat deze een belangrijke impact zullen hebben op de toekomstige beveiliging van onze kritische infrastructuur en defensie. We zien belangrijke innovatiekansen in het tijdig inzetten op deze innovatieprioriteiten, en deze vervolgens succesvol toe te passen binnen in zowel civiele als militaire toepassingen.

Post-Quantum Cryptografie (PQC)

Cryptografie is een heel cruciale bouwsteen in de beveiliging van applicaties en systemen, en wordt dan ook wijdverspreid toegepast, in onze dagdagelijkse apparaten en toepassingen, in ons thuis- en kantoornetwerk, maar ook binnen kritische infrastructuur en defensie.

Met de komst van quantum computing is het essentieel om deze cryptografische oplossingen quantum-veilig te maken en te beschermen tegen side-channel aanvallen. Hierbij is er nood aan zowel de ontwikkeling en implementatie van de volgende generatie, schaalbare post-quantum algoritmen en hun toepassingen, als het aanpassen van de hard- en softwaresystemen zodat ze crypto agility ondersteunen – dat ze met name vlot kunnen migreren van een oudere naar een nieuwere crypto oplossing.

Innovatiekansen[2]

- Het uitwerken van de volgende generatie cryptografische algoritmen en protocollen.
- Efficiënte implementaties van post-quantum crypto oplossingen, zowel in software als hardware.
- Het verhogen van crypto-agility van systemen en risico-gebaseerd migreren tussen cryptografische oplossingen.
- Het testen van software- en hardware implementaties op side-channel aanvallen.

Cybersecurity voor AI

Het gebruik en de integratie van AI in toepassingen en systemen zorgt voor ongekende innovatie opportuniteiten, zowel in de civiele markt als binnen defensie. Helaas wordt met het gebruik en de integratie van AI ook het aanvalsoppervlak mee uitgebreid, en zijn deze AI-gebaseerde toepassingen vaak kwetsbaar voor nieuwe AI-gerichte aanvalstechnieken, zeker in de context van GenAI/LLM-gebaseerde oplossingen.

Om voluit te kunnen inzetten op de AI-gebaseerde innovatie in kritische sectoren en in defensie, is het belangrijk om hun beveiligings- en betrouwbaarheidsaspecten volledig in kaart te kunnen brengen en te controleren, zowel tijdens de ontwikkeling als tijdens het gebruik van AI-gebaseerde systemen.

Innovatiekansen[2]

- Het vroegtijdig inschatten van mogelijke beveiligingsrisico's bij de integratie van AI in bestaande en nieuwe systemen, en nemen van afdoende maatregelen.
- Het testen en beschermen van operationele systemen tegen nieuwe AI-gerichte aanvalstechnieken.
- Het bestuderen van nieuwe aanvals- en verdedigingstechnieken tegen AI-gebaseerde systemen.

Sovereign Cloud

Vanuit een veranderende geopolitieke context alsook de kenmerkende oligopolie van enkele grote techbedrijven, is het belangrijk om controle te behouden (of terug in handen te nemen) over data, toepassingen en diensten – zowel naar confidentialiteit, integriteit als beschikbaarheid. Vandaar ook vraag naar een waaier van "soevereine clouddiensten", gaande van bijkomende beveiligingsmechanismen in bestaande cloud omgevingen tot volledig autonome, lokale datacenters (en diensten).

Innovatiekansen[2]

- Aanbieden van gedecentraliseerde (cloud)diensten voor soevereine en veilige opslag en verwerking van gegevens.
- Ontwikkeling van bijkomende beveiligingsmechanismes, die gebruikt kunnen worden in bestaande cloud omgevingen (bv gebaseerd op SGX, TDX).
- Cyber-resiliente cloud- en edge-infrastructuur – Vlaamse IT-bedrijven kunnen hybride cloud- en edge-oplossingen aanbieden die voldoen aan militaire security-standaarden en Europese soevereiniteitseisen.

Secure & Resilient Communication

Communication Security (ComSec) binnen cybersecurity omvat alle maatregelen, technieken en technologieën die de vertrouwelijkheid, integriteit en beschikbaarheid van communicatie waarborgen. In een militaire context voor bedrijven betekent dit het beveiligen van data- en spraakverbindingen, satellietcommunicatie, drones en commandosystemen tegen onderschepping, manipulatie of sabotage door tegenstanders. Bedrijven die actief zijn in defensietechnologie werken hier vaak met end-to-end encryptie, kwantumveilige communicatie, netwerksegmentatie en geavanceerde authenticatieprotocollen om te voldoen aan de hoge eisen van NAVO- en EU-defensiestandaarden.

Het belang van Communication Security voor defensie ligt in de noodzaak om kritieke militaire en strategische informatie te beschermen, ook in complexe multinationale operaties. Voor Vlaamse bedrijven creëert dit opportuniteiten in domeinen zoals kwantumcryptografie, satelliet- en 5G/6G-beveiliging, bescherming tegen protocolaanvallen en jamming, en veilige IoT-netwerken voor maritieme en luchtvaarttoepassingen.

Innovatiekansen[2]

- Kwantumveilige encryptie – Ontwikkeling van post-kwantum cryptografische oplossingen om communicatie toekomstbestendig te maken.
- Satelliet- en dronecommunicatiebeveiliging – Creëren van beveiligde communicatieprotocollen voor ruimtevaart- en luchtvaarttoepassingen.
- 5G/6G-beveiliging – Innovaties in mobiele netwerkbeveiliging voor tactische en kritieke militaire operaties.
- Resilient communicatie netwerken, die beschermen tegen protocolaanvallen, betrouwbare communicatie garanderen in geval van jamming en congestie.
- Secure IoT voor defensie – Ontwikkeling van veilige communicatiestandaarden voor onbemande voertuigen en sensornetwerken in militaire context.
- Cyber-resilience in maritieme communicatie – Versterking van communicatienetwerken in havens en offshore-gebieden en andere kritieke infrastructuur tegen cyberaanvallen.

CONTROL - Cyber Operations Technologies

CONTROL: Technology to support and enable Cyber Operations

Cyber Operations Technologies in een defensiecontext omvatten alle technologische oplossingen en diensten die militaire en civiele actoren ondersteunen bij het plannen, uitvoeren en coördineren van cyberoperaties. Het gaat zowel om defensieve als offensieve capaciteiten, waarbij data-analyse, automatisering, AI en veilige communicatie-infrastructuren samenkomen om cyberdreigingen tijdig te detecteren, tegen te houden en te neutraliseren. Deze technologieën zijn essentieel voor moderne krijgsmachten, waar digitale oorlogsvoering en bescherming van kritieke infrastructuur een strategische prioriteit zijn. Ze vormen de technologische ruggengraat voor alles van threat intelligence en situational awareness tot operational command en crisisrespons.

Het is voor Vlaanderen bijzonder opportuun om binnen Cyber Operations Technologies te investeren in Cyberspace Intelligence, Surveillance and Reconnaissance (CyISR), Cyber Defense Situation Awareness, Red Teaming en Command-and-Control (C2) services omdat deze technologieën een cruciale rol spelen in zowel defensie- als kritieke infrastructuurbeveiliging. CyISR en Cyber Defense Situation Awareness vormen de ruggengraat voor proactieve dreigingsdetectie en incidentrespons, terwijl Red Teaming cruciaal is voor het testen en valideren van de weerbaarheid. C2-services maken vervolgens een snelle coördinatie en besluitvorming mogelijk, zowel binnen militaire netwerken als voor civiel-militaire samenwerking in kritieke infrastructuur.

Een gefaseerde roadmap kan starten met de ontwikkeling van geavanceerde CyISR-sensoren en datafusie-technologieën (korte termijn), gevolgd door AI-gedreven situation awareness-platformen en simulatieomgevingen voor Red Teaming (middellange termijn). Op lange termijn kan Vlaanderen zich richten op volledig geïntegreerde Command-and-Control-diensten die interoperabel zijn binnen NAVO- en EU-standaarden. Door deze stappen gefaseerd uit te rollen, kunnen Vlaamse bedrijven niet alleen bijdragen aan nationale defensiebehoeften, maar ook een sterke internationale positie verwerven binnen Europese defensieprogramma's zoals EDF en PESCO, met economische spin-offs richting kritieke sectoren zoals energie, maritieme infrastructuur en smart cities.

Cyberspace intelligence, Surveillance and Reconnaissance (CyISR)

Cyberspace Intelligence, Surveillance and Reconnaissance (CyISR) in een militaire context omvat het geheel van digitale inlichtingen-, bewakings- en verkenningsactiviteiten in het cyberdomein. Voor bedrijven die actief zijn in defensie en kritieke infrastructuur betekent dit het ontwikkelen en inzetten van geavanceerde tools en diensten voor het verzamelen, analyseren en interpreteren van cyberdreigingen in real time. CyISR combineert threat intelligence, netwerkbewaking, data-analyse en vaak ook AI-gedreven anomaliedetectie om vijandige activiteiten vroegtijdig te identificeren en te neutraliseren, vergelijkbaar met klassieke ISR-operaties, maar dan volledig binnen het digitale slagveld.

Voor defensie is CyISR cruciaal om cyberaanvallen te voorkomen, missies te beschermen en operationele continuïteit te waarborgen. Voor Vlaamse bedrijven opent dit economische kansen in domeinen zoals AI-gebaseerde dreigingsdetectie, beveiligde communicatieplatformen, en digitale tweelingen voor cyberdreigingssimulatie. Concreet kunnen Vlaamse bedrijven oplossingen aanbieden voor NAVO-projecten, EU-defensie-initiatieven zoals EDIRPA, of cyber ranges voor training en testomgevingen, wat zowel hun technologische positie als exportmogelijkheden versterkt.

Innovatiekansen[2]

- AI-gedreven dreigingsanalyse – Vlaamse cybersecurity expertise kan worden ingezet voor real-time detectie en voorspelling van cyberaanvallen.
- Cyber threat intelligence platforms – Dankzij samenwerking met Europese partners kan Vlaanderen leidende rollen spelen in het opzetten van gedeelde threat intelligence hubs voor NAVO en EU.
- Edge computing en IoT-beveiliging – De industriële basis in Vlaanderen biedt mogelijkheden voor beveiliging van OT-netwerken in havens, energie en productieomgevingen.
- Automatisering en orkestratie van cyberdefensie – Vlaamse softwarebedrijven kunnen geavanceerde command-and-control platformen ontwikkelen voor snelle en gecoördineerde respons op cyberdreigingen.

Cyber Defense Situation Awareness

Cyber Defense Situation Awareness (CDSA) in een militaire context verwijst naar het vermogen om continu een volledig en actueel beeld te hebben van de digitale dreigingen, kwetsbaarheden en de status van alle IT- en OT-systemen. Voor bedrijven die actief zijn in defensie- of kritieke infrastructuurketens betekent dit het opzetten van geïntegreerde systemen die netwerkverkeer, endpoints, cloudomgevingen en industriële processen in real-time monitoren. Hierbij wordt gebruikgemaakt van geavanceerde sensoren, threat intelligence feeds, en AI-gestuurde analyses om cyberaanvallen vroegtijdig te detecteren, hun impact in te schatten en passende verdedigingsmaatregelen te coördineren.

Voor Vlaanderen is dit cruciaal omdat zowel de militaire als civiele sector steeds meer verweven zijn en cyberaanvallen vaak grensoverschrijdend zijn. Vlaamse bedrijven kunnen nieuwe economische opportuniteiten benutten door bijvoorbeeld AI-oplossingen te ontwikkelen voor vroegtijdige dreigingsdetectie, digitale tweelingen voor cyber-risicosimulatie, of beveiligde communicatieplatformen voor militaire en civiele toepassingen. Denk aan samenwerking met defensie voor maritieme cyberbewaking in Zeebrugge, of het leveren van cyber-sensoren en anomaly-detectiesoftware voor kritieke energie- en transportsystemen. Dit opent ook deuren naar Europese programma's zoals EDF en Horizon Europe, waarin dergelijke technologieën sterk worden gestimuleerd.

Innovatiekansen[2]

- AI-gestuurde dreigingsdetectie – Vlaamse cybersecurity expertise en data-analyse kan worden ingezet om geautomatiseerde systemen te bouwen die cyberaanvallen vroegtijdig herkennen en voorspellen.
- Digitale tweelingen voor cyberinfrastructuur – Sterke industriële en maritieme technologieclusters bieden kansen voor real-time simulaties van kritieke infrastructuur om cyberrisico's te analyseren en te beperken
- Integratie van OT- en IT-beveiliging – Vlaamse maakindustrie en havenbedrijven kunnen oplossingen ontwikkelen die industriële processen en IT-netwerken in één beveiligd overzicht integreren.
- Energie- en maritieme cyberbeveiliging – Vlaamse Blue Economy-initiatieven bieden opportuniteiten om cyberbeveiliging in offshore wind, energieopslag en scheepvaart te versterken.

Red teaming

Red teaming binnen cybersecurity in een militaire context houdt in dat gespecialiseerde teams – vaak samengesteld uit ethische hackers en veiligheidsexperts – realistische cyberaanvallen simuleren en uitvoeren op netwerken, systemen en operationele technologie (OT) om kwetsbaarheden bloot te leggen. In tegenstelling tot klassieke penetratietests richt redteaming zich niet alleen op technologische zwaktes, maar ook op processen, menselijke factoren en responscapaciteiten. Het doel is om de weerbaarheid van militaire organisaties en hun leveranciersketens te testen in realistische, vaak geavanceerde aanvalsscenario's, waarbij technieken van statelijke actoren of geavanceerde dreigingsgroepen worden nagebootst.

Voor defensie is dit cruciaal omdat moderne conflicten hybride zijn: naast fysieke dreigingen spelen digitale aanvallen een steeds grotere rol. Voor Vlaamse bedrijven creëert dit economische opportuniteiten in domeinen zoals OT-security voor havens en energie, AI-gedreven aanvalssimulaties en cyberranges voor training. Concreet kunnen bedrijven cybersecurity-KMO's redteamingdiensten ontwikkelen voor militaire partners of kritieke infrastructuurbeheerders, terwijl onderzoeksinstellingen gespecialiseerde opleidingen en testomgevingen kunnen aanbieden. Dit opent de deur naar Europese defensieprojecten, NAVO-samenwerkingen en commerciële toepassingen voor sectoren als scheepvaart, luchtvaart en energie.

Innovatiekansen[2]

- kritieke infrastructuurbeveiliging – Vlaanderen biedt heel wat kansen voor red teaming oplossingen gericht op kritische sectoren zoals scheepvaart, havens en energie-infrastructuur.
- Simulatie en serious gaming – De Vlaamse gaming- en XR-sector kan realistische, interactieve simulaties ontwikkelen voor red teaming-training en besluitvorming onder druk.

Command-and-Control services

Command-and-Control (C2) services binnen cybersecurity vormen de ruggengraat van digitale militaire operaties, waarbij real-time coördinatie, situational awareness en snelle besluitvorming cruciaal zijn. In een militaire context voor bedrijven omvat dit beveiligde communicatienetwerken, gedistribueerde data-analyse en AI-ondersteunde besluitvormingstools die zorgen voor een naadloze koppeling tussen operationele eenheden, sensoren en commandoposten. Technologieën zoals zero-trust netwerken, quantum-resistente encryptie en edge computing worden hierbij steeds belangrijker om zowel cyber- als kinetische operaties te beschermen tegen vijandige actoren.

Voor defensie en de Vlaamse economie biedt de ontwikkeling van C2-services grote opportuniteiten. Vlaamse bedrijven met expertise in cybersecurity, AI, 5G/6G-communicatie en high-performance computing kunnen bijvoorbeeld oplossingen leveren voor beveiligde cloudgebaseerde C2-platformen, digitale tweelingen voor militaire operaties en autonome dronesystemen met cyberveilige commandostructuren. Concrete kansen liggen in samenwerking met NAVO-initiatieven, Europese defensieprogramma's en maritieme projecten zoals beveiligde C2-netwerken voor offshore infrastructuur en havenbescherming, waarin Vlaanderen via zijn maritieme en technologische clusters een sterke rol kan spelen.

Innovatiekansen[2]

- Beveiligde 5G/6G-communicatie – Vlaanderen heeft een solide telecom- en IoT-sector die oplossingen kan bouwen voor lage-latentie, versleutelde C2-netwerken voor militaire en kritieke infrastructuur.
- Digitale tweelingen voor simulatie en training – Met expertise in industrie 4.0 en digital twins kan Vlaanderen gesimuleerde C2-omgevingen creëren voor defensietraining en risicobeheer.
- Autonome systemen en drones – Vlaanderen beschikt over sterke maakindustrie en robotica-expertise voor cyberveilige commandostructuren in autonome lucht- en maritieme systemen.
- Maritieme en havenbeveiliging – Met sterke maritieme clusters kan Vlaanderen C2-oplossingen ontwikkelen voor offshore windparken, havens en logistieke ketens onder dreiging van cyberaanvallen.

Conclusie

Vlaanderen beschikt over uitzonderlijke troeven om een leidende rol te spelen in cybersecurity voor kritische infrastructuur en defensie. Met meer dan veertig jaar ervaring in cybersecurityonderzoek en een sterk industrieel weefsel van meer dan 170 bedrijven, heeft Vlaanderen een internationale reputatie opgebouwd in domeinen zoals veilige softwareontwikkeling, systeem- en hardwarebeveiliging, OT- en netwerkbeveiliging en security monitoring. Het leiderschap van initiatieven zoals het OWASP SAMM-project en de ontwikkeling van de wereldwijd gebruikte AES encryptie standaard onderstrepen de innovatieve capaciteit en de maturiteit van de Vlaamse cybersecuritysector.

Tegelijkertijd worden de uitdagingen groter: toenemende geopolitieke spanningen, geavanceerde digitale dreigingen en de vraag van nationale en internationale defensiepartners (NAVO, EU, Belgische Defensie) creëren een dringende nood aan robuuste en schaalbare cyberdefensieoplossingen. Het Vlaamse Defensieplan koppelt daarom de sterktes van Vlaamse hightechbedrijven, kennisinstellingen en digitale infrastructuurspelers aan deze internationale noden.

De vier strategische pijlers – **FORTIFY** (security-by-design), **SHIELD** (operationele beveiliging), **SURGE** (emerging technologies) en **CONTROL** (cyberoperaties) – bieden een toekomstgericht kader waarin Vlaanderen niet alleen defensieve capaciteiten kan versterken, maar ook nieuwe industriële kansen kan creëren. Innovatie in post-quantumcryptografie, beveiliging van AI-technologie, soevereine cloudoplossingen en veilige communicatienetwerken kan Vlaanderen positioneren als betrouwbare, toekomstgerichte technologiepartner voor defensie en kritieke infrastructuur.

Door deze sterktes te valoriseren en samenwerking tussen industrie, onderzoek en beleid te intensiveren, kan Vlaanderen een Europese koploper worden in geavanceerde cyberdefensie-oplossingen – met een dubbele impact: verhoogde nationale en internationale veiligheid én een sterke impuls voor economische groei en technologische innovatie.

Impulsprogramma Defensie

Oriëntatie roadmap:

Autonome Technologie voor Veiligheid en Defensie

Flanders Make vzw

24 Oktober 2025

Table of Contents

Visie en context voor autonome systemen in defensie

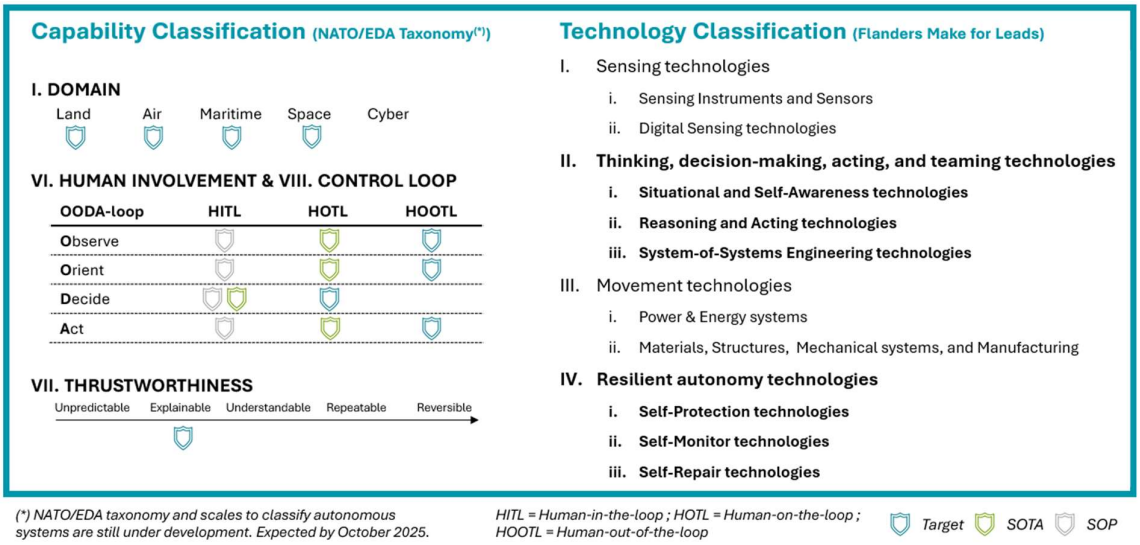
De nieuwste technologieën zorgen voor een ware revolutie in de manier hoe uitdagingen in veiligheid en defensie aangepakt worden. De belangrijkste impact van technieken zoals onder andere AI, semantische perceptie, veilige vormen van data communicatie, nieuwe sensing technologie, hogere performantie van edge hardware in combinatie met een algemene verregaande vorm van digitalisatie zorgt ervoor dat systemen steeds meer intelligentie bevatten om zich aan te passen aan de omgeving en communicatie technologie bevatten om te interageren met andere stakeholders in het ecosysteem.

Op die manier **verschuift de rol van de 'human expert' vanuit het real-time operationele richting tactisch en strategische.** Experts in veiligheid en defensie krijgen op deze manier een heel andere rol toebedeeld in conflict situaties en zullen sterk afhankelijk worden van de 'capabilities' en 'skills' van de vloot van intelligente systemen die ze beheren. Deze vloten van systemen zullen trouwens niet alleen defensieve of offensieve skills krijgen, maar in de nabije toekomst ook 'refurbishing' en zelfs 'upgrading' capabilities om zichzelf of andere devices in de vloot te herstellen, sterker te maken of zelfs nieuwe skills te geven.

In deze oriëntatieroadmap rond 'Autonome Technologie voor Veiligheid en Defensie' zal de focus niet zozeer liggen op het ontwerp van individuele, intelligente devices of de veilige communicatie hiertussen[1], maar veeleer over **hoe een hybride vloot van intelligente rijdende, varende of in de lucht of ruimte vliegende drones samen en autonoom een opdracht kunnen uitvoeren** in een ongestructureerde omgeving, met beperkte communicatiemogelijkheden en onder dreiging van vijandelijke aanwezigheid. Mogelijke toepassing van deze technologie is niet enkel tijdens een conflictsituatie, maar evenzeer vooraf binnen een monitoring of exploratie missie of nadien, bijvoorbeeld bij het demilitariseren van zones.

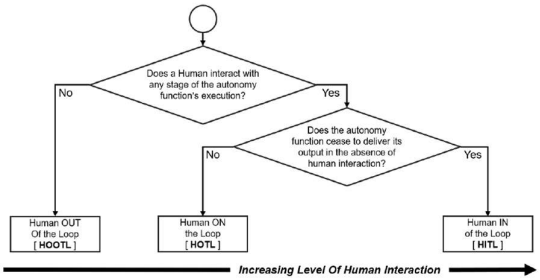
Deze roadmap sluit nauw aan bij de NAVO/EDA taxonomie oefening over autonome systemen die momenteel loopt en waarvan er eind 2025, na presentatie op REPMUS 2025, een publicatie wordt verwacht. Voor EDA kadert dit binnen hun Action Plan Autonomous Systems (APAS) project. Deze taxonomie klasseert technologieën en systemen volgens niveau van autonomie om procurement en technologisch onderzoek hierrond te faciliteren. De tussentijdse versie (juni 2025) van deze taxonomie wordt in deze oriëntatie roadmap gebruikt om de doelstelling en scope te beschrijven, zoals aangegeven in volgende figuur:

[1] Hier verwijzen we naar andere oriëntatieroadmaps bvb rond CyberSecurity (communicatie), AI for Defence, Geo-intelligence of FLAG (UAS, Luchtvaart en Drones).



Figuur: Links: Doelstelling en scope van deze oriëntatie roadmap volgens de tussentijdse (juni 2025) NAVO/EDA taxonomie voor classificatie autonome systemen op basis van hun capabilities ; Rechts: Technologie Taxonomie om de enabling technologieën te beschrijven

Binnen deze NAVO/EDA context beschrijft men het niveau van autonomie vanuit de betrokkenheid van de mens per functionele taak. Deze taken worden bekeken vanuit de OODA-loop (Observe, Orient, Decide en Act) waarbij de menselijke betrokkenheid gaat van Human-in-the-Loop (HITL) over Human-on-the-Loop (HOTL) tot Human-out-of-the-Loop (HOOTL). **Een taak wordt pas autonoom beschouwd vanaf HOTL**[2]. Een systeem wordt pas volledig autonoom beschouwd als alle taken minstens HOTL zijn. Onbemande systemen ('Unmanned Systems') zijn daarom ook niet noodzakelijk autonoom.



Figuur : Onderscheid tussen HITL, HOTL en HOOTL gedefinieerd door NAVO/EDA in hun tussentijdse Taxonomie juni 2025

Aan de hand van de **OODA-loop** is er een duidelijke ambitie vooruitgeschoven om deze de komende jaren **sterk 'autonoom' te maken**, startend vanuit de huidige technologie (State-of-Practice, SoP). De SoP is vaak eerder 'tele-operated' of 'remote-operated' waarbij verschillende taken, waaronder beslissingsneming ('Decision'), HITL vereisen[3][4][5][6]. Daarom wordt deze SoP dus niet als autonoom beschouwd. EDA verwacht dat op korte tot middellange termijn deze systemen semi-autonoom kunnen worden[7]. Volledige autonomie is het lange termijn doel waarbij alle OODA-loop taken volledig HOOTL zullen zijn. De OODA-loop zal ook het raamwerk zijn waarbinnen de activiteiten binnen deze roadmap zullen worden gesitueerd.

[2] RMA (Royal Military Academy), "Payload carrier UAS for tactical logistics", april 2025
[3] CSIS (Center for Strategic & International Studies), "Ukraine's Future Vision and Current Capabilities for Waging AI-enabled Autonomous Warfare", maart 2025
[4] Breakingdefense.com, "Trained on classified battlefield data, AI multiplies effectiveness of Ukraine's drones: Report", maart 2025
[5] Defensie, "Strategische Visie Defensie 2025", juli 2025
[6] https://www.vrt.be/vrtnws/nl/2025/08/02/gronddrones-oekraine-arnaud-de-decker/
[7] EDA, "The EDA Action Plan on Autonomous Systems", 2024

EDA beschrijft in hun APAS acht technische functionaliteiten waarover een systeem moet kunnen beschikken om als autonoom beschouwd te worden[8]. Geïnspireerd door de functionele technologie taxonomie van NASA[9] kunnen deze technologieën in de Leads Technologie Taxonomie voor autonome defensiesystemen opgedeeld worden in vier categorieën dewelken ook matchen met het Vlaams ecosysteem. Twee specifieke categorieën zijn prioritair voor onze oriëntatieroadmap omdat die direct gelinkt zijn met het inzetten van hybride vloten van slimme devices met een verregaande graad van autonomie en dus ook resilience:

II. Thinking, Decision-Making, Acting and Teaming technologies

Gaat in het algemeen over technologie die onmiddellijk gelinkt is aan uitwisseling van geo-specifieke informatie tussen/over verschillende slimme, mobiele devices, als input voor navigatie en/of als basis voor het uitvoeren van een bepaalde autonome missie (bvb scannen van risico gebieden op mijnen). Vervolgens wordt deze informatie gebruikt voor het plannen, aansturen en uitvoeren van taken van een system-of-systems waarbij verschillende systemen samenwerken als één team. Hierbij wordt zowel naar de operatie van een system-of-systems gekeken als over diens hele levenscyclus.

IV: Resilient autonomous technologies

Deze technologie categorieën slaan zowel op device niveau (bvb self-assessment van de functies) als op vlootniveau waarbij vanuit een health-monitoring aanpak via redundantie op skill niveau missies kunnen gerealiseerd worden, ondanks het falen van een bepaalde device-specifieke skill of zelfs het wegvallen van een volledige device.

Deze technologie oriëntatieroadmap is sterk gebaseerd op 'Foresight' en benut ten volle de technologie en applicaties die aangeboden worden vanuit andere oriëntatie roadmaps. Door deze hoge graad van innovatie vanuit de ambitie om op de grens van state-of-the-art (SOTA) te gaan werken, zal het zeer belangrijk worden om niet alleen na te denken over beschikbare technologieën, maar ook over hoe nieuwe technologieën sneller kunnen worden geïntegreerd. Daarom zal de **focus niet enkel op het operationele vlootmanagement liggen – wat technologisch al zeer uitdagend is - maar nog meer op het boosten van de innovatiecyclus**. Het wordt namelijk niet alleen de uitdaging om betere vloten te hebben dan de competitie, maar nog belangrijker, sneller te leren van voorbije missies en nieuwe, SOTA technologieën te adopteren. Om hierin te slagen binnen een internationaal consortium van meerdere bedrijven en stakeholders zal het essentieel zijn om zeer actief in te zetten op innovatieve ontwerp en management methodologieën die binnen het algemene kader van 'Systems-Of-Systems' (SoS) kunnen worden gesitueerd[10].

Deze **roadmap speelt in op 'emerging technologies'**, die vaak nog in ontwikkeling zijn binnen de universiteiten, onderzoekcentra of vlaamse bedrijven inclusief high-tech start-ups, scale-ups, en KMO's. Om een positie op te nemen op het Europees vlak, zal het zaak worden om zo snel mogelijk de krachten te bundelen in de vorm van een ecosysteem met een duidelijke strategie rond formeel samenwerkingsmodel (eg Open-Source Software model), opbouw en delen van strategische datasets én intensieve samenwerking binnen een confidentiële en secure co-creatie centra.

[8] EDA, "The EDA Action Plan on Autonomous Systems", 2024

[9] https://techport.nasa.gov/taxonomy/8817

[10] Binnen een internationaal kader wordt al jaren ingezet op de zogenaamde DoDaF framework voor het beheer van complexe, totaalsystemen zowel ogenblikkelijk als vanuit een lifecycle management perspectief: https://dodcio.defense.gov/Library/DoD-Architecture-Framework/dodaf20_ontology1/

Sterk Vlaams ecosysteem rond autonome technologie

Vlaanderen heeft een sterk ecosysteem van high-tech bedrijven, onderzoekcentra en industriefederaties voor onderzoek en ontwikkeling van verscheidene technologieën om de graad van autonomie van systemen te verhogen. Deze technologieën worden meestal in de eerste plaats ontwikkeld voor civiele toepassingen, maar vinden ook hun toepassing binnen defensienoden. In totaal zijn er, onder andere uit Flanders Make's klantendatabase en uit de Agoria BSDI ledenljist, ***meer dan 120 bedrijven in Vlaanderen*** geïdentificeerd die technologie ontwikkelen die mogelijk toepasbaar is voor autonome systemen voor veiligheid en defensie.

Methode om het Vlaamse Ecosysteem voor autonome technologie te categoriseren

Voor het management van de technologieën voor autonome systemen binnen defensie en veiligheid werd een Technologie Taxonomie opgesteld. Deze is gebaseerd op de functionele beschrijving van autonome systemen door EDA binnen hun APAS project[11] en de Technologie Taxonomie 2024 van NASA[12]. De classificatie van de technologische bouwblokken kan vervolgens gelinkt worden aan de expertisedomeinen van de bedrijven en onderzoekscentra in het Vlaamse ecosysteem.

De **Technologie Taxonomie onderscheidt vier brede technologiedomeinen**:

I. ***Sensing Technologies***: Dit zijn technologieën om data te verzamelen over de omgeving of zichzelf via fysieke sensoren, meetsystemen of digitale tools. Deze technologieën ondersteunen de "Observe"-fase van de OODA-loop.
II. ***Thinking, Decision-making, Acting, and Teaming Technologies***: Dit zijn technologieën de verzamelde data uit ('I. Sensing Technologies') verwerkt om er inzichten uit te halen, beslissingen te nemen en actie aan te sturen. Hierbij dient rekening gehouden te worden met de andere systemen binnen hetzelfde system-of-systems voor optimale synergiën. Deze technologieën ondersteunen de "Orient"-, "Decide"- en "Act"-fase van de OODA-loop.
III. ***Movement Technologies***: Dit zijn technologieën die het systeem de besloten actie uit ('II. Thinking, …') effectief te laten uitvoeren. Dit omvat zowel technologieën om het systeem van de juiste energie te voorzien alsook deze energie om te zetten in de gewenste beweging.
IV. ***Resilient Autonomy Technologies***: Dit zijn technologieën die ervoor zorgen dat het systeem en het system-of-systems zichzelf autonoom kan monitoren, beschermen en indien nodig herstellen.

Voor elk van deze vier domeinen en hun subdomeinen zijn de stakeholders binnen het Vlaamse ecosysteem in kaart gebracht.

[11] EDA, "The EDA Action Plan on Autonomous Systems", 2024
[12] https://techport.nasa.gov/taxonomy/8817

Overzicht van het Vlaamse Ecosysteem

Technology Domain	Subdomain	Definition	Primary function and application	Key Technologies within the Flemish ecosystem	Companies in Flanders
I. Sensing Technologies	I.I. Sensing Instruments and Sensors	Technologieën om data te verzamelen over de omgeving of zichzelf via fysieke sensoren, meetsystemen.	De vloot van autonome systemen en de individuele systemen fysische data laten verzamelen.	Halfgeleider sensoren, fotonica-gebaseerde sensoren, multi- en hyperspectrale camera's, LiDAR, Radar, Infrarood, GNSS, …	**> 25**
	I.II. Digital Sensing Technologies	Technologieën om data te verzamelen over de omgeving of zichzelf via digitale tools.	De vloot van autonome systemen en de individuele systemen digitale data laten verzamelen.	Robotic Process Automation (RPA), data scraping, …	
II. Thinking, Decision-making, Acting, and Teaming Technologies	II.I. Situational and Self-Awareness Technologies	Situatiebewustzijn en zelfbewustzijnstechnologieën ondervragen, identificeren en evalueren zowel de toestand van de omgeving als de toestand van het systeem.	De vloot van autonome systemen en de individuele systemen inzichten laten genereren uit de verzamelde data.	Machine Vision, semantische perceptie en wereld modelleren voor navigatie, robotica, terrein inspectie, …	**> 45**
	II.II. Reasoning and Acting Technologies	Redeneer- en handel-technologieën analyseren en evalueren situaties (heden, toekomst of verleden) ten behoeve van besluitvorming en het aansturen van acties om een doel of missie te bereiken.	De vloot van autonome systemen en individuele systemen beslissingen laten nemen en acties genereren op basis van de gegeneerde inzichten.	Navigatie software, Planning en Scheduling software, …	
	II.III. System-of-Systems Engineering Technologies	Deze technologieën maken het mogelijk om een verzameling van onafhankelijke systemen te integreren tot een groter systeem dat unieke capaciteiten levert die geen van de afzonderlijke systemen op zichzelf kan realiseren.	Ervoor zorgen dat de individuele systemen binnen een vloot samenwerken als één team alsook over hun levenscyclus.	Collaboration technologieën, interaction technologieën en system engineering technologieën.	

Technology Domain	Subdomain	Definition	Primary function and application	Key Technologies within the Flemish ecosystem	Companies in Flanders
III. Movement Technologies	III.I. Power and Energy Systems	Systemen of componenten om energie op te slaan, om te zetten of over te brengen.	Het autonome systeem voorzien van energie en deze energie omzetten naar de gewenste vorm of arbeid.	Motoren, batterijen, transmissies, tandwielen, lagers.	**> 15**
	III.II. Materials, Structures, Mechanical Systems, and Manufacturing	Mechanische systemen, structuren en high-tech materialen waaruit deze bestaan alsook de productiemethodes om deze structuren te produceren.	De arbeid omzetten naar de gewenste actie door middel van een fysieke structuur die geproduceerd dient te worden.	Metalen, kunststoffen, lichtgewicht structuren, topologie optimalisatie, CAD software, tribologie, vermoeiing, structuurdynamica, additive manufacturing, …	**> 30**
IV. Resilient Autonomy Technologies	IV.I. Self-Protection Technologies	Zelfbeschermingstechnologieën stellen systemen in staat om zich proactief of reactief te verdedigen tegen dreigingen.	De vloot en het systeem autonoom laten uitvoeren van beschermende maatregelen zoals bijvoorbeeld ontwijkende manoeuvres, het uitschakelen van kwetsbare subsystemen of het activeren van fysieke en digitale beschermlagen.	Tools ter ondersteuning van beslissingsneming van acties van de vloot	**> 20** (incl. verschillende bedrijven binnen Tech Domain II)
	IV.II. Self-Monitor Technologies	Zelfmonitoringstechnologieën zorgen ervoor dat het systeem voortdurend zijn eigen interne toestand bewaakt, inclusief mechanische, elektrische en softwarecomponenten.	Autonome vloten vroegtijdig degradatie, afwijkingen of aanstaande defecten te signaleren en hierop besluiten en actie ondernemen over bijvoorbeeld noodprocedures of onderhoud.	State-of-Health inschatting en anomalie detectie op vlootniveau	
	IV.III. Self-Repair Technologies	Deze technologieën stellen systemen in staat om zichzelf gedeeltelijk of volledig te herstellen, zodat ze hun missie kunnen voortzetten.	Autonome vloten en systemen zichzelf laten herstellen in geval van schade aan UXVs of andere agenten.	Tools ter ondersteuning van beslissingsneming en update van vloot formatie en ReX acties.	

Key Lessons Learned

Op basis van de bovenstaande ecosysteem mapping kunnen volgende voorname inzichten bekomen worden:

- Meerderheid van de geïdentificeerde bedrijven in het vlaamse ecosysteem rond autonome systemen is (publiekelijk) **gefocust op de civiele industrie en publiekelijk (nog) niet actief in de defensie-industrie**. Bijgevolg is er voor autonome technologie voor defensie een veel groter potentieel dan momenteel publiek is gekend.
- De meeste bedrijven in het vlaamse ecosysteem zijn **actief op meer dan één technologiedomein** binnen de bovenstaande taxonomie. Bovendien zijn er ook verschillende bedrijven die werken aan de **integratie van verschillende domeinen** zoals volledige outdoor voertuigen en machines.
- De geïdentificeerde vlaamse bedrijven zijn een **mix van zowel start-ups, scale-ups, KMO's als multinationals** verdeeld over verschillende stappen van de waardeketen.

Oriëntatieroadmap Autonome Technologie voor Veiligheid en Defensie

De oriëntatieroadmap rond 'Autonome Technologie voor Veiligheid en Defensie' is opgebouwd uit ***twee complementaire pijlers*** om tot een totaalconcept te komen (zie figuur pagina 14):

- De innovatiecylus op vlootniveau versnellen
- Weerbare, autonome missies met hybride vloten van drones/UXV's

Pijler 1: De innovatiecyclus op vlootniveau versnellen

Deze pijler zet in op het **samenstellen van intelligente autonome vloten doorheen diens levenscycli**. Hier wordt niet alleen gefocust op de operationele fase met de capaciteiten van de vloot om de missie uit te voeren, maar ook op de andere fases in de end-to-end levenscyclus met het inzetten van slimme, mobiele eenheden als onderdeel van de vloot om tijdens het verloop van de missie de nodige herstellingen en upgrades uit te voeren om steeds de hoogste graad van weerbaarheid op vlootniveau te hebben.

Deze pijler is opgebouwd uit ***drie bouwstenen***:

- Gedigitaliseerd end-to-end levenscyclusbeheer
- Gedistribueerde microfabrieken
- Productietechnieken en ReX-methoden

Bouwblok 1.1: Gedigitaliseerd end-to-end levenscyclusbeheer

Gedigitaliseerd end-to-end levenscyclusbeheer heeft als doel **over de verschillende levenscycli van de vloten de samenwerking, onderlinge interactie en samenstelling te optimaliseren** door voortdurend te leren van de huidige en voorgaande levenscycli om zowel de prestaties als de doorlooptijd te verbeteren. Dit vereist dat data wordt verzameld en gedeeld over de verschillende fases van de levenscyclus heen zoals bijvoorbeeld het gebruiken van data tijdens de operationele fase tijdens de herstelfase of ontwerpfase van de volgende versie.

Enkele ***voorbeelden*** van uitdagingen binnen deze bouwblok zijn de integratie van real-time telemetrie van UXV's met onderhoudslogboeken of het kiezen van de meest geschikte ReX actie voor een UXV rekening houdend met vroegtijdige schadedetectie bij andere UXV's tijdens de lopende operatie.

Thematische doelstellingen – Innovatiekansen

- Waarborgen van de **samenwerking en interactie** van verschillende autonome systemen **over hun eigen en elkaars levenscycli heen** zodat informatie uit elke levensfase van elk systeem met elkaar gedeeld wordt om continu van elkaar te leren.
- Optimale **samenwerking en interactie** tussen verschillende autonome systemen met **verschillende specialisaties, versies en state-of-health**.
- Steeds de **optimale vlootsamenstelling van autonome systemen** voor de missie garanderen, rekening houdend met de verschillende specialisaties, versies en state-of-health van de verschillende systemen.

Bouwblok 1.2: Gedistribueerde microfabrieken

Het **herstel en upgraden van de vloot gebeurt in gedistribueerde (semi-)autonome microfabrieken**. Deze vormen samen een netwerk van geografisch verspreide kleinschalige, mogelijks mobiele, faciliteiten gespecialiseerd in lokale productie, onderhoud en ReX van High-Mix, Low-Volume producten. Deze microfabrieken zijn zelf een systeem binnen de autonome systems-of-systems vloot.

Enkele ***voorbeelden*** van uitdagingen binnen de gedistribueerde microfabrieken bouwblok is de integratie van geavanceerde en nauwkeurige productie- en ReX technologie in compacte verplaatsbare modules of het waarborgen van de kwaliteit en nauwkeurigheid in een extreme omgeving.

Thematische doelstellingen – Innovatiekansen

- **Flexibele, compacte en verplaatsbare** omgeving voor productie, onderhoud en ReX van verschillende versies van de autonome systemen die voor de missie gebruikt worden.
- De microfabrieken voeren hun taken uit met **minimale menselijke tussenkomst** (**HOTL**, zie pijler 2).
- Gedistribueerde microfabrieken met elk hun eigen specialisatie **werken optimaal samen binnen een system-of-systems**.

Bouwblok 1.3: Productietechnieken en ReX-methoden

Deze microfabrieken beschikken over alle nodige functionaliteiten die nodig zijn voor **lokale productie en ReX** (hergebruik, revisie, remanufacturing en recycling). Voorbeelden hiervan zijn additive manufacturing, visuele kwaliteitsinspectie, niet-destructieve inspectie en kwalificatie van vlootelementen voor nauwkeurige conditiebewaking, met als doel het nemen van passende ReX-maatregelen.

Enkele ***voorbeelden*** van uitdagingen binnen deze bouwblok zijn het verleggen van de SOTA in additieve manufacturing technieken of niet-destructieve inspectie rekening houdend met de korte beschikbare doorlooptijd en extreme omstandigheden.

Thematische doelstellingen – Innovatiekansen

- Ontwikkeling van **mobiele en compacte productie en ReX technieken** die toepasbaar zijn in een verplaatsbare en compacte ruimte met maximaal hergebruik van materialen en componenten.
- Ontwikkeling van **mobiele en compacte niet-destructieve inspectietechnieken** die inzetbaar zijn voor kwaliteitscontrole en conditiebewaking in een verplaatsbare en compacte ruimte.

Pijler 2: Veerkrachtige, autonome missies met hybride vloten van drones/UXV's

Deze pijler focust op het **autonoom opereren van vloten van intelligente drones of UXV's** in ongestructureerde omgevingen onder vijandige dreiging en zonder betrouwbare communicatie.

Voortbouwend op de OODA-loop is deze pijler opgebouwd uit ***vijf bouwstenen***:

- Observeren ('Observing')
- Oriënteren ('Orienting')

- Beslissingsneming (‘Deciding’)
- Handelen (‘Acting’)
- Teamvorming en samenwerking (‘Teaming’)

Bouwblok 2.1: Observeren (‘Observing’)

Het observeren omvat het **verzamelen van gegevens** uit verschillende lagen van de omgeving of het interne systeem zelf.

Enkele ***voorbeelden*** van uitdagingen binnen het observeren zijn het capteren van omgevingsparameters in extreme weersomstandigheden, het capteren van data over gecamoufleerde objecten, of het capteren van specifieke details op het terrein vanop grote afstand.

Thematische doelstellingen – Innovatiekansen

- Het verzamelen van de gegevens dient te gebeuren zonder menselijke tussenkomst (**HOOTL**).
- Robuuste en betrouwbare sensoren die **kunnen omgaan met extreme externe invloeden** zoals weersomstandigheden of verstorende signalen.
- Uitgebreid portfolio aan sensoroplossingen om **niet-zichtbare objecten zichtbaar te maken**.

Bouwblok 2.2: Oriënteren (‘Orienting’)

Voor het oriënteren dienen de **verzamelde gegevens te worden verwerkt, geanalyseerd, gecontextualiseerd en omgezet naar informatie en inzichten ten behoeve van besluitvorming**. Dit omvat het onderzoeken, identificeren en evalueren van zowel de toestand van de omgeving als van het systeem.

Enkele ***voorbeelden*** van uitdagingen binnen het oriënteren zijn het correct identificeren van gecamoufleerde objecten met semantische perceptie, het inschatten van de state-of-health van ULVs, of het detecteren van anomalieën op het terrein.

Thematische doelstellingen – Innovatiekansen

- De ‘orienting’ fase dient te gebeuren zonder menselijke tussenkomst (**HOOTL**).
- Intelligente algoritmes die sensor data combineren en **verborgen objecten, patronen of inzichten bloot leggen** om real-time een gemeenschappelijk en betrouwbaar wereldbeeld op te bouwen voor de beslissingsnemingsfase.

Bouwblok 2.3: Beslissingsneming (‘Deciding’)

Tijdens de beslissingsneming worden deze **verzamelde inzichten gebruikt om te redeneren, mogelijke taken te analyseren en evalueren, om daarop de meest geschikte actie te kiezen** om de doelstellingen te bereiken.

Enkele ***voorbeelden*** van uitdagingen binnen de beslissingsneming zijn het kiezen van de meest geschikte missie actie of het plannen in tijd en ruimte van missies en acties van vlootelementen.

Thematische doelstellingen – Innovatiekansen

- De “Decide” fase dient te kunnen gebeuren zonder menselijke tussenkomst maar met menselijke interactie mogelijk (**HOTL**).

- Optimale trade-off tussen **optimale en snelle besluitvorming** voor het **real-time** plannen en controleren van acties gaande van de operatie van een missie tot het ontwerp, productie en ReX van autonome systemen en vloten.

Bouwblok 2.4: Handelen ('Acting')

De bouwblok Handelen zorgt voor het uitvoeren van de gekozen actie en het monitoren van de directe resultaten om de correcte uitvoering te waarborgen.

Enkele ***voorbeelden*** van uitdagingen binnen deze bouwblok zijn het robuust en betrouwbaar werken van de actuatoren en aandrijvingen onder extreme weersomstandigheden en landschappen.

Thematische doelstellingen – Innovatiekansen

- Het uitvoeren van acties dient te gebeuren zonder menselijke tussenkomst (**HOOTL**).
- Robuuste en betrouwbare **actuatoren en aandrijvingen** die kunnen **omgaan met extreme externe invloeden** zoals weersomstandigheden of verstorende signalen.
- **Robuuste, sterke, slijtvaste mechanismen en structuren** die de uptime van de autonome systemen garanderen en voorspelbaar maken.
- **Energie-efficiënte en lichtgewicht mechanismen en structuren** die de operationele duur van de autonome systemen maximaliseren onder beperkte energievoorraad.

Bouwblok 2.5: Teamvorming en samenwerking ('Teaming')

De systemen en agenten werken niet in silo's, dus is ook de bouwblok 'Teaming' van groot belang. Deze samenwerkings- en interactietechnologieën moeten **meerdere systemen of agenten optimaal laten samenwerken als één hybride team**. Deze systemen of agenten kunnen bemand of onbemand zijn, evenals menselijke operatoren zijn.

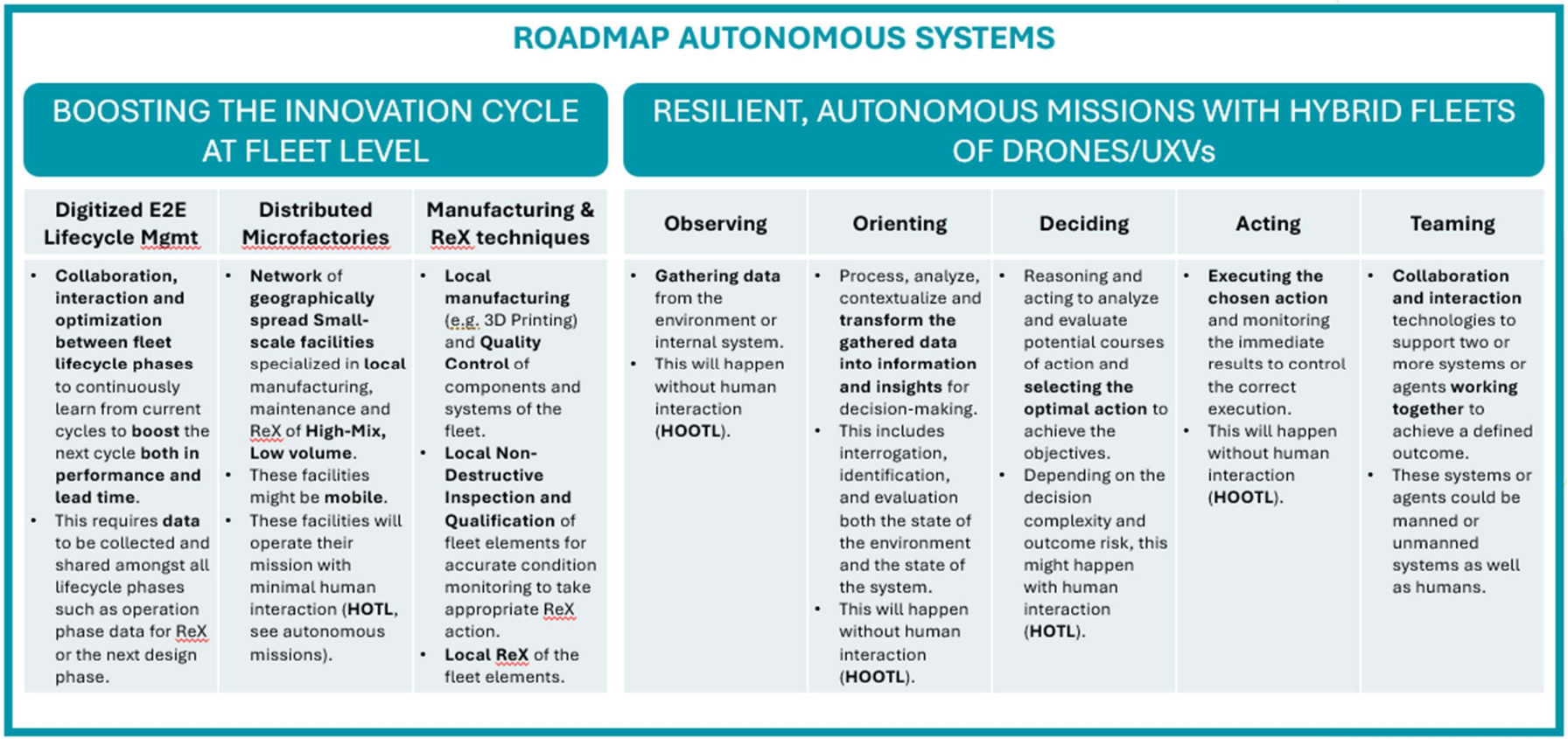
Enkele ***voorbeelden*** van uitdagingen binnen de 'Teaming' bouwblok zijn het inschatten van de intentie van andere systemen of het onderhandelen tussen agenten.

Thematische doelstellingen – Innovatiekansen

- De verschillende autonome systemen moeten kennis en informatie met elkaar delen om een **gezamenlijk wereldmodel te bouwen** waarop ze ageren.
- De verschillende autonome systemen moeten **elkaars gedrag en intenties correct kunnen inschatten**.
- De verschillende autonome systemen moeten met elkaar kunnen **onderhandelen over doelen en taken** om tot een gezamenlijk akkoord te komen over de uit te voeren acties.

Mogelijke synergiën

Deze oriëntatieroadmap rond 'Autonome Technologie voor Veiligheid en Defensie' is toepasbaar op autonome systemen op land, op water, in de lucht en in de ruimte voor verschillende types missies inclusief lokale productie en ReX. Daarnaast maken de autonome technologieën ook gebruik van technologieën zoals AI, Geo-intelligence, communicatie en Cybersecurity. Bijgevolg heeft deze roadmap **sterke synergiën mogelijk met roadmaps van verschillende andere Leads**, zowel langs de technologische kant als de toepassingenkant.



Figuur: Visuele oriëntatieroadmap Autonome Technologie voor Veiligheid en Defensie

Conclusie

De nieuwste technologieën zorgen er voor dat meer en meer vloten van kleinere toestellen ingezet worden voor veiligheid en defensie, elk met een eigen intelligentie, communicatie en perceptie mogelijkheden. Op vandaag zijn dit eerder van op afstand gestuurde units, maar **in de nabije toekomst zullen deze toestellen meer en meer 'autonomie' krijgen om zelf te interageren met omgeving en andere toestellen.** Toekomstige toepassingsmodellen zullen daarom veel meer enten op het correct beheren van dergelijke 'autonome vloten' die gezamenlijk een missie uitvoeren zowel operationeel als vanuit een life cycle management. Deze foresight sluit ook aan bij het toekomstmodel dat door NAVO en EDA wordt vooropgesteld en waar op internationaal vlak voor de volgende 5 tot 10 jaar een roadmap rond zal worden opgebouwd.

Vlaanderen heeft een sterk ecosysteem van hoogtechnologische bedrijven rond het automatiseren van off-road voertuigen, kleine vaartuigen en vliegende toestellen vaak met high tech sensing apparatuur voor civiele toepassingen, maar zeer nauw gelinkt met de technologische behoeftes vanuit veiligheid en defensie. Daarenboven heeft Vlaanderen via de strategische onderzoekcentra toegang tot unieke technologie om dit ecosysteem de mogelijkheden te bieden om een actieve rol te gaan spelen in de Europese roadmap rond autonome technologie voor veiligheid en defensie.

In deze oriëntatie roadmap rond Autonome Technologie voor Veiligheid en Defensie zal ingezet worden op het **autonoom opereren van vloten van intelligente toestellen** in ongestructureerde omgevingen met onbetrouwbare communicatie en onder vijandige dreigingen. Dit niet enkel tijdens een conflict situatie, maar ook ervoor, bijvoorbeeld tijdens prospectie, en achteraf, bijvoorbeeld bij het demilitariseren. Daarenboven zal worden nagedacht **hoe dergelijke vloten beter kunnen worden samengesteld** door niet alleen te focussen op capaciteiten voor het uitvoeren van de missie doelstelling zelf, maar ook op het inzetten van slimme, mobiele units die productiemogelijkheden hebben om tijdens de missie zelf de gepaste herstel en verbeter operaties uit te voeren om zo de hoogste graad van weerbaarheid op vloot niveau te behalen.

Roadmap Energie & Veiligheid

Vlaamse innovatie voor een veerkrachtige en strategisch autonome energievoorziening binnen Defensie, Europa, en de NAVO.

Studie uitgevoerd in opdracht van: WEWIS - Vlaanderen
Oktober 2025

vito
Vision on technology for a better world
vito.be

Roadmap Energie & Veiligheid

Vlaamse innovatie voor een veerkrachtige en strategisch autonome energievoorziening binnen Defensie, Europa, en de NAVO.

VITO
Boeretang 200
2400 MOL
Belgium
BTW No: BE0244.195.916
vito@vito.be – www.vito.be
IBAN BE34 3751 1173 5490 BBRUBEBB

SAMENVATTING

De Roadmap Energie en Veiligheid, opgesteld in opdracht van WEWIS Vlaanderen, kadert binnen de ambitie om energiezekerheid, technologische innovatie en defensieve weerbaarheid samen te brengen in één geïntegreerde visie. Energie is vandaag een kernonderdeel van veiligheid: zonder betrouwbare, autonome en duurzame energievoorziening kunnen noch de samenleving, noch Defensie efficiënt functioneren.

De recente geopolitieke ontwikkelingen, waaronder de oorlog in Oekraïne, hebben de kwetsbaarheid van gecentraliseerde energievoorzieningen en de strategische afhankelijkheid van fossiele brandstoffen scherp blootgelegd. In dit veranderende veiligheidslandschap vormt de transitie naar duurzame en gedistribueerde energiebronnen een structurele noodzaak voor Europa en zijn lidstaten.

De Europese Unie erkent energiezekerheid als een strategische pijler van haar veiligheidsarchitectuur. Beleidsinitiatieven zoals de *EU Climate Change and Defence Roadmap*[1] (EEAS, 2022), het REarmEU-initiatief en de Net-Zero Industry Act benadrukken dat energie, klimaat en defensie onlosmakelijk met elkaar verbonden zijn. Deze visie wordt gedeeld door de NAVO, die in haar *Climate Security Action Plan*[2] (2022) stelt dat "*energy resilience <…> are central to operational readiness*."

Binnen dit kader bevindt Vlaanderen zich in een sleutelpositie. Met een sterke industriële basis, een robuuste kennisinfrastructuur en beleidsautonomie in energie en innovatie beschikt Vlaanderen over de troeven om bij te dragen aan Europese strategische autonomie. De Vlaamse energie- en technologiesector is toonaangevend in netbeheer, vermogenselektronica, batterijtechnologie, hernieuwbare energie en waterstof, en ontwikkelt innovatieve concepten zoals Small Modular Reactors (SMR), waterstof, ammoniak en (Sustainable) Aviation Fuel ((S)AF).

Vlaanderen heeft bovendien een unieke positie in offshore energie en maritieme technologie. De Noordzeeregio vormt een strategische schakel in de ontwikkeling van energie-eilanden, meshed grids en internationale interconnecties, waarmee Vlaanderen zich profileert als architect van de Europese energie-infrastructuur. Deze expertise versterkt ook de energiezekerheid van defensieve operaties, logistieke hubs en maritieme installaties.

De roadmap benadrukt de nood aan veerkrachtige infrastructuren, autonome microgrids en geïntegreerde energieoplossingen die bestand zijn tegen fysieke, cyber- en hybride dreigingen. Elektrificatie van voertuigen, schepen en vliegtuigen vermindert niet enkel emissies, maar ook logistieke kwetsbaarheid en detecteerbaarheid tijdens missies.

De Roadmap Energie en Veiligheid schetst hoe Vlaanderen zijn kennis, infrastructuur en innovatievermogen kan inzetten om deze energietransitie te versnellen. Het document brengt de technologische prioriteiten, strategische partnerschappen en dual-use mogelijkheden in kaart, met als doel Vlaanderen te positioneren als een Europese voortrekker in duurzame energiezekerheid, veerkracht en strategische autonomie.

INHOUDSTAFEL

LIJST VAN AFKORTINGEN

AI	Artificial Intelligence / Artificiële Intelligentie
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance
CF SEDSS	Consultation Forum for Sustainable Energy in the Defence and Security Sector
COE	Centre of Excellence
DC	Direct Current
DEFRA	Defence-related Research Action
DIANA	Defence Innovation Accelerator for the North Atlantic
DIM	Detectie, Identificatie en Monitoring
EDA	European Defence Agency
EDF	European Defence Fund
EEAS	European External Action Service
EMP/EMI	Electromagnetic Pulse / Electromagnetic Interference
EMS	Energy Management System
ENE	Energy & Environment
ENSEC COE	Energy Security Centre of Excellence
ESG	Environmental, Social, Governance
EU	Europese Unie
ISR	Intelligence, Surveillance and Reconnaissance
KMO	Kleine of middelgrote onderneming
NAVO / NATO	Noord-Atlantische Verdragsorganisatie / North Atlantic Treaty Organization
NIF	NATO Innovation Fund
OEC	Operational Energy Concept
OSRA	Overarching Strategic Research Agenda
PFAS	Per- en polyfluoralkylstoffen
PESCO	Permanent Structured Cooperation
PV	Photovoltaic
R&D	Research and Development
REarmEU	European Defence Industrial Reinforcement through Common Procurement Act
RES	Renewable Energy Sources
SAF	Sustainable Aviation Fuel
SAS-190	Research Symposium, titled “Enhancing Energy Security Resilience, Capabilities, and Interoperability”
Seveso	Europese richtlijn inzake industriële risico’s
SOC	Strategisch Onderzoekscentrum
STO	Science and Technology Organization
TBB	Technology Building Block
TRL	Technology Readiness Level
vRES	variable Renewable Energy Sources
VITO	Vlaamse Instelling voor Technologisch Onderzoek
VLAIO	Vlaams Agentschap Innoveren & Ondernemen
WEWIS	Departement Werk, Economie, Wetenschap, Innovatie en Sociale Economie

1 VISIE EN CONTEXT

1.1 Energie als operationeel domein

Energie is uitgegroeid tot een kerncomponent van moderne oorlogsvoering. Waar het vroeger een logistieke randvoorwaarde was, vormt het vandaag een strategische capability die rechtstreeks bepaalt hoe strijdkrachten kunnen optreden, communiceren, bewegen en overleven. Zonder energie valt commando en controle stil, verliezen sensoren hun ogen en worden wapensystemen inert. Energievoorziening is zo onlosmakelijk verbonden met operationele paraatheid, autonomie en slagkracht.

De militaire inzetbaarheid van een natie hangt af van haar vermogen om in crisissituaties onafhankelijk energie te produceren, op te slaan en te distribueren naar troepen en bevolking. In het huidige geopolitieke klimaat, waarin bevoorradingslijnen doelwit zijn en kritieke infrastructuur structureel onder druk staat, wordt energie een operationeel domein op zich, vergelijkbaar met land, zee, lucht, ruimte en cyber.

1.2 Exponentieel stijgende energiebehoefte van moderne krijgsmachten

Tegelijk neemt de energie-afhankelijkheid van defensie exponentieel toe. Moderne krijgsmachten opereren binnen een sterk gedigitaliseerde omgeving waarin sensorfusie, satellietcommunicatie, radarsystemen en datacenters continu energie vragen. Waar een conventionele brigade in de twintigste eeuw voornamelijk afhankelijk was van brandstof en munitie, vraagt een hedendaagse eenheid daarbovenop nog eens een constante stroomvoorziening voor computing, dataverwerking en elektronische oorlogsvoering.

Het groeiende gebruik van kunstmatige intelligentie, autonome platformen en cyberoperaties verhoogt die vraag verder. AI-systemen voor besluitvorming, beeldherkenning of logistieke planning draaien op energie-intensieve servers en edge-computing-toepassingen. De versnelde en verhoogde implementatie en uitrol van autonome wapensystemen, drones, onbemande vaartuigen en sensornetwerken maakt een betrouwbare energie-architectuur noodzakelijk die ook in crisisomstandigheden blijft functioneren.

1.3 Digitale afhankelijkheid en tactische kwetsbaarheid

Daarnaast vergen nieuwe wapengeneraties, zoals directed energy weapons, elektromagnetische lanceersystemen en elektronische tegenmaatregelen, een enorme piekcapaciteit aan stroomvoorziening en thermisch beheer. Zelfs de meest geavanceerde C4ISR-netwerken (Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance) functioneren slechts zolang hun energie-infrastructuur intact blijft.

Ook ondersteunende domeinen zoals cyberdefensie en digitale veiligheid zijn direct afhankelijk van energiecontinuïteit: datacenters, cryptografische sleutelservers, en satellietuplinks moeten 24/7 beschikbaar en beschermd worden. De energievraag van Defensie is dus niet enkel logistiek, maar strategisch-exponentieel. Dit sterk gedreven door digitalisering, miniaturisering en elektrificatie van elke laag in de militaire waardeketen.

1.4 Van hulpbron naar strategische capability

Deze evolutie dwingt de hele sector rond veiligheid en defensie om energie niet langer als hulpbron, maar als kritieke capability te behandelen. Het is namelijk een domein dat actief moet worden ontworpen, beschermd en geoptimaliseerd, met dezelfde aandacht als wapensystemen of munitievoorraden.

1.5 Kritieke energie-uitdagingen voor defensie

De oorlog in Oekraïne heeft de kwetsbaarheid van Europese energie-infrastructuren pijnlijk zichtbaar gemaakt. Stroomonderbrekingen, sabotage van pijpleidingen en cyberaanvallen op energie-netwerken hebben aangetoond dat een energieverstoring, het volledige (verdedigings)systeem kan ontregelen. De grote stroompanne van 2024 in Spanje, Portugal en Zuid-Frankrijk vormde een recent voorbeeld van hoe één storing in het transmissienet zich razendsnel vertaalt in logistieke en veiligheidsproblemen.

Defensie moet daarom inzetten op energetische autonomie, redundantie en robuuste infrastructuur — systemen die operationeel blijven, zelfs bij sabotage, storingen of langdurige onderbreking van civiele netten. De hedendaagse energie-uitdagingen zijn meerdimensionaal en situeren zich op vijf strategische fronten:

(i) **Energiezekerheid en strategische autonomie**: de afhankelijkheid van buitenlandse brandstoffen en kritieke grondstoffen blijft een strategische kwetsbaarheid. De afbouw van Russische olie- en gasimporten benadrukte hoe energieafhankelijkheid militaire paraatheid rechtstreeks beïnvloedt. Defensie moet daarom kunnen produceren, opslaan en verdelen zonder civiele netten of instabiele toevoerketens. Nieuwe generaties microgrids, brandstofcellen en mobiele energiecontainers maken dit mogelijk, zoals aangetoond in HYDE (DEFRA) en INDY (EDF), voorbeelden van energieonafhankelijke kampementen die autonomie en continuïteit verzekeren in contested omgevingen.

(ii) **Bescherming van kritieke infrastructuur**: energie-infrastructuren zijn uitgegroeid tot primaire doelwitten binnen hybride oorlogsvoering. De studie Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats (Defence Industry Europe, 2024) wijst erop dat onderzeese kabels, hoogspanningslijnen en brandstofdepots de kwetsbaarste schakels zijn in de Europese weerbaarheid. Bescherming vergt een combinatie van fysieke beveiliging, cyber-fysieke monitoring, redundante verbindingen en bescherming tegen elektromagnetische impulsen (EMP/EMI). Vlaanderen kan hier aansluiten met zijn sterke industrie in netbeveiliging, automatisering en sensorexpertise.

(iii) **Operationele energie-efficiëntie en veerkracht**: veel militaire installaties zijn afhankelijk van één toevoerlijn of beperkt aantal distributiepunten. Een robuuste energiearchitectuur vraagt modulaire, gedistribueerde netwerken die kunnen isoleren (“islanding”), zichzelf herstellen na storing en lokaal energie kunnen bufferen. Hybride aandrijving, stille generatoren en Energy Management Systems met prioriteitssturing versterken de autonomie van mobiele en vaste operaties.

(iv) **Klimaat- en omgevingsweerbaarheid**: extreem weer vormt een groeiende operationele bedreiging. Overstromingen kunnen munitieopslagplaatsen, tankinstallaties of datacenters uitschakelen; stormen en blikseminslag bedreigen transmissienetten; langdurige droogte of hitte beperkt energie-efficiëntie en koeling. Daarnaast vormen geomagnetische stormen en zonnestormen een

onderschat risico voor satelliet- en communicatiesystemen. De integratie van klimaatweerbaarheid in defensieve energie-ontwerpen, via verhoogde installaties, redundante koelcircuits, en schok- en waterbestendige netcomponenten, wordt een kernvoorwaarde voor operationele continuïteit.

(v) **Technologische interoperabiliteit en validatie**: de transitie naar alternatieve brandstoffen, batterij- en waterstoftechnologie biedt Defensie een strategisch voordeel: minder logistieke druk, lagere thermische en akoestische signatuur, en grotere autonomie in operatie. Tegelijk vereist dit dat alle nieuwe energiecomponenten – van brandstofcellen en batterijen tot converters en netcontrollers – voldoen aan strikte veiligheids-, betrouwbaarheid- en interoperabiliteitsnormen binnen EU- en NAVO-kaders. Vlaanderen kan hier een sleutelrol spelen door test- en certificatie-infrastructuur uit te bouwen die civiele innovatie vertaalt naar mission-proven energieoplossingen voor defensie.

Deze energie-uitdagingen zijn fundamenteel strategisch: energie bepaalt de snelheid, effectiviteit, uithouding en veerkracht van militaire operaties. Zonder een veilige, redundante en autonome energievoorziening kan geen enkel wapensysteem, communicatie- of commandostructuur functioneren. Het niet kunnen beveiligen of herstellen van energie, zal onherroepelijk leiden tot een verlies in slag-, bescherm-, of herstelkracht.

1.6 Energie-infrastructuur als strategisch aanvalsoppervlak

De geopolitieke realiteit van de afgelopen jaren toont dat energie-infrastructuren niet langer passieve civiele objecten zijn, maar actieve doelwitten binnen hybride en actieve oorlogsvoering. Waar klassieke oorlogsvoering zich vroeger beperkte tot het directe slagveld, wordt vandaag een hyrbride strijd gestreden tegen Europe en de NAVO via kabels, pijpleidingen en infrastructuur. Deze vormen de ruggengraat van zowel de militaire als de economische paraatheid van Europa.

Binnen deze hybride oorlogsvoering zijn onderzeese kabels cruciaal en maken ze deel uit van een uitzonderlijk kwetsbare energie- en communicatieruggengraat. Incidenten in de Noordzee en de Baltische Zee, waaronder schade aan gasleidingen, energie- en datakabels, tonen aan hoe eenvoudig lokale verstoringen kunnen uitgroeien tot een grootschalige crisis. Het herstellen of bewaken hiervan vraagt gespecialiseerde maritieme sensornetwerken, onbemande platforms en satelliet ondersteunde monitoring, domeinen die vandaag de dag nog beter georganiseerd kunnen worden maar waarin Vlaanderen, met zijn maritieme en ruimtevaartcapaciteiten, een belangrijke rol kan spelen.

Ook de offshore windmolenparken in de Noordzee zijn potentieel kwetsbare doelwitten. Ze leveren niet alleen een groeiend aandeel van de Europese elektriciteitsproductie, maar fungeren ook als logistieke en digitale knooppunten. Hun omvang en nabijheid tot internationale wateren maken ze gevoelig voor sabotage en fysieke verstoring. De bescherming van deze installaties vraagt om geïntegreerde beveiligingsconcepten waarin energiebeheer, maritieme surveillance en cyberbeveiliging samenkomen.

Daarnaast blijft de dreiging van sabotage aan nucleaire installaties, zowel operationele kerncentrales als opslaglocaties voor splijtstof, een strategische zorg binnen Europa. Dergelijke aanvallen of infiltraties zouden niet alleen fysieke, maar ook maatschappelijke en psychologische impact hebben. Een gecoördineerde aanpak van nucleaire veiligheid en energiebeveiliging, ondersteund door sensortechnologie, noodplanning en stralingsmonitoring, wordt essentieel voor nationale veerkracht.

Ten slotte worden olie- en gasleveringen steeds vaker gebruikt als instrument van geopolitieke druk. De verstoring van pijpleidingen en terminals in Oost- en Zuid-Europa, evenals de blokkering van energievoorziening via maritieme routes, hebben aangetoond dat energieafhankelijkheid rechtstreeks kan worden vertaald naar strategische kwetsbaarheid. Voor Defensie betekent dit dat energievoorziening niet enkel een kwestie van productie is, maar van strategische autonomie, bevoorradingsdiversificatie en real-time situational awareness over de hele logistieke keten.

1.7 Koppeling aan Europees en internationaal beleidskader

1.7.1 Energiezekerheid als strategische pijler binnen NAVO en EU

Binnen Europa is energie uitgegroeid tot een structurele pijler van het defensiebeleid. Energiezekerheid, redundantie en veerkracht staan centraal in recente NAVO- en EU-strategieën, niet als milieudoel, maar als operationele noodzaak.

De *EU Climate Change and Defence Roadmap*[1] (EEAS, 2022) en de *NATO Climate Security Action Plan*[2] (2022) erkennen dat energievoorziening rechtstreeks de paraatheid, mobiliteit en slagkracht van strijdkrachten bepaalt. Beide kaders leggen de nadruk op drie thema's: (**i**) bescherming van kritieke energie-infrastructuur, (**ii**) energie-autonome operaties via microgrids en modulaire opslag, en (**iii**) integratie van hernieuwbare of alternatieve bronnen in militaire systemen zonder verlies van operationele betrouwbaarheid zoals waterstof, synthetische brandstoffen en batterijopslag.

De NAVO behandelt energie inmiddels als operationeel domein via haar *Operational Energy Concept* (OEC) en de publicaties van het *NATO Energy Security Centre of Excellence*[3] (ENSEC COE). Deze leggen de nadruk op resilience, interoperability en sovereign control over energievoorziening in militaire operaties. De verschillende NATO Energy Security Strategies[4-6] (ENSEC COE, 2023) stelt expliciet dat energie-soevereiniteit een kernvoorwaarde is voor operationele vrijheid, terwijl het SAS-190 Symposium on Enh*ancing Energy Security, Resilience, Capabilities and Interoperability*[7] (STO, 2024) oproept tot meer standaardisatie en gedeelde testinfrastructuren voor kritieke energie-technologieën.

1.7.2 Onderzoek en samenwerking binnen het Europese defensiekader

Het European Defence Agency (EDA) concretiseert dit via CapTech 14 Energy & Environment (EnE). Onderzoek en ontwikkeling binnen deze CapTech focussen op (**i**) TBB03: Engine and power distribution system efficiency technologies, met nadruk op motor-, aandrijf- en vermogensefficiëntie; (**ii**) TBB04: Energy management technologies: innovative and efficient systems, gericht op slimme netsturing, EMS-optimalisatie en cyber-fysieke beveiliging; (**iii**) TBB09: Energy and environmental technology systems integration, dat zich richt op de koppeling van energie-, opslag- en controle-systemen binnen geïntegreerde defensie-platformen.

Daarnaast biedt *het Consultation Forum for Sustainable Energy in Defence and Security*[8] (CF SEDSS) een structureel samenwerkingsplatform waar lidstaten werken aan grid resilience, off-grid toepassingen en beveiliging van energie-netwerken tegen cyber- en hybride dreigingen.

Concrete oproepen door oa. het European Defence Fund versterken verder deze prioriteiten door (**i**) EDF-2025-RA-EnergyResilience: ontwikkeling van resilient off-grid systemen en autonome energievoorziening voor ontplooide operaties. (**ii**) EDF-2025-RI-EnergyStorage: veilige, modulaire en transporteerbare opslagtechnologieën, inclusief batterij- en

waterstofoplossingen met militaire validatie. (**iii**) EDF-2025-RA-CriticalInfrastructure: bescherming van energie- en communicatienetten tegen hybride aanvallen en verstoringen. Gezamenlijk bouwen deze programma's aan een Europees raamwerk waarin energie-zekerheid, redundantie en interoperabiliteit worden behandeld als kerncapaciteiten van defensie.

1.8 Strategische vertaling voor Vlaanderen

Vlaanderen vervult een sleutelrol binnen de Europese en trans-Atlantische energie-architectuur. Dankzij zijn beleidsbevoegdheden in energie en innovatie en zijn sterke industriële en kennisbasis kan Vlaanderen civiele energie-expertise vertalen naar strategische toepassingen voor defensie en veiligheid. Als innovatie gedreven regio met toonaangevende spelers in energieopslag, netbeheer, waterstof, digitalisering en systeemintegratie kan Vlaanderen uitgroeien tot een schakelregio voor energiezekerheid en technologische weerbaarheid binnen het federale en Europese defensiekader.

1.8.1 Vlaanderen binnen het federaal, Europees en Trans-Atlantisch kader

België onderschrijft deze Europese en NAVO-initiatieven en heeft energie als een van de strategische prioriteiten verankerd. Vlaanderen beschikt, binnen dat federale kader, over cruciale bevoegdheden op het vlak van energie, innovatie en economie, en kan daardoor civiele en militaire energie-innovatie structureel verbinden.

Vlaanderen beschikt over een uitzonderlijk sterke kennis- en industriële basis, dankzij bedrijven, speerpuntclusters, universiteiten, strategische onderzoekscentra en een dynamisch netwerk van KMO's en scale-ups in netbeheer, opslag, waterstof, batterijmaterialen, vermogenselektronica en energiebeheer. Deze ecosystemen dragen al bij aan Europese onderzoeksprogramma's rond grid resilience, opslag en elektrificatie van mobiliteit, en kunnen met beperkte aanpassing worden vertaald naar defensie- en veiligheidscontexten.

Vlaanderen kan zo fungeren als brug tussen de Europese energie- en defensieagenda en de Belgische militaire praktijk. Door militaire (oefen)terreinen, havens en logistieke knooppunten in te zetten als test- en demonstratiezones voor microgrids, autonome energieoplossingen en opslagtechnologie, ontstaat een living-lab omgeving waar civiele en militaire partners gezamenlijk kunnen innoveren.

1.8.2 Strategische rol van Vlaanderen

De strategische rol van Vlaanderen binnen het domein energie en defensie bestaat uit drie complementaire pijlers:

(i) **Innovatieversneller**: Vlaanderen kan civiele onderzoeksprogramma's koppelen aan defensieve noden en zo de ontwikkeling van technologieën rond energie-autonomie, opslag, vermogensefficiëntie en netbeveiliging versnellen. Door deze innovatieketen uit te breiden tot TRL 8-9 wordt de stap van lab naar operatie sterk verkort.

(ii) **Test- en demonstratieregio**: Militaire/Vlaamse (oefen)terreinen, havens en logistieke knooppunten kunnen fungeren als living labs voor energie-oplossingen: microgrids, batterij- en waterstofsystemen, slimme netten en beveiligde energie-architecturen. Deze sites vormen het ontbrekende validatieniveau tussen civiel

onderzoek en operationele inzet, vergelijkbaar met internationale referentie-sites binnen NAVO- en EDA-kader.

(iii) **Brug tussen beleid, industrie en defensie**: Vlaanderen kan als structureel knooppunt fungeren tussen federale defensie, Vlaamse agentschappen, kennisinstellingen en bedrijven. Door gedeelde roadmaps, dual-use calls en matchmaking te organiseren, wordt de samenwerking tussen de Vlaamse energie-innovatiesector en defensie structureel en toekomstgericht verankerd.

1.8.3 Kansen en opportuniteiten

De koppeling tussen energie, technologie en veiligheid creëert voor Vlaanderen een reeks strategische kansen. Door bestaande sterktes in energieproductie onderzoek, opslag, netbeheer, digitalisering, autonomie, ruimtevaart en cyberveiligheid te verbinden, kan Vlaanderen uitgroeien tot een referentieregio voor energiezekerheid en operationele weerbaarheid binnen Europa.

(i) **Veerkrachtige en sovereine infrastructuur**: de versterking van defensieve en civiele installaties in Vlaanderen zoals havens, logistieke corridors, luchthavens en militaire domeinen, biedt kansen om energie autonome en redundante microgrids te testen. Vlaamse innovaties in waterstofproductie, batterijopslag, vermogenselektronica en slimme energie-sturing kunnen hier geïntegreerd worden in infrastructuren die bestand zijn tegen onderbreking, sabotage, overstromingen of andere vormen van verstoringen.

(ii) **Beveiliging van kritieke infrastructuur**: Vlaanderen beschikt over sterke industriële en onderzoeks-capaciteit in AI, sensortechnologie, dataverwerking en predictive maintenance, waarmee energie- en netwerkbeveiliging kan worden versterkt. Deze technologieën laten toe om storingen, cyberaanvallen en fysieke beschadiging van energievoorzieningen vroegtijdig te detecteren en te herstellen. Het gebruik van digital twins kan hierbij van pas komen.

(iii) **Energie voor autonome en onbemande systemen**: de opkomst van drones, robotica en onbemande voertuigen creëert nood aan lichte, veilige en modulaire energiebronnen. De Vlaamse expertise in batterij-technologie, brandstofcellen en power electronics ondersteunt de elektrificatie van militaire platformen en hybride aandrijfsystemen voor land-, zee- en luchttoepassingen.

(iv) **Digitale en cyber-fysieke energiebeveiliging**: met zijn geavanceerde cyber-ecosysteem heeft Vlaanderen de kennis om Energy Security Operations Centres (E-SOC's) te ontwikkelen die operationele energievoorziening beschermen tegen cyberdreigingen, datalekken en verstoringen van industriële controlesystemen.

(v) **Ruimte-, maritieme en autonome koppelingen**: energie vormt de verbindende laag tussen meerdere domeinen waarin Vlaanderen uitblinkt. Energiebeheer voor satellieten, schepen en sensornetwerken verbindt de ruimte-, maritieme en autonome roadmaps tot één geïntegreerde innovatie-as. Vlaamse technologie in piconetwerken, fotonica en micro-energieopslag kan hier de ruggengraat vormen van een multidomein-energiesysteem.

(vi) **Proeftuin voor dual-use innovatie**: de combinatie van civiele infrastructuur en defensieve testterreinen maakt Vlaanderen bij uitstek geschikt als living lab voor energie-innovatie. Havens, oefenterreinen en industriële sites kunnen worden ingezet om off-grid energieoplossingen, cyber-beveiligde netwerken en hybride brandstofsystemen in realistische omstandigheden te demonstreren en te valideren.

Door deze ecosystemen samen te brengen en te koppelen aan Europese programma's zoals EDF, DIANA, CF SEDSS en CapTech EnE, kan Vlaanderen een leidende rol opnemen in de ontwikkeling van een energie-resilient defensie-architectuur waarin autonomie, veerkracht en interoperabiliteit centraal staan.

1.9 Naar een toekomstgerichte energie-architectuur

De energietransitie binnen defensie is tegelijk een veiligheidsuitdaging en een economische kans. Energie bepaalt niet enkel het tempo van operaties, maar ook de robuustheid van onze infrastructuur en de legitimiteit van defensie in een samenleving die duurzaamheid eist.
Door zijn innovatievermogen en kennisinfrastructuur kan Vlaanderen bijdragen aan een nieuwe generatie energie-architecturen voor defensie: emissiearm, cyberveilig, autonoom en circulair. Deze architectuur versterkt niet alleen militaire paraatheid, maar ook industriële veerkracht en maatschappelijke draagkracht.

Energieonafhankelijkheid is een strategische noodzaak: zonder veilige, autonome energievoorziening kan noch Defensie, noch de samenleving veerkrachtig functioneren.

2 ECOSYSTEEM MAPPING

2.1 Doel en scope

De mapping binnen het technologiedomein energie & veiligheid biedt een overzicht van het Vlaamse industriële en wetenschappelijke potentieel in energieproductie, energieopslag en energienetwerken, met bijzondere aandacht voor de veiligheids- en defensiedimensie.
Ze maakt zichtbaar welke bedrijven, kennisinstellingen en organisaties vandaag beschikken over de technologische capaciteiten om bij te dragen aan energiezekerheid, veerkracht en strategische autonomie; drie pijlers die centraal staan in zowel de Europese als de NAVO-agenda voor defensie en veiligheid.

De analyse richt zich op ondernemingen met een duidelijke innovatiecomponent, onderzoeksactiviteit of relevante ervaring in hightechdomeinen zoals batterijtechnologie, waterstof, vermogenselektronica, netbeheer, smart grids en energiebeheer. De geografische afbakening omvat Vlaanderen en het Brussels Hoofdstedelijk Gewest, aangezien veel ondernemingen zowel een operationele als juridische aanwezigheid in beide regio's hebben.

Het doel van deze mapping is niet louter inventarisatie, maar strategisch inzicht: hoe kan het bestaande civiele ecosysteem, dat wereldwijd erkend wordt voor zijn energie-innovatie, worden ingezet voor dual-use toepassingen binnen defensie, en hoe kunnen bestaande programma's worden benut om Vlaamse bedrijven sneller in die Europese en Trans-Atlantische veiligheidsketen te positioneren.

2.2 Methodologie

De mapping werd opgebouwd op basis van een gestructureerde, data-gedreven aanpak. Vertrekkend vanuit open databronnen, sectorfederaties, speerpuntclusters, onderzoeksnetwerken en deelnemerslijsten van thematische events, werd een longlist samengesteld van 117 Vlaamse bedrijven en instellingen die actief zijn in de energiesector.

Aanvullende validatie gebeurde via de Strategische Onderzoekscentra (SOC's) en Europese partnerschappen zoals CapTech 14 Energy & Environment, CF SEDSS en EDF-calls. Enkel ondernemingen met een aantoonbare innovatieve rol, R&D-activiteit of deelname aan onderzoeksprojecten werden opgenomen. Louter uitvoerende installateurs of constructeurs zonder eigen ontwikkelingscapaciteit werden uitgesloten.

Om duplicatie te vermijden werden dochterondernemingen en divisies samengevoegd onder één merknaam. Elk bedrijf werd geclassificeerd volgens zijn technologie-domein (productie, opslag, grid) en volgens de EDA-OSRA-taxonomie, die de link legt met Europese defensieonderzoeken.

2.3 Resultaten

De mapping identificeerde 117 bedrijven actief in het Vlaamse energie-ecosysteem:

(i) 70 zijn actief in energieproductie en brandstoffen (inclusief hernieuwbare en synthetische brandstoffen);
(ii) 40 in energieopslag en batterijtechnologie;
(iii) 52 in energienetwerken, energiemanagement en gridtechnologie.

Er is aanzienlijke overlap tussen de categorieën, wat de verwevenheid toont van het Vlaamse innovatie-ecosysteem.
Van deze 117 ondernemingen hebben 14 bedrijven vandaag reeds een gekende defensieactiviteit, terwijl 53 bedrijven actief samenwerken met VITO of deelnemen aan gezamenlijke onderzoeksprojecten.

De bedrijven bestrijken een brede waaier aan technologieën: van brandstofcellen, power electronics en thermische systemen tot energiebeheerplatformen, cyberbeveiliging van energienetten en microgridcontrole.

2.4 Analyse en inzichten

De resultaten tonen een uitgesproken sterkte in slimme netwerken, energieopslag, batterijtechnologie en waterstof, sectoren waarin Vlaanderen een Europese voortrekkersrol vervult. Het ecosysteem onderscheidt zich door de combinatie van industriële maturiteit en een dynamische laag van innovatieve kmo's en scale-ups.

Toch blijkt uit de analyse dat slechts een klein deel van dit ecosysteem vandaag structureel gelinkt is aan defensie. Veel actoren opereren nog uitsluitend in een civiele context, ondanks hun directe relevantie voor militaire toepassingen zoals energiebeveiliging, microgrids, off-grid opslag en vermogensefficiënte aandrijfsystemen.

Deze beperkte koppeling heeft niet enkel technologische, maar ook structureel-culturele oorzaken. Defensie en veiligheid waren tot voor kort gevoelige domeinen binnen civiele innovatie en financiering: deelname aan militaire of dual-use projecten werd vaak als risicovol beschouwd door banken, investeringsfondsen en internationale partners. Vlaamse bedrijven die actief waren in energie en infrastructuur vermeden daarom expliciet verwijzingen naar defensie, om geen hinder te ondervinden bij kredietverlening of export.

Sinds de recente Europese herbewapening, de oorlog in Oekraïne en de oprichting van programma's als EDF, DIANA en ReArmEU, is dit beeld echter sterk aan het verschuiven. Defensie wordt nu erkend als een legitieme en strategische innovatiepartner, en de vroegere terughoudendheid maakt plaats voor gerichte samenwerking en valorisatie. De uitdaging blijft echter dat de civiele innovatieketen wel over de juiste kennis en infrastructuur beschikt, maar nog mist aan validatiekaders, begeleiding naar de defensiemarkt, bepaling van de noden en testfaciliteiten.

2.5 Lessons learned en beleidsimplicaties

2.5.1 Beperkte vertaling van civiele sterktes naar defensie

De Vlaamse energie-industrie beschikt over sterke technologische capaciteiten, dit in netbeheer, opslag, waterstof, batterijtechnologie en vermogenselektronica maar de structurele aansluiting bij Defensie blijft beperkt. De meeste innovaties bevinden zich nog in een civiel kader, ondanks hun directe relevantie voor militaire energiezekerheid en infrastructuurbeveiliging.

De drempel lag tot voor kort vooral bij perceptie en financiering: samenwerking met Defensie werd als risicovol beschouwd door banken en investeerders. Dat paradigma verschuift snel onder invloed van de Europese herbewapening en funding programma's. Vlaanderen kan nu zijn civiele innovatiebasis versneld valoriseren binnen dit nieuwe strategische kader.

2.5.2 Nood aan coördinatie en testcapaciteit

De analyse toont een duidelijke behoefte aan structurele coördinatie tussen Defensie, Vlaamse agentschappen en de energiesector. Innovatie verloopt vandaag gefragmenteerd over clusters en onderzoeksprogramma's, zonder centrale afstemming met defensieve noden. Een geïntegreerde aanpak is noodzakelijk;

(i) gedeelde test- en validatie-infrastructuren op zowel civiele, militaire domeinen als havenzones;
(ii) gezamenlijke roadmaps en matchmaking tussen Vlaamse bedrijven en defensiepartners;
(iii) een versneld traject voor certificatie van civiele technologieën en het toekennen van veiligheidsmachtigingen.

Deze aanpak kan de kloof tussen onderzoek en inzetbare capaciteit verkleinen en Vlaanderen positioneren als testregio voor energie-resilient defence binnen Europa.

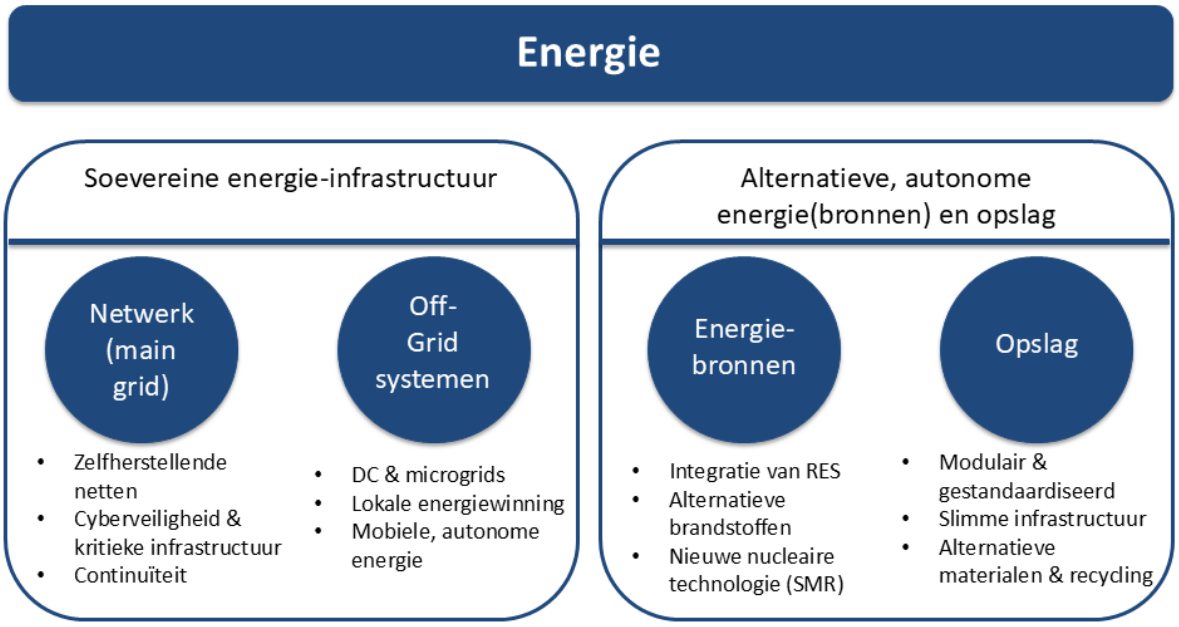
2.5.3 Beleidsimplicaties voor Vlaanderen

Vlaanderen kan zijn bestaande expertise in energiebeheer, industriële veiligheid en netsturing rechtstreeks toepassen in defensieve contexten, met bijzondere aandacht voor kritieke infrastructuur, logistieke knooppunten en energie-intensieve installaties. De koppeling van civiele en militaire innovatieprocessen vraagt om een beleidsmatig verankerde dual-use strategie waarin energiezekerheid, weerbaarheid en strategische autonomie samenkomen.

2.6 Conclusie

De Vlaamse energie- en technologiesector vormt een solide basis om bij te dragen aan Europese en trans-Atlantische energiezekerheid. De noodzakelijke bouwstenen zijn aanwezig: kennis, industrie en infrastructuur. De uitdaging is coördinatie. Door bestaande sterktes te verbinden in een gezamenlijke governance en validatiekader kan Vlaanderen uitgroeien tot een Europese referentie voor energy-resilient defence.

3 ROADMAP



Figuur 1 - Eenvoudige weergave van de roadmap Energie & Veiligheid. De volledige roadmap is als bijlage achteraan terug te vinden.

3.1 Netwerk

3.1.1 Visie

De veerkracht en veiligheid van het hoofdnet zijn essentieel voor zowel civiele als militaire operaties. Naarmate de digitalisering en de afhankelijkheid van offshore en gedistribueerde hernieuwbare energiebronnen (RES) toenemen, worden energiesystemen steeds sterker met elkaar verbonden en daardoor kwetsbaarder voor hybride dreigingen, cyberaanvallen en fysieke verstoringen.

Om een ononderbroken energievoorziening te garanderen voor kritieke infrastructuur en defensie-installaties, is een netwerk nodig dat niet afhankelijk is van centrale coördinatie of dat zich autonoom kan herstellen wanneer die coördinatie uitvalt.
Het netwerk van de toekomst moet evolueren naar een autonome, zelfherstellende en gedistribueerde architectuur, die geavanceerde detectie, lokale intelligentie en veilige communicatie combineert om de functionaliteit onder crisisomstandigheden te waarborgen.

3.1.2 Focuslaag en bijbehorende bouwstenen

De bouwstenen kunnen worden onderverdeeld in preventieve maatregelen, gericht op interne technische risico's en externe dreigingen, en corrigerende maatregelen, gericht op herstel en continuïteit.

Preventieve maatregelen omvatten geavanceerde detectie, anomaliedetectie en cyberbestendige coördinatielagen die storingen of aangetaste componenten isoleren voordat er cascade-effecten optreden.
Aan de corrigerende kant maakt lokale EMS-gestuurde coördinatie tussen sectoroverschrijdende bronnen, zoals batterijsystemen en thermische opslag, een dynamische herbalancering van spanning en frequentie mogelijk bij ontkoppeling of verstoring. De integratie van warmteopslag en hybride thermisch-elektrische bronnen verhoogt bovendien het aanpassingsvermogen van het systeem om fluctuaties op te vangen en de continuïteit van de dienstverlening te behouden.

Naast operationele stabiliteit is fysieke en digitale beveiliging tegen terrorisme, spionage, sabotage, subversie en georganiseerde misdaad (TESSOC) onmisbaar. Dit vereist proactieve dreigingsanalyse, continue monitoring van afwijkend gedrag en gecoördineerde defensieve reacties op alle activa, exploitanten en toeleveringsketens.

Conventionele procedures voor black start en netherstel zijn doorgaans afhankelijk van gecentraliseerde controlekamers en vaste herstelplannen, wat een enkel storingspunt creëert bij cyberaanvallen of fysieke ontkoppeling.
Om dit te vermijden, is een gedistribueerde cel- of zwermarchitectuur wenselijk: een netwerk van met elkaar verbonden microgrids en energieclusters die zichzelf kunnen organiseren, de frequentie stabiliseren en kritieke belastingen autonoom beheren.

Elke lokale cel, bestaande uit gedistribueerde energiebronnen, hernieuwbare productie-eenheden en flexibele vraagcomponenten, moet autonoom kunnen:

(i) afwijkingen detecteren,
(ii) zichzelf of een aangetaste buurcel isoleren,
(iii) de werking herstellen,
(iv) en veilig herverbinden met het netwerk.

Dit vergt gedistribueerde intelligentie aan de rand van het net, ondersteund door interoperabele datastandaarden en veilige communicatie met lage latentie tussen lokale controllers.

Belangrijke technologische bouwstenen zijn onder meer:

(i) autonome microgrid coördinatie,
(ii) gedecentraliseerd databeheer en replicatie,
(iii) AI-ondersteund situationeel bewustzijn,
(iv) betrouwbare randcomputing,
(v) geïntegreerde cyberbeveiliging die data-integriteit en authenticatie garandeert.

Het integreren van mobiele energiedragers, zoals voertuig-tot-net-systemen, verhoogt de flexibiliteit voor kritieke diensten. Daarnaast moeten wet- en regelgevingskaders evolueren om tijdelijke lokale autonomie toe te staan tijdens nationale noodsituaties, zodat installaties veilig kunnen blijven functioneren buiten de normale marktcontext.

3.1.3 Voorbeeldonderzoek

Onderzoek moet zich in eerste instantie richten op het identificeren van kwetsbaarheden en het monitoren van kritieke infrastructuur, zowel op het land als op zee. Daarnaast is uitgebreid ontwerp- en implementatieonderzoek nodig om de overgang naar gedistribueerde en flexibele energiesystemen te versnellen.

Belangrijke onderzoeksdomeinen zijn onder andere:

(i) veerkrachtige en zelfherstellende netinfrastructuren,
(ii) lokaal marktontwerp,
(iii) uitwisseling van energie tussen gelijken (peer to peer),
(iv) dynamische verbindingsmechanismen,
(v) en gedistribueerde black start-capaciteiten.

Veiligheid en cybersecurity vormen een centraal aandachtspunt, met nadruk op het ontwikkelen van nieuwe concepten voor energie- en datadeling en veilige platformen voor meerdere energiedragers.

Relevante onderzoeksthema's zijn onder meer:

(i) geavanceerde EMS met voorspellende planning en besturing,
(ii) AI-gebaseerde anomaliedetectie en foutanalyse,
(iii) modelvoorspellende controle voor hybride energiesystemen,
(iv) veilige gegevensuitwisseling en interoperabiliteit,
(v) digitale tweelingen voor simulatie van storingen en herstelacties.

Daarnaast omvat onderzoek naar gedistribueerde microgrids de ontwikkeling van cellulaire architecturen (zoals Web of Cells en Fractal Grids), beveiligde communicatie, AI-ondersteunde lastverdeling en redundante coördinatieplatformen. Deze innovaties versterken de defensieve dimensie van het Vlaamse energiesysteem en garanderen dat essentiële activa operationeel blijven, zelfs onder extreme of betwiste omstandigheden.

3.2 Offgrid systemen

3.2.1 Visie

Off grid energiesystemen en microgrids, die autonoom kunnen functioneren met behulp van geavanceerde energiebeheersystemen, zijn cruciaal voor veerkrachtige operaties. Ze optimaliseren het gebruik van lokale energiebronnen en bieden veilige energievoorziening op land en op zee. Dankzij innovatieve netwerktechnologieën zoals DC-microgrids, energieopslag en intelligente sturing kunnen deze systemen zelfs onder extreme omstandigheden blijven functioneren. Bovendien zijn off-grid oplossingen vaak mobiel, wat essentieel is voor militaire inzetbaarheid.

Microgrids op basis van hernieuwbare energiebronnen bieden een sterke verdediging tegen cyberdreigingen (ook in 3.3): ze kunnen zich, onmiddellijk na detectie van een bedreiging, isoleren van het hoofdnet en autonoom blijven functioneren.

3.2.2 Focuslaag en bouwstenen

Klassieke wisselstroommicrogrids (50 Hz of 400 Hz) zijn vandaag een volwassen technologie, ook voor militaire toepassingen. De onderzoeksfocus verschuift daarom naar DC-microgrids, die minder energie verliezen en beter geschikt zijn voor directe koppeling met zonnepanelen en batterijen. Ze vereenvoudigen bovendien de besturing, omdat geen synchronisatie met de

spanningsgolfvorm nodig is. De belangrijkste uitdaging is echter betrouwbare foutdetectie en beveiliging tegen stroomonderbrekingen.

Kleinschalige stadsverwarmingssystemen op basis van geothermie of zonne-energie winnen aan belang, zowel in civiele als militaire context. Voor militaire basissen kunnen laagtemperatuurwarmtenetten die verschillende hernieuwbare bronnen combineren, zoals geothermie, zon, wind en biogas, de energiezekerheid aanzienlijk verhogen.

Off-grid systemen vereisen geavanceerde energiebeheersystemen die flexibel en prioriteitgestuurd belastingen plannen op basis van de beschikbare lokale bronnen. Deze systemen moeten robuust, transparant en energie-efficiënt zijn en gebruikmaken van hybride AI-technologieën voor voorspelling en optimalisatie. Ze moeten zowel wisselstroom- als gelijkstroomnetten ondersteunen en koppelingen tussen elektrische en thermische netten integreren.

Ook in de transportsector ontstaan kansen voor elektrificatie van logistiek en operaties te land, ter zee en in de lucht. Door de combinatie van gelijkstroomnetten, warmteterugwinning en energiebeheer kan de efficiëntie van transporteenheden aanzienlijk worden verhoogd, met minder afhankelijkheid van fossiele brandstoffen en lagere operationele risico's. Vlaamse kennisinstellingen hebben al ervaring met elektrificatie van schepen, systeemveiligheid en batterij-integratie, wat een solide basis biedt om interoperabele en veilige energiearchitecturen te ontwikkelen.

3.2.3 Voorbeeldstudies

Onderzoek richt zich op robuuste, energiezuinige off-grid toepassingen die bruikbaar zijn onder uiteenlopende geografische omstandigheden. Belangrijke uitdagingen zijn de detectie van stroomonderbrekingen, bescherming tegen vlambooggevaar, standaardisatie en interoperabiliteit.

Verder is er nood aan dynamische concepten voor off-grid en on-grid systemen, met lokale optimalisatiealgoritmen voor mobiele militaire basissen, schepen en kampementen. Andere onderzoeksrichtingen omvatten de hybridisatie van dieselelektrische voortstuwing met batterijopslag, de elektrificatie van voertuigen en robuuste fysieke en cyberbeveiliging van autonome energie-eilanden.

3.3 Alternatieve, autonome energie(bronnen)

3.3.1 Visie

Het vergroten van energieautonomie en bevoorradingszekerheid door minder afhankelijkheid van fossiele brandstoffen is cruciaal voor zowel civiele als militaire toepassingen. Hernieuwbare en alternatieve energiebronnen worden hierdoor een strategische pijler van operationele paraatheid, logistieke efficiëntie en veiligheid.

De integratie van energie uit zon, wind, biobrandstoffen, waterstof en nieuwe nucleaire technologieën zoals Small Modular Reactors (SMR) versterkt de strategische autonomie van Defensie. Deze technologieën maken het mogelijk om lokaal, betrouwbaar en schaalbaar energie te produceren, ook in afgelegen en/of risicovolle omgevingen.

Elektrische en hybride systemen bieden bijkomende tactische voordelen: minder geluid, lagere warmteafgifte, hogere betrouwbaarheid en een kleiner logistiek spoor. Dit verhoogt niet alleen de efficiëntie, maar ook de veiligheid van militaire operaties.

3.3.2 Focuslaag en bouwstenen

Modulaire en mobiele systemen
Verplaatsbare, modulaire installaties op basis van hernieuwbare energie, zoals mobiele zonne- of windeenheden, maken snelle inzet, herplaatsing en energievoorziening mogelijk op tijdelijke basissen. Dergelijke systemen kunnen energie leveren voor basisvoorzieningen, waterzuivering, laadstations en andere elektrische apparatuur.

Nieuwe brandstoffen en aandrijfsystemen
De elektrificatie van militaire platforms, voertuigen, schepen en vliegtuigen is een groeiende trend die de storingsgevoeligheid vermindert en autonoom gebruik ondersteunt. Hernieuwbare brandstoffen zoals (Sustainable) Aviation Fuel ((S)AF), ammoniak en waterstof vormen haalbare alternatieven voor diesel en kerosine. Daarnaast bieden mixed-fuel toepassingen, bijvoorbeeld dieselmotoren die draaien op mengsels van diesel met waterstof of ammoniak, interessante perspectieven voor maritieme operaties. Deze technologieën verminderen de afhankelijkheid van fossiele brandstoffen en versterken de energieautonomie.

Koelings- en thermische systemen
De efficiëntie van toekomstige energiesystemen hangt sterk samen met thermisch beheer. Verschillende types koeling, waaronder klassieke watergekoelde systemen, hybride oplossingen en luchtgekoelde componenten, spelen een cruciale rol in het verlengen van de levensduur en prestaties van energie-eilanden en batterijopslag. Vlaanderen beschikt over een sterke kennisbasis in koeltechnologie, thermische optimalisatie en warmteregeling via zijn onderzoeksinstellingen en industrie, die deze kennis kunnen vertalen naar defensieve toepassingen.

Nucleaire energieoplossingen
Small Modular Reactors (SMR) vormen een nieuwe generatie compacte, veilige kernreactoren die een constante, onafhankelijke baseload energie kunnen leveren, met potentieel voor inzet op afgelegen militaire sites of logistieke hubs. Door hun modulaire opzet, passieve veiligheidssystemen en schaalbaarheid kunnen SMR's een robuuste aanvulling vormen op hybride energievoorzieningen, mits strikte veiligheids- en governancekaders.

3.3.3 Voorbeeldstudies

Hoewel sommige technologieën al worden toegepast in defensiecontext, blijft grootschalige integratie van alternatieve energie nog beperkt.

Toekomstig onderzoek moet zich richten op:

(i) verhoging van de efficiëntie, modulariteit en mobiliteit van systemen op basis van hernieuwbare energie;
(ii) integratie van hernieuwbare en alternatieve energie in gebouwen, voertuigen en drones;
(iii) toepassing van waterstof, SAF, ammoniak en mixed fuel motoren in maritieme en luchtvaartplatforms;
(iv) ontwikkeling van SMR concepten voor kleinschalige, veilige baseloadvoorziening op militaire sites;
(v) optimalisatie van koeling en thermisch beheer in autonome energie installaties, gekoppeld aan Vlaamse expertise in energie en warmtebeheer.

3.4 Energieopslag

3.4.1 Visie

Defensie heeft nood aan veilige, kwalitatieve en robuuste batterijoplossingen die een sleutelrol spelen in het verminderen van de afhankelijkheid van fossiele brandstoffen, het verhogen van operationele flexibiliteit en het verbeteren van energie-efficiëntie. Zowel mobiele systemen zoals voertuigen, drones en draagbare apparatuur, als stationaire toepassingen binnen microgrids of off-grid locaties, profiteren van geavanceerde energieopslag. Bij de ontwikkeling van militaire batterijtechnologieën staan veiligheid, duurzaamheid en interoperabiliteit centraal.

Deze oplossingen moeten functioneren binnen een context van extreme omstandigheden, zoals hoge en lage temperaturen, trillingen en langdurige opslag. Daarnaast is er een duidelijke nood aan standaardisatie om logistiek en onderhoud te vereenvoudigen. Ook de afhankelijkheid van kritieke grondstoffen binnen een geopolitiek spanningsveld vraagt om alternatieve technologieën en circulaire benaderingen.

3.4.2 Focuslaag en bijbehorende bouwstenen

De ontwikkeling van modulaire en gestandaardiseerde lichtgewicht batterijopslag is essentieel voor meer flexibiliteit en efficiëntie. Denk aan snelle vervanging in het veld, schaalbaarheid van energiecapaciteit, interoperabiliteit tussen systemen en kostenbesparing in ontwikkeling en onderhoud. Dit vereist een uniform en uitwisselbaar batterijontwerp (bv. gestandaardiseerde afmetingen en connectoren) dat compatibel is met verschillende batterijtechnologieën en inzetbaar is op zowel mobiele als stationaire platformen. De keuze van technologie hangt af van de toepassing: sommige vereisen hoge vermogens, andere een lange levensduur of grotere energiedichtheid.

Veiligheid is cruciaal. Een incident met een batterij kan materiële schade veroorzaken, levens in gevaar brengen en missies verstoren. Daarom zijn strenge eisen nodig op vlak van ontwerp, materiaalkeuze en monitoring. Dit vraagt om robuuste constructies die bestand zijn tegen trillingen en extreme temperaturen, maar ook om intrinsiek veilige technologieën zoals solid-state batterijen of natrium-ion (Na-ion). Daarnaast zijn functies zoals kortsluitbeveiliging, thermische controle, optimaal thermisch management en isolatiebewaking onmisbaar.

Intelligente batterijmanagementsystemen (BMS) kunnen bijdragen aan veiligheid, duurzaamheid en efficiëntie. Door slim gestuurde monitoring kunnen anomalieën vroegtijdig worden opgespoord, en kan onderhoud voorspellend worden ingepland op basis van de batterijstatus. Geavanceerd beheer helpt ook om degradatie te beperken. Het BMS moet compatibel zijn met verschillende batterijtypes en configureerbaar zijn voor uiteenlopende toepassingen. Interoperabiliteit over data uitwisseling en -beheer is hier zeker een vereiste. Een digitaal batterijpaspoort platform versterkt dit streven naar meer optimaal batterijbeheer.

Efficiënte temperatuurregeling is belangrijk voor de levensduur en de prestaties van de batterij. Batterijen werken het best bij bepaalde temperaturen. Optimaal thermisch beheer van batterijen draait dan ook om het handhaven van een temperatuur om de prestaties en levensduur te maximaliseren. Zowel te hoge als te lage temperaturen zijn schadelijk: extreme temperaturen verminderen de capaciteit en kunnen de batterij permanent beschadigen of de levensduur bekorten. Systemen met actieve koeling of verwarming zijn dan ook essentieel voor een optimaal beheer van de batterij.

In missiegebieden is netstroom vaak niet beschikbaar. Daarom is er nood aan robuuste, mobiele en autonome laadsystemen. Belangrijke vereisten zijn snelle laadtijden, schaalbaarheid (meerdere batterijen tegelijk laden), automatische herkenning van

batterijmodules en compatibiliteit met hernieuwbare energiebronnen zoals zonnepanelen. De ontwikkeling en implementatie van een slim laadbeheer ondersteunt een optimale batterijwerking.

Naast veiligheid is de ontwikkeling van alternatieve technologieën ook belangrijk voor het vinden van de meest geschikte oplossing per toepassing én voor het verminderen van afhankelijkheid van kritieke grondstoffen. Technologieën zoals natrium-ion, lithium-zwavel (LiS), zink-, magnesium- of aluminium-gebaseerde batterijen bieden interessante perspectieven. Hierbij moet ook aandacht gaan naar de haalbaarheid van grondstofontginning, ondersteund met levenscyclusanalyse, en naar de recyclage van batterijmaterialen.

Tot slot is het testen en valideren van batterijoplossingen onontbeerlijk. Vlaanderen beschikt over een sterke basisinfrastructuur en expertise, die met gerichte investeringen verder uitgebouwd kan worden tot een strategisch voordeel.

3.4.3 Voorbeeldonderzoek

In lijn met bovenstaande visie vormt de ontwikkeling en validatie van een modulair lichtgewicht batterijconcept met slimme monitoring, optimaal thermisch management, schaalbare laadinfrastructuur en hoge veiligheidsstandaarden, de basis voor succesvolle integratie van batterijen in uiteenlopende militaire toepassingen, zowel mobiel als stationair. Daarnaast kan Vlaanderen zich ook toeleggen op een adoptie van een digital batterijpaspoort platform en het inzitten daarvan voor duurzaam batterijbeheer.

Voorspellend onderhoud en slim opladen en (thermisch) beheren van batterijen met verminderde degradatie zijn zeker toolsets die een aanzienlijke toegevoegde waarde kunnen opleveren en daarom de moeite waard zijn om in te investeren voor de ontwikkeling en implementatie.

Om een nog sterkere positie te nemen en houden binnen een Europese en globale context is het cruciaal voor Vlaanderen om te blijven investeren in de zoektocht naar alternatieve batterijtechnologieën, eventueel en idealiter met lokale en/of Europese winning en raffinage van de grondstoffen. Levenscyclus (kost) analyses kunnen helpen bij deze strategische keuze.

Vlaanderen kan zich ook duidelijk profileren als een regio voor het testen en valideren van batterijoplossingen in verschillende omstandigheden met gespecialiseerde testplatformen die ook openstaan voor co-ontwikkeling.

3.5 Mogelijke synergieën

Energie Roadmap Synergieën	
Maritiem	Offshore windenenergie, energie-eiland, batterij en brandstofceltechnologie, energievoorziening
Space	Energieopwekking, opslag en management, propulsie
AI	Compute energieconsumptie en -management
Cyber	Energieinfrastructuur cyberbeveiliging
Autonomie	Movement (energievoorziening) technologieen
Luchtvaart en Drones	Aandrijving en energiebeheer
Biotechnologie	Energy-efficient manufacturing biosynthetic materials, energy-efficient exoskeletons
cUAS	bescherming energiecentrales, microgolftechnologie, energiemanagement
Omgeving	energiemanagement sensornetwerken
Geo-Intelligence	AI en sensornetwerken, autonome energieopwekking

4 BESLUIT

De Roadmap Energie en Veiligheid, opgesteld in opdracht van WEWIS Vlaanderen, kadert binnen de ambitie om energiezekerheid, technologische innovatie en defensieve weerbaarheid samen te brengen in één geïntegreerde visie. Energie is, zeker de dag van vandaag, een strategische pijler van veiligheid: zonder betrouwbare, autonome en beschikbare energievoorziening kunnen noch de samenleving, noch Defensie efficiënt functioneren.

De oorlog in Oekraïne heeft de kwetsbaarheid van gecentraliseerde energievoorzieningen en de afhankelijkheid van fossiele brandstoffen scherp blootgelegd. Europa en zijn lidstaten moeten versneld overschakelen op duurzame, gedistribueerde en veilige energiebronnen om hun strategische autonomie en veerkracht te versterken. De Europese Unie erkent dit in initiatieven zoals de *EU Climate Change and Defence Roadmap* (EEAS, 2022), REarmEU en de *Net Zero Industry Act*. Ook de NAVO stelt in haar *Climate Security Action Plan* (2022) dat energiezekerheid en energietransitie centraal staan voor operationele paraatheid.

Voor België betekent dit een dubbele uitdaging én kans: het versterken van de nationale energieautonomie en het verankeren van die capaciteit binnen de Europese veiligheidsstrategie. Vlaanderen beschikt hierbij over een sleutelpositie dankzij zijn industriële kracht, kennisinfrastructuur en beleidsautonomie in energie en innovatie. De Vlaamse energie- en technologiesector is toonaangevend in onder andere netbeheer, vermogenselektronica, batterijtechnologie, waterstof en hernieuwbare energie, en ontwikkelt baanbrekende concepten zoals Small Modular Reactors (SMR), (Sustainable) Aviation Fuel ((S)AF) en alternatieve brandstoffen zoals ammoniak en waterstof.

Vlaanderen onderscheidt zich bovendien door zijn unieke positie in offshore energie en maritieme technologie. De Vlaamse kustzone vormt een strategisch knooppunt binnen de Europese energiearchitectuur, met grootschalige projecten rond offshore wind, energie-eilanden en internationale interconnecties. Deze infrastructuren versterken niet enkel de Europese bevoorradingszekerheid, maar ook de logistieke en operationele slagkracht van Defensie en NAVO-operaties in de Noordzeeregio.

De roadmap benadrukt de nood aan veerkrachtige infrastructuren, autonome microgrids en geïntegreerde energieoplossingen die bestand zijn tegen cyberdreigingen en fysieke verstoringen. Vlaanderen beschikt over de kennis, industrie en testinfrastructuur om deze systemen te ontwikkelen en valideren via zijn onderzoeksinstellingen, strategische clusters en bedrijven.

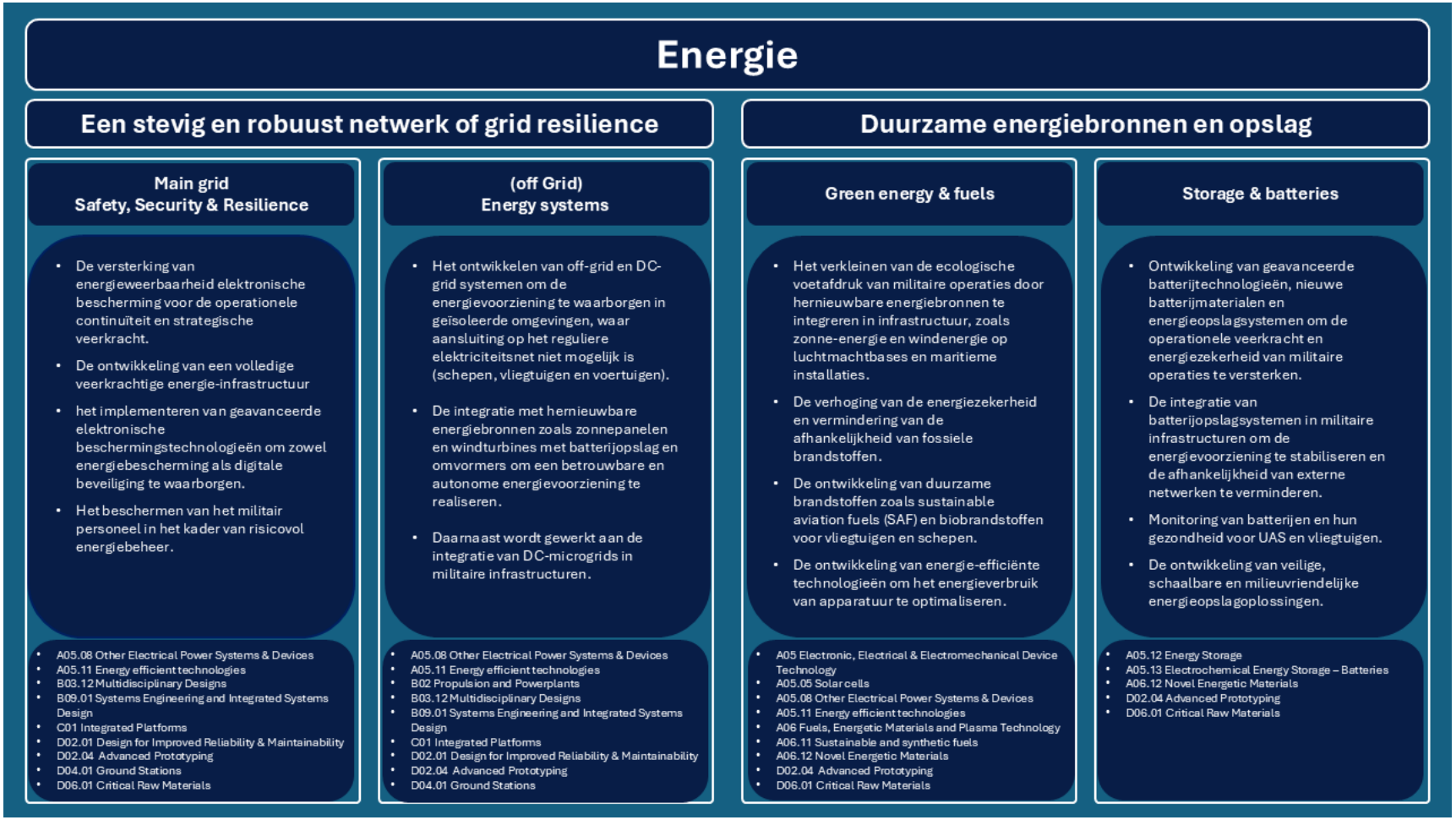
De Roadmap Energie en Veiligheid toont hoe Vlaanderen zijn innovatievermogen kan inzetten om energiezekerheid, duurzaamheid en veiligheid te verbinden tot één geïntegreerde strategie. Door civiele en militaire technologieontwikkeling samen te brengen, kan Vlaanderen uitgroeien tot een Europese referentieregio voor duurzame energie, strategische autonomie en operationele veerkracht.

5 LITERATUURLIJST

1. The EU' climate change and defence roadmap. (n.d.). EEAS. https://www.eeas.europa.eu/eeas/eu-climate-change-and-defence-roadmap_en
2. Nato. (n.d.). NATO Climate Change and Security Action Plan. NATO. https://www.nato.int/cps/en/natohq/official_texts_185174.htm
3. NATO ENSEC COE. (2025, July 24). Home - NATO ENSEC COE. https://www.enseccoe.org/
4. Öğütçü, M., Mistretta, G., Evin, A., Amato, M., Gazzini, C., Cellino, A., Wieczorkiewicz, J., Grazioso, A., Van Den Berg, J., Aboualatta, A., Obeid, J., & Hooker, R. D. (2024). ENERGY STRATEGIES 2024. In A. Minuto-Rizzo, M. Nielsen, S. La Tella, N. Chekrouni, NATO Defense College Foundation, NATO Science for Peace and Security Programme, The Policy Center for the New South, Compagnia di San Paolo Foundation, The NATO Defense College, & Middle East Institute Switzerland, Le Méridien Visconti Hotel (p. 2.30pm-7.15pm) [Conference-proceeding]. https://www.natofoundation.org/wp-content/uploads/2024/11/NDCF-PRESS-Energy-strategies-2024-ENG.pdf
5. Energy Strategies 2023: The Mediterranean: New Resources and Integration. (2023). Ledizioni srl. https://natofoundation.org/wp-content/uploads/2023/09/NDCF-Publication-Energy-Strategies-2023-Web.pdf
6. Signorelli, G. & NATO Energy Security Centre of Excellence. (n.d.). Military aspects of energy security with emphasis on interdependencies between the civil energy sector as a supplier and military as a consumer. In ENERGY H IG HLIG HTS. https://www.enseccoe.org/wp-content/uploads/2024/01/2021-10.pdf
7. NATO Science and Technology Organization. (2025, August 1). Enhancing energy security resilience, capabilities and interoperability | NATO Science and Technology Organization. https://www.sto.nato.int/document/enhancing-energy-security-resilience-capabilities-and-interoperability/
8. Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS). (2017). A ROADMAP FOR SUSTAINABLE ENERGY MANAGEMENT IN DEFENCE AND SECURITY SECTOR. https://eda.europa.eu/docs/default-source/events/eden/phase-i/guidance/consultation-forum-for-sustainable-energy-in-the-defence-and-security-sector---guidance-document.pdf

6 BIJLAGES

6.1 Roadmap



vision on technology
for a better world

Roadmap Omgeving & Veiligheid

Vlaamse innovatie voor een weerbare, duurzame en veilige leefomgeving in dienst van Defensie, Europa, en de NAVO.

Roadmap uitgevoerd in opdracht van: WEWIS - Vlaanderen
Oktober 2025

vito
Vision on technology for a better world
vito.be

Roadmap Omgeving & Veiligheid

Vlaamse innovatie voor een weerbare, duurzame en veilige leefomgeving in dienst van Defensie, Europa, en de NAVO.

VITO
Boeretang 200
2400 MOL
Belgium
BTW No: BE0244.195.916
vito@vito.be – www.vito.be
IBAN BE34 3751 1173 5490 BBRUBEBB

SAMENVATTING

De Roadmap Omgeving & Veiligheid, uitgevoerd in opdracht van WEWIS Vlaanderen, bevestigt Vlaanderen als een sleutelregio in de Europese ambitie om duurzaamheid, veiligheid en technologische innovatie te verbinden. De bescherming van onze leefomgeving is niet langer enkel een ecologische doelstelling, maar een strategische capaciteit die rechtstreeks bijdraagt aan de weerbaarheid van Defensie en de maatschappij.

Vlaanderen beschikt over een uitzonderlijk sterke industriële en wetenschappelijke basis die de ontwikkeling van dual use oplossingen mogelijk maakt. De regio onderscheidt zich door haar expertise in chemie, materialen, biotechnologie, milieusanering, sensortechnologie en circulaire processen. Deze kennisdomeinen worden ondersteund door toonaangevende onderzoeksinstellingen en clusters, die het fundament vormen van een geïntegreerd ecosysteem voor duurzame veiligheid.

De strategische ligging van Vlaanderen versterkt dit profiel. De aanwezigheid van grootschalige industriële clusters, de haven van Antwerpen Brugge als wereldwijde chemische hub, en de Noordzeeregio als toegangspoort tot Europa maken Vlaanderen tot een cruciale schakel in energievoorziening, logistiek en infrastructuurbescherming. Tegelijk brengen deze troeven ook uitdagingen met zich mee: hoge bevolkingsdichtheid, complexe industriële activiteit en kwetsbaarheid voor CBRN e incidenten vragen om geavanceerde detectie, monitoring en saneringstechnologieën waarin Vlaanderen zich technologisch kan onderscheiden.

Binnen de roadmap worden vier strategische pijlers onderscheiden:

(i) **CBRN-e:** Detectie, identificatie, mitigatie en bescherming tegen chemische, biologische, radiologische, nucleaire en explosieve dreigingen.
(ii) **Weerbaarheid van natuurlijke hulpbronnen**: Bescherming van bodem, water en lucht, en van de kritieke infrastructuren die daarop steunen.
(iii) **Critical Raw Materials** (CRM): Zekerstelling en circulair gebruik van schaarse en strategische grondstoffen.
(iv) **Safe & Sustainable by Design** (SSbD): Duurzaam en veilig ontwerp van materialen, processen en infrastructuren gedurende de hele levenscyclus.

De Vlaamse sterktes in sensoren, datafusie, sanering en circulaire materialen sluiten rechtstreeks aan bij Europese en NAVO-prioriteiten rond klimaat, veiligheid en strategische autonomie. Vlaanderen kan deze capaciteiten benutten om concrete toepassingen te ontwikkelen voor defensie, civiele bescherming en infrastructuurbeheer. Door de koppeling van civiele innovatie aan militaire noden versterkt Vlaanderen niet enkel de nationale weerbaarheid, maar ook de Europese veiligheid.

De roadmap beveelt aan om de samenwerking tussen Defensie, Vlaamse agentschappen, kennisinstellingen en industrie structureel te verankeren via gedeelde test en demonstratieomgevingen, geïntegreerde financiering en gezamenlijke innovatieagenda's. Zo kan Vlaanderen evolueren van een sterk maar gefragmenteerd ecosysteem naar een Europese referentieregio voor omgevingsveiligheid, duurzame weerbaarheid en dual-use innovatie.

INHOUDSTAFEL

LIJST VAN AFKORTINGEN

AI	Artificiële Intelligentie
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance & Reconnaissance
CBRN-e	Chemisch, Biologisch, Radiologisch, Nucleair en explosief
CF SEDSS	Consultation Forum for Sustainable Energy in the Defence and Security Sector
CRM	Critical Raw Materials
CRMA	Critical Raw Materials Act
DEFRA	Defence-related Research Action
DIANA	Defence Innovation Accelerator for the North Atlantic
DIM	Detectie, Identificatie en Monitoring
EDA	European Defence Agency
EDF	European Defence Fund
EEAS	European External Action Service
EU	Europese Unie
ISR	Intelligence, Surveillance and Reconnaissance
NAVO / NATO	Noord-Atlantische Verdragsorganisatie / North Atlantic Treaty Organization
NIF	NATO Innovation Fund
PESCO	Permanent Structured Cooperation
PFAS	Per- en polyfluoralkylstoffen
R&D	Research & Development
REarmEU	European Defence Industrial Reinforcement through Common Procurement Act
Seveso	Europese richtlijn inzake industriële risico's
SPS	Science for Peace and Security Programme
SSbD	Safe and Sustainable by Design
TRL	Technology Readiness Level
VITO	Vlaamse Instelling voor Technologisch Onderzoek
VLAIO	Vlaams Agentschap Innoveren & Ondernemen
WEWIS	Departement Werk, Economie, Wetenschap, Innovatie en Sociale Economie

1 VISIE EN CONTEXT

1.1 De omgeving als strategisch domein voor veiligheid en defensie

Onze leefomgeving – bodem, water en lucht – is niet enkel een levensvoorwaarde, maar een strategische component van onze nationale veiligheid en veerkracht. Ze vormt de fysieke ruimte waarin bevolking, infrastructuur en strijdkrachten opereren, en vormt tegelijk de natuurlijke buffer die ons beschermt tegen de gevolgen van klimaatverandering, vervuiling en grondstoffen schaarste.

Binnen het veiligheids- en defensiekader wordt deze omgeving steeds meer erkend als deel van het operationeel domein: het beïnvloedt de paraatheid van troepen, de continuïteit van missies, de logistieke ketens én de legitimiteit van militaire aanwezigheid in de samenleving. De bescherming, monitoring en sanering van die omgeving zijn dus rechtstreeks verbonden met de inzetbaarheid van de strijdkrachten.

Een duurzame, omgevingsbewuste defensie is geen randvoorwaarde, maar een operationele noodzaak. Klimaatverandering, milieuregels, vervuiling en de druk op kritieke hulpbronnen bepalen de contouren van toekomstige missies. Daarom is dit alles van levensbelang en moet een veilige, weerbare maatschappij worden onderhouden, beschermd en verder ontwikkeld. Tijdens conflicten, militaire acties of oefeningen maakt de omgeving echter deel uit van het strategische en tactische kader. Vlaanderen, met zijn industriële en kennisbasis, kan hier het verschil maken door technologieën en processen te ontwikkelen die tegelijk veiligheid, duurzaamheid en strategische autonomie versterken.

1.2 CBRN-e als kernuitdaging

Een moderne defensieorganisatie opereert in een complex risicolandschap waarin chemische, biologische, radiologische, nucleaire en explosieve (CBRN-e) dreigingen opnieuw sterk op de voorgrond treden. Deze dreigingen omvatten zowel klassieke risico's (zoals munitieresten en chemische wapens) als nieuwe vormen van hybride dreiging, waarbij industriële, medische of civiele stoffen bewust worden ingezet als destabiliserend wapen.

Vlaanderen en Brussel vormen een strategische maar kwetsbare regio door de combinatie van hoge industriële bebouwing, logistieke knooppunten en internationale instellingen. De aanwezigheid van havens, luchthavens en petrochemische clusters, met de Haven van Antwerpen-Brugge als een van de grootste chemische- en logistieke complexen ter wereld, verhoogt het risico op CBRN-e-incidenten. Tegelijk huisvest de regio talloze Seveso-bedrijven en vormt te een belangrijk kruispunt voor Europees lucht- en goederenverkeer via Zaventem, Deurne, en Oostende. De Vlaamse havens en verschillende anders transportassen vervullen bovendien een cruciale rol binnen de NAVO-logistiek en militaire mobiliteit, onder meer voor troepenverplaatsingen, materieeltransport en maritieme bevoorrading. België herbergt bovendien het NAVO-hoofdkwartier, diverse EU-instellingen en internationale financiële organisaties, wat de nood aan geïntegreerde detectie-, respons- en beveiligingssystemen verder benadrukt.

Daarnaast blijft ook de moderne CBRN-(e) dreiging actueel: het gebruik van nieuwe chemische agentia, de groeiende risico's van industriële ongevallen en de kans op bio(techno)logische of radiologische incidenten tonen aan dat Detectie, Identificatie en Monitoring (DIM) en Mitigatie essentieel zijn voor operationele paraatheid. De snelle vooruitgang in biotechnologie, synthetische biologie en genetische manipulatie vergroot

bovendien het risico dat biologische agentia doelbewust of accidenteel worden ingezet. Nieuwe technologieën maken het mogelijk om pathogenen of toxines te ontwikkelen met relatief beperkte middelen, wat de drempel voor misbruik verlaagt en nieuwe vormen van asymmetrische dreiging creëert. Recente mondiale gezondheidscrisissen hebben aangetoond hoe biologische incidenten in staat zijn om samenlevingen en logistieke systemen op grote schaal te ontwrichten. Ze benadrukken het belang van structurele paraatheid, robuuste detectiesystemen en geïntegreerd beleid voor crisisrespons.

De nucleaire component vormt binnen dit geheel een belangrijke pijler. België beschikt niet alleen over nucleaire reactoren maar ook over een studiecentrum voor kernenergie (SCK-CEN), over internationaal erkende expertise in nucleaire veiligheid, stralingsbescherming, opslag van radioactief materiaal, radio-ecologie en nucleaire geneeskunde. België vervult een sleutelrol binnen het Joint Research Centre (JRC) van de Europese Unie, onder meer in onderzoek naar stralingsdetectie, nucleaire forensica en veilig afvalbeheer. De verdere uitbouw van ondergrondse opslag- en testinfrastructuur in België via NIRAS creëert bijkomende mogelijkheden voor onderzoek naar veilige berging, monitoring en hersteltechnieken bij radiologische incidenten – kennis die zowel civiel als militair inzetbaar is en bijdraagt aan de Europese nucleaire weerbaarheid.

Vlaanderen beschikt via zijn RTO's, universiteiten, en zijn rijke industriële basis over sterke capaciteiten in oa. sensortechnologie, chemische analyse(s), biotechnologie, materiaalkunde, textiel (persoonlijke beschermingsmiddelen), lucht-, bodem- en watermonitoring en kan daarmee bijdragen aan deze Europese agenda's. Het koppelen van de civiele milieu- en omgevingsmonitoring-expertise aan defensietoepassingen via dual-use innovatie is een logische volgende stap voor het Vlaamse ecosysteem.

1.3 Milieu- en omgevings gerelateerde (be)dreigingen in België en Europa

Naast de CBRN-e risico's waarmee Defensie structureel geconfronteerd wordt, is er een toenemend risico van omgevingsgerelateerde (be)dreigingen die rechtstreeks de operationele capaciteit, infrastructuur en veiligheid beïnvloeden. Deze uitdagingen zijn niet hypothetisch, maar manifesteren zich steeds vaker in de dagelijkse werking van onze strijdkrachten, civiele bescherming en logistieke ketens. Daarbij komt dat de afhankelijkheid van kritische grondstoffen de bevoorradingszekerheid onder druk zet en zo een directe impact heeft op de strategische autonomie van Defensie. Bovendien moeten ook de steeds strengere regelgeving en maatschappelijke eisen op het vlak van omgevings en klimaat gerespecteerd worden. Deze verplichtingen vormen niet alleen een extra uitdaging, maar kunnen ook beschouwd worden als bijkomende bedreigingen voor de operationele flexibiliteit en het gebruik van infrastructuur en materieel.

Deze voornaamste structurele dreigingen omvatten; (**i**) **Vervuiling en verontreiniging**, al dan niet historisch, op oefenterreinen, depots en onderhoudszones door brandstoffen, zware metalen, PFAS en explosieven. De aanwezigheid van zware metalen, chemische residuen en explosieve restanten na militaire operaties of incidenten vraagt om geïntegreerde detectie- en saneringsoplossingen. De situatie in Oekraïne toont hoe grootschalige vervuiling van landbouw- en civiele gronden langdurige risico's creëert en de nood aan snelle technologische interventies benadrukt. (**ii**) **Klimaatverandering en extreme weersomstandigheden** die militaire infrastructuur, missies en logistieke corridors onder druk zetten. Overstromingen bedreigen munitieopslagplaatsen en schietterreinen, terwijl langdurige droogte of hittegolven het gebruik van oefenterreinen en het functioneren van voertuigen en personeel beperken. Bovendien leidt klimaatverandering tot verschuivingen in het leefgebied van ziekteverspreiders, waardoor Defensie bij buitenlandse missies extra rekening moet houden

met nieuwe gezondheidsrisico's. (**iii**) **Afhankelijkheid van kritieke grondstoffen en niet-duurzame productieketens** voor militair materieel, elektronica en energieopslag. Schaarste aan zeldzame aardmetalen, gallium (5G communicatie), germanium (nachtkijkers), lithium en kobalt (batterijen), antimoon (kogels) en andere metalen en mineralen beïnvloedt de bevoorradingszekerheid en strategische autonomie van Europese defensiesystemen. (**iv**) Toenemende **maatschappelijke en regelgevende eisen** op het vlak van omgevings en klimaat, zowel Europees (ESG, emissienormen) als Vlaams (vergunningsplicht, stikstof, PFAS). Defensie moet daardoor steeds vaker rekening houden met thema's als duurzaamheid en vervuiling bij aanbestedingen, materiaalbeheer en infrastructuurontwikkeling.

1.4 Koppeling aan Europese en internationale strategieën

1.4.1 CBRN-e als pijler voor veiligheids- en omgevingsbeleid

Europa wordt geconfronteerd met een heropleving van CBRN-e dreigingen met een steeds hybrider karakter. Naast klassieke militaire risico's groeit het gevaar dat civiele, industriële of medische stoffen doelbewust worden ingezet voor maatschappelijke ontwrichting. De oorlog in Oekraïne, spanningen rond nucleaire installaties en de verspreiding van dual-use technologieën tonen de kwetsbaarheid van Europa, terwijl vijandige actoren internationale verdragen zoals de *Chemical en Biological Weapons Convention* openlijk ondermijnen en zich niet aan regels houden. Daarbovenop neemt ook het risico op accidentele incidenten en onbedoelde emissies toe door verouderde infrastructuur en een toename aan gevaarlijke transporten en industriële activiteiten.

Operationeel blijven de uitdagingen groot: verouderde detectiecapaciteit, beperkte interoperabiliteit tussen lidstaten en een tekort aan gespecialiseerde expertise en medische voorraden. De integratie van CBRN-detectie met digitale dreigingsanalyse en artificiële intelligentie verloopt traag, terwijl nieuwe milieueisen, zoals PFAS-vrije materialen en schone decontaminatie, bijkomende beperkingen en dus nieuwe innovatie vragen.
Deze problematiek wordt internationaal erkend als een van de meest complexe veiligheidsuitdagingen. Binnen de NAVO krijgt de aanpak vorm via het *Joint CBRN Defence Capability Development Framework* en de *CBRN Defence Policy*[1] (2023), die inzetten op interoperabiliteit, gezamenlijke opleiding en capaciteitsopbouw tussen civiele en militaire partners. De *NATO Combined Joint CBRN Defence Task Force*[2] fungeert daarbij als operationeel speerpunt, terwijl de *Allied Command Transformation* (ACT) doctrines ontwikkelt voor geïntegreerde detectie, sanering en medische respons.

Op EU-niveau wordt deze visie geconcretiseerd via het *EU CBRN Action Plan*[3] (2020–2025) en het *Euro-Atlantic Disaster Response Coordination Centre* (EADRCC). Volgens de CapTech 12 - CBRN & Human Factors van het Europees Defensieagentschap (EDA) omvatten de belangrijkste onderzoeks- en ontwikkelingsdomeinen: (**i**) Detectie- en identificatiesystemen voor CBRN-agentia, ook voor grens- en logistieke controles, (**ii**) Persoonlijke beschermingsmiddelen en collectieve bescherming van infrastructuur (TBB 05-07), (**iii**) Gevaarbeheer, modellering en simulatie (TBB 08), (**iv**) Bescherming van kritieke infrastructuur en water-/voedselvoorziening (TBB 09-10), (**v**) Medische tegenmaatregelen en diagnostiek (TBB 11), (**vi**) Integratie van menselijke factoren, training en prestatiemonitoring.
Het *EU CBRN Centre of Excellence Network* (EU CBRN CoE), gecoördineerd door *The European External Action Servic*e (EEAS), versterkt bovendien de kennisuitwisseling en standaardisering tussen lidstaten. Binnen de *NATO Medical Doctrine* (AMedP-7.1)[4] wordt de link tussen CBRN-risico's en omgevingsbeheer expliciet gemaakt: detectie, sanering en herstel van getroffen gebieden vormen er structurele onderdelen van de operationele gezondheids- en nazorg.

Door de aard en schaal van deze risico's is CBRN-e uitgegroeid tot een internationaal en gespecialiseerd domein waarin civiele en militaire diensten structureel samenwerken. In veel landen ligt de eerste respons bij brandweer en civiele bescherming, terwijl Defensie instaat voor strategische ondersteuning, logistiek en medische evacuatie, onder meer bij het transport van hoogbesmettelijke of hemorragische patiënten. België geldt hierin als voorbeeld van civiel-militaire samenwerking, waarbij Defensie fungeert als schakel tussen medische diensten, internationale partners en logistieke capaciteiten, en zo een speerpunt vormt voor CBRN-respons binnen Europa.

Vlaanderen kan binnen dit kader een voorloperspositie innemen door zijn sterktes in sensortechnologie, nucleaire expertise, chemie, biotechnologie en circulaire materialen te koppelen aan defensieve toepassingen. Daarnaast zijn data-analyse, modellering en predictieve technologieën van cruciaal belang binnen het CBRN-e domein. Door geavanceerde datamodellen en artificiële intelligentie in te zetten voor de vroegtijdige detectie, risico-inschatting en simulatie van CBRN-e incidenten, kan Vlaanderen bijdragen aan een snellere en meer gerichte respons. Dit versterkt niet alleen de operationele paraatheid, maar maakt het ook mogelijk om proactief bedreigingen te identificeren en de impact ervan te beperken. Het integreren van deze digitale competenties in defensiegerichte innovaties zorgt ervoor dat Vlaanderen zich onderscheidt als een strategische partner op het snijvlak van technologie, veiligheid en duurzaamheid.

1.4.2 Omgeving als strategische hefboom voor weerbaarheid

Omgevingsuitdagingen staan centraal in de *EU Climate Change and Defence Roadmap*[5] (EEAS, 2022), *Water resilience strategy*[6] (European Commission) het eerste Europese beleidskader dat omgeving en klimaat expliciet verbindt met veiligheid en defensie. De roadmap benoemt drie strategische sporen: (**i**) Klimaatbestendige defensiecapaciteiten voor militaire infrastructuur, materieel en operaties. Deze moeten worden aangepast aan stijgende temperaturen, extreme neerslag en zeespiegelstijging voor wiens deze een bedreiging vormen. (**ii**) Duurzame operaties door oa. reductie van emissies, circulair materiaalgebruik en veilige afvalstromen binnen alle NAVO- en EU-missies. Dit verlaagt niet alleen de ecologische voetafdruk, maar ook de logistieke kwetsbaarheid en de thermische signatuur van operaties, met directe tactische voordelen. (**iii**) Klimaat, rampen en conflictzones als geïntegreerd responsdomein: militaire technologie zoals satellietconstellaties, sensornetwerken en datamodellen wordt ingezet voor vroegtijdige detectie, impactanalyse en ondersteuning van civiele en internationale hulpstructuren.

Parallel hieraan heeft de NAVO in 2021 het *NATO Climate Change and Security Centre of Excellence* (CCASCEO, te Vilnius) opgericht en verschillende rapporten zoals *NATO Climate Change and Security Impact Assessment*[7] (2023) goedgekeurd tesamen met een rapport *Advancing climate security and defence*[8] (2025). Deze strategieën erkennen dat klimaatverandering de strategische omgeving, militaire installaties en logistieke ketens beïnvloedt en dat bondgenoten hun operaties moeten aanpassen aan een veranderende omgeving. De NAVO stelt daarbij expliciet dat "*climate change is a defining challenge of our time, with a profound impact on Allied security*" (*NATO Climate Change and Security Impact*[7], 2023).

Binnen het EDA concretiseert de CapTech 14 "Energy and Environment" deze visie in R&D-prioriteiten. De focus ligt op: (**i**) Omgevingsmonitoring, waterbeheer en emissiereductie op militaire sites, (**ii**) circulaire materiaalstromen en afvalbeheer, (**iii**) energie-efficiënte infrastructuur en mobiliteit, (**iv**) bescherming tegen omgevings- en industriële risico's, (**v**) de vervuiling van lucht, bodem, water of via geluid.

Daarnaast biedt het Co*nsultation Forum for Sustainable Energy in the Defence and Security Sector* (CF SEDSS) binnen EDA een platform waar lidstaten samenwerken aan energiebeheer, klimaatadaptatie en de integratie van hernieuwbare energie in defensie-installaties.

Een bijkomende versterking van deze Europese beleidslijn kwam er met het *REarmEU*-initiatief (2024), het Eu*ropean Defence Industrial Reinforcement through Common Procurement Act*[9]. Dit plan koppelt de industriële herbewapening van Europa expliciet aan duurzaamheid en klimaatbestendigheid. *REarmEU* maakt deel uit van de bredere *Green Deal Industrial Plan*[10] en de *Net-Zero Industry Act*[11], en stelt dat nieuwe investeringen in defensieproductie enkel toekomstbestendig zijn als ze voldoen aan de principes van water- en energie-efficiëntie, emissiereductie, circulaire productie en verantwoorde materiaalvoorziening. Het bouwt verder op de *Critical Raw Materials Act*[12] (CRMA) en de *EU Taxonomy for Sustainable Activities*[13], en stimuleert zo een geïntegreerde benadering van veiligheid, industrie en klimaat.

Samen met de EU- en NAVO-roadmaps vormt *REarmEU* de economische pijler van een nieuw Europees paradigma van “klimaatintelligente defensie”: een benadering waarin vergroening, industriële versterking en operationele weerbaarheid elkaar versterken.

1.5 Strategische vertaling voor Vlaanderen

Vlaanderen staat in een sleutelpositie binnen de transitie naar een duurzamere en veerkrachtigere defensiestructuur. De huidige veiligheidscontext toont dat omgeving, energie en technologie niet langer losstaan van veiligheid, maar er integraal deel van uitmaken. Waar klassieke defensie zich concentreerde op fysieke dreigingen, ligt de nadruk vandaag op strategische autonomie, technologische onafhankelijkheid en duurzame weerbaarheid.

1.5.1 Vlaanderen binnen het federaal, Europees en Trans-Atlantisch kader

België onderschrijft de Europese en NAVO-initiatieven, zoals EDA CapTechs over energie en CBRN, CF SEDSS-platform, en nog tal van andere, en bepaalt zo mee de contouren van de Europese dual-use innovatieagenda. Binnen dat federale kader beschikt Vlaanderen, dankzij zijn bevoegdheden op het vlak van omgeving, energie, innovatie en economie, over een unieke hefboompositie om civiele en militaire synergie structureel te versterken.

Deze Vlaamse bevoegdheden maken het mogelijk om gericht beleid te voeren op de raakvlakken van omgevingsbescherming, technologische ontwikkeling en industriële innovatie. Via zijn onderzoeksinstellingen, universiteiten, speerpuntclusters en economische instrumenten kan Vlaanderen zowel de civiele als defensiegerichte innovatieketen ondersteunen. Daarmee vormt Vlaanderen een intermediaire schakel tussen Europese beleidskaders, federale defensienoden en Vlaamse economische partners.

1.5.2 Strategische rol van Vlaanderen

Vlaanderen kan, dankzij zijn sterk innovatief karakter, een intermediaire schakel spelen tussen Europese beleidskader, Belgische defensienoden en de Vlaamse economische partners door; (**i**) Innovatie en technologieontwikkeling te versnellen door civiele onderzoeksprogramma’s te koppelen aan defensie- en veiligheidsvraagstukken. Deze innovatie zal op zijn beurt het Vlaamse ecosysteem en zijn kmo’s en bedrijven stimuleren. (**ii**) Als test- en demonstratieregio door oefenterreinen, havens, logistieke knooppunten en industriële sites in te zetten als living labs voor dual-use technologieën. Deze kunnen dienen voor het testen van sensoren,

autonome energieoplossingen, saneringstechnieken, circulaire bouwmaterialen en omgevingsmonitoring. (**iii**) Brug tussen industrie, beleid en Defensie door samenwerking te faciliteren tussen Vlaamse bedrijven, onderzoeksinstellingen, clusters en overheden, en hen gericht te verbinden met federale en Europese partners binnen programma's als het European Defence Fund (EDF), DIANA, de EDA CapTechs en REarmEU.

1.5.3 Kansen en opportuniteiten

De koppeling tussen omgeving, technologie en veiligheid opent voor Vlaanderen een reeks strategische kansen. Door de bestaande kennis in energie, data, biotech, ruimtevaart, maritieme technologie en autonomie samen te brengen, kan Vlaanderen uitgroeien tot een Europese voorloper in omgevingsveiligheid en duurzame weerbaarheid.

(i) **Vlaanderen als proeftuin voor innovatieve, weerbare infrastructuur**: de versterking van defensieve en civiele infrastructuur in Vlaanderen zoals havens, logistieke knooppunten, en oefenterreinen biedt kansen om klimaatbestendige, circulaire, en energie- en waterautonome systemen te testen.

(ii) **Nieuwe generatie omgevingsmonitoring en risicobeheer**: Vlaanderen kan zijn leiderspositie in sensortechnologie, datafusie en AI benutten om een integraal systeem voor omgevingsbewaking te ontwikkelen, van luchtkwaliteit tot waterveiligheid en bodemvervuiling. Door sensoren op land, in lucht, onder water en in de ruimte te combineren, ontstaat een multidomeinbeeld van de omgeving. Dit kan zowel worden gebruikt voor rampenpreventie, CBRN-detectie als voor structurele monitoring van kritieke installaties.

(iii) **Autonome en robotische systemen voor sanering en respons**: de Vlaamse expertise in autonome robotica en mechatronica maakt de weg vrij voor onbemande interventie- en saneringssystemen. Drones, onderwaterrobots en grondvoertuigen kunnen ingezet worden voor detectie en neutralisatie van explosieven, chemische lekkages of vervuiling na incidenten.

(iv) **CBRN- en biotechnologie voor omgevingsveiligheid en gezondheid**: Vlaanderen beschikt over sterke wetenschappelijke en industriële capaciteiten in zowel biotechnologie als sensortechnologie. Door deze domeinen te verbinden kan het ecosysteem bijdragen aan de detectie, analyse en mitigatie van chemische, biologische en radiologische dreigingen. Nieuwe biosensoren en fotonische detectiesystemen kunnen toxische stoffen of pathogenen in lucht, water of bodem snel identificeren, terwijl membraan- of bio-based filters en enzymatische processen worden ingezet voor oa. PFAS-afbraak, waterzuivering en sanering. PFAS-afbraak, waterzuivering en sanering.

(v) **Slim water- en grondstoffenbeheer als veiligheidsfactor**: Toegang tot water en kritieke grondstoffen wordt steeds meer een veiligheidsvraagstuk, onze infrastructuur is de dag van vandaag erg kwetsbaar, denk maar aan een besmetting van ons drink- of grondwater. Vlaanderen kan hier zijn sterktes in circulaire economie, watertechnologie (inclusief (drink)waterzuivering), sensoring, en procesindustrie inzetten. Het betreft hier ook mobiele technologie die snelle mobilisatie en demobilisatie toelaten van off-grid zuiveringssystemen in operaties op het terrein of na incidenten om snelle heropbouw te doen.

(vi) **Maritieme en kustgebonden weerbaarheid**: De Vlaamse kustzone is tegelijk een logistieke poort en een kwetsbare zone voor klimaat- en veiligheidsdreigingen. Door maritieme, offshore en omgevingstechnologie te combineren kan Vlaanderen uitgroeien tot een blue defence & resilience hub.

1.5.4 Toekomstgerichte visie

De transitie naar een duurzame, technologische defensie creëert kansen voor Vlaamse bedrijven en kennisinstellingen om niet alleen economische meerwaarde, maar ook maatschappelijke veerkracht te genereren. Door zijn innovatiekracht te koppelen aan federale en Europese investeringsprogramma's kan Vlaanderen bijdragen aan een toekomstgerichte defensieve maatschappij die niet enkel robuuster, maar ook groener, slimmer en strategisch autonomer is.

Vlaanderen kan zo uitgroeien tot een referentieregio voor omgevingsveiligheid en dual-use innovatie, waar duurzaamheid, technologie en veiligheid elkaar versterken. Door actief in te spelen op de Europese en NAVO-prioriteiten bouwt Vlaanderen mee aan een nieuw model van groene defensie, waarin omgevingsbescherming en strategische weerbaarheid hand in hand gaan – en waar civiele innovatie de basis vormt van militaire paraatheid.

2 ECOSYSTEEM MAPPING

2.1 Doel en scope

De ecosysteemmapping die uitgevoerd werd binnen het technologiedomein Environment/Omgeving & Veiligheid biedt een overzicht van het Vlaamse potentieel in omgeving, kritieke materialen en CBRN-e. Ze maakt zichtbaar welke bedrijven, kennisinstellingen en organisaties vandaag over de nodige technologische en wetenschappelijke capaciteiten beschikken om een rol te spelen in de transitie naar een duurzamere, weerbare defensie.

De analyse richt zich op ondernemingen met een duidelijke innovatiecomponent, een bewezen onderzoeksactiviteit of een relevant trackrecord. De geografische afbakening omvat Vlaanderen en het Brussels Hoofdstedelijk Gewest, aangezien de juridische zetel en de operationele tewerkstelling bij veel bedrijven gespreid zijn over beide regio's.
Het doel van de mapping is niet louter inventarisatie maar is gericht op het bekomen van inzicht: ze toont hoe het bestaande civiele ecosysteem kan worden ingezet voor defensieve en dual-use toepassingen. De resultaten dienen als basis voor de verdere concretisering van het Vlaams Impulsprogramma voor Defensie en Veiligheid, en voor de selectie van toekomstige pilootprojecten binnen dit domein.

2.2 Methodologie

De mapping werd opgebouwd volgens een gestructureerde, data-gedreven aanpak die vergelijkbaar is met de methodologie die voor andere Vlaamse technologiedomeinen wordt gehanteerd. Vertrekkend vanuit open bronnen, sectorfederaties, speerpuntclusters en onderzoeksnetwerken werd een longlist samengesteld van bedrijven en organisaties actief binnen CBRN-e, omgeving, kritieke materialen, sanering, circulaire processen en duurzaamheid.
Aanvullende identificatie gebeurde via de Strategische Onderzoekscentra, via deelnemerslijsten van relevante congressen en via netwerken van innovatieplatformen. Vervolgens werd deze lijst gefilterd om enkel ondernemingen op te nemen met een aantoonbare innovatieve rol, een R&D-activiteit of deelname aan onderzoeksprojecten. Louter uitvoerende aannemers of pure maakbedrijven zonder eigen ontwikkelingscapaciteit werden niet opgenomen.

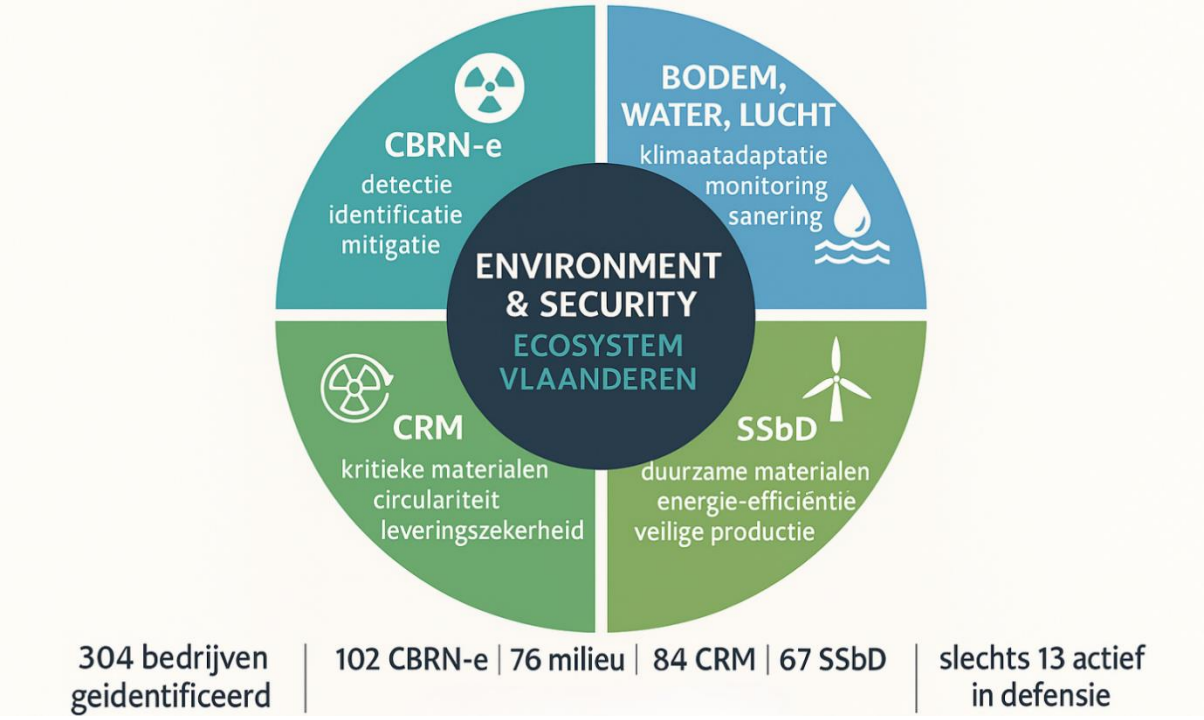
Om duplicatie te vermijden werden dochter- of zusterbedrijven samengebracht onder één bedrijfsnaam. Elke organisatie werd geclassificeerd volgens haar relevante technologiedomeinen: CBRN-e, omgeving (bodem, lucht, water), kritieke materialen en duurzaamheid/Safe and Sustainable by Design. De lijst werd gevalideerd via kruiscontrole met bestaande initiatieven binnen DIANA (*Defence Innovation Accelerator for the North Atlantic*), NIF (*NATO Innovation Fund*), SPS (*Science for Peace and Security Programme*), EDF (*European Defence Fund*), PESCO (*Permanent Structured Cooperation*) en DEFRA (*Defence-related Research Action*) om te bepalen in welke mate de actoren vandaag al betrokken zijn bij internationale dual-use en defensiegerelateerde trajecten.

2.3 Resultaten

In totaal werden 304 bedrijven en organisaties geïdentificeerd met directe of indirecte relevantie voor het domein Environment & Security. Van deze groep vertonen 102 ondernemingen een duidelijke link met CBRN-e (detectie, identificatie, monitoring en mitigatie). Zesentachtig organisaties zijn actief in de bredere omgevingssector, voornamelijk

rond waterbeheer, luchtkwaliteit en bodemsanering. Vierentachtig bedrijven werken aan processen en technologieën rond kritieke materialen, recyclage en hergebruik, terwijl zevenenzestig spelers zich richten op duurzame productie, circulaire materialen of Safe-and-Sustainable-by-Design-oplossingen.

Hoewel de categorieën elkaar deels overlappen, bieden ze een representatief beeld van de omvang, diversiteit en maturiteit van het Vlaamse ecosysteem. Slechts dertien actoren bleken momenteel betrokken bij internationale defensie- of veiligheidsprojecten. Dit beperkte aandeel benadrukt dat Vlaanderen over een sterk technologisch potentieel beschikt, maar dat de structurele vertaling naar de defensiesector nog in haar beginfase zit.



Figuur 1 - Overzicht van het Vlaamse ecosysteem binnen het technologiedomein Environment & Security. SSbD: Safe and Sustainable by Design. CRM: Critical Raw Materials.

2.4 Analyse en inzichten

De resultaten tonen een uitgesproken sterkte in chemie, materialen, sanering en duurzame processen. Vlaanderen huisvest met de Antwerpse chemiecluster één van de grootste en financieel meest robuuste industriële complexen van Europa, met bedrijven die wereldspelers zijn in de domeinen van energie-intensieve productie, zuivering en afvalverwerking. Daarnaast beschikt Vlaanderen over een uitzonderlijk sterke kennisinfrastructuur. Onderzoeksinstellingen spelen een sleutelrol in de ontwikkeling van omgevingstechnologie en de ondersteuning van industrie.

De samenwerking tussen onderzoek, industrie en beleid vormt een belangrijke hefboom. Agentschappen zorgen voor de beleidsmatige vertaling van onderzoeksresultaten naar toepassingen op het terrein. De innovatie wordt bovendien versneld door het strenge regelgevend kader rond omgeving, afval en veiligheid, dat ondernemingen verplicht om voortdurend te investeren in schonere, veiligere en efficiëntere processen.
Toch is er vandaag nog weinig sprake van een structurele koppeling tussen dit sterke civiele ecosysteem en de veiligheids- en defensiesector. De meeste actoren werken in een zuiver

civiel kader en zijn zich niet bewust van hun relevantie voor defensieve toepassingen. Het bestaande potentieel wordt dus nog onvoldoende benut. De technologische fit is nochtans aanzienlijk: innovaties in monitoring, sanering, circulaire productie, energie-efficiëntie en risicobeheer sluiten rechtstreeks aan bij de noden van Defensie en civiele bescherming.

2.5 Vaststellingen en beleidsimplicaties

2.5.1 Civiele sterktes, beperkte vertaling naar defensie

De mapping toont dat Vlaanderen beschikt over een uitzonderlijk sterke industriële en wetenschappelijke basis in omgeving, chemie, energie en materialen, maar dat deze kracht vandaag nog onvoldoende wordt benut binnen veiligheids- en defensiecontext. De technologieën die in Vlaanderen ontwikkeld worden, van sanerings- en monitoringoplossingen tot circulaire productieketens, sluiten naadloos aan bij de operationele noden van Defensie. Toch blijft de structurele vertaling van civiele innovatie naar dual-use toepassing beperkt.

De kloof tussen potentieel en toepassing is niet technologisch, maar structureel van aard. Vlaanderen beschikt over de kennis, infrastructuur en ondernemingen, maar mist de mechanismen om civiele innovaties te valideren, te certificeren en te valoriseren voor operationele inzet. Het ontbreken van gedeelde testfaciliteiten en veiligheidsmachtigingen vormt een belangrijke drempel, vooral voor kmo's die moeilijk toegang vinden tot defensienetwerken en validatieprocedures. Grotere bedrijven beschikken wel over schaal en internationale ervaring, maar missen vaak directe aansluiting bij onderzoeks- of beleidsinitiatieven.

2.5.2 Versnippering in samenwerking en beleid

Samenwerking binnen het Vlaamse ecosysteem verloopt vandaag nog te gefragmenteerd. Sterke netwerken bestaan binnen civiele domeinen zoals voor CBRN-e, energie, chemie, circulaire economie en sanering, maar deze zijn zelden structureel verbonden met de (inter)nationale veiligheidsagenda. Hierdoor blijven veel technologieën met directe defensierelevantie, zoals sensornetwerken, risicomodellering, waterbeheer of duurzame bouw, voornamelijk beperkt tot civiele toepassingen. De (historische) beleidsinstrumenten en financieringskanalen versterken die fragmentatie, net zoals het dogma dat erg lang rond defensie en veiligheid hing. Vlaamse instellingen zoals VLAIO, OVAM, VMM en de Strategische Onderzoekscentra ondersteunen omgevingstechnologie, terwijl Defensie hoofdzakelijk opereert binnen Europese kaders als EDA, EDF en DIANA. Vlaamse bedrijven die hun innovatie willen inzetten in een veiligheidscontext, botsen daardoor op verschillende administratieve en normatieve lagen. Zonder gecoördineerde beleidslijn blijven de meeste samenwerkingen afhankelijk van toevallige projectkansen in plaats van een geïntegreerde strategie.

2.5.3 Behoefte aan integratie en gedeelde infrastructuur

De analyse toont dat de belangrijkste hefboom voor groei ligt in de integratie van beleid, infrastructuur en financiering. Vlaanderen heeft nood aan geïntegreerde proeftuinen en testomgevingen waar civiele technologieën gevalideerd kunnen worden in realistische operationele omstandigheden. Militaire domeinen, oefenterreinen en havenzones kunnen hiervoor dienen als living labs voor sanering, monitoring, energie-autonomie en circulaire bouw. Dergelijke omgevingen vormen de ontbrekende schakel tussen laboratoriumonderzoek en daadwerkelijke inzetbaarheid en versnellen de stap van TRL 6–9 naar operationele implementatie.

Daarnaast is een systematische vraag-aanbodmatching cruciaal. Door de noden van Defensie te koppelen aan beschikbare Vlaamse technologieën via een gestandaardiseerde vraag-aanbodmatrix, kunnen actoren sneller partnerschappen vormen. Zo wordt duidelijk welke technologieën kansrijk zijn voor dual-use ontwikkeling en welke expertise nog ontbreekt.

Tot slot is er nood aan versnelling en valorisatie. Technologieën in de overgangsfase tussen onderzoek en marktintroductie vragen specifieke begeleiding richting certificatie, veiligheidsmachtiging en aansluiting bij Europese programma's. Het Vlaamse Impulsprogramma kan hier een structurele rol opnemen door TRL 6–9-projecten te ondersteunen die strategische autonomie combineren met maatschappelijke veerkracht.

2.5.4 Gebruik van bestaande expertise en regelgeving

Een bijkomende beleidskans ligt in de vertaling van de bestaande Seveso-expertise naar defensieve contexten. Vlaanderen beschikt over unieke kennis rond risicozonering, noodplanning en industriële veiligheid. Die ervaring kan worden toegepast op munitieopslagplaatsen, logistieke ketens en infrastructuren waar gevaarlijke stoffen aanwezig zijn. Door civiele veiligheidsstandaarden te integreren in militaire omgevingen, kan Defensie niet alleen operationele veiligheid verhogen, maar ook maatschappelijke draagkracht en expertise versterken.

Daarnaast kan Vlaanderen zijn ervaring met milieuregulering, circulaire economie en energiebeheer inzetten als beleidsmodel binnen de Europese veiligheidsarchitectuur. De koppeling van civiele en militaire duurzaamheidsdoelstellingen kan Vlaanderen positioneren als laboratoriumregio voor defensie: een plek waar omgevingstechnologie, industriële innovatie en veiligheidsbeleid samenkomen.

2.5.5 Van kennis naar coördinatie

De belangrijkste les uit de ecosysteemanalyse is dat de toekomst van duurzame veiligheid niet begint bij nieuwe technologie, maar bij het verbinden van bestaande sterktes. Vlaanderen beschikt over de kennis, netwerken en industriële slagkracht om snel te schakelen. Wat vandaag ontbreekt, is coördinatie: het systematisch verbinden van onderzoek, industrie en beleid via gedeelde structuren, testinfrastructuren en financiering.

Door deze coördinatie te organiseren kan Vlaanderen zijn ecosysteem heroriënteren naar operationele waardecreatie. Het openstellen van testfaciliteiten, het opzetten van gezamenlijke validatie- en certificatiekaders en het beter afstemmen van Vlaamse, federale en Europese financieringslijnen zijn hierbij cruciaal.

De analyse toont dat het momentum aanwezig is. De Europese herbewapening, de Green Deal en de maatschappelijke druk creëren een nieuw beleidskader waarin veiligheid, omgeving en technologie elkaar versterken. Vlaanderen kan dit momentum benutten om zijn civiele innovatiebasis te verbinden met defensieve noden en zo een nieuwe industriële pijler van duurzame veiligheid te ontwikkelen.

2.5.6 Beleidsrichting voor de volgende fase

De ecosysteemmapping vertaalt zich in drie strategische prioriteiten voor Vlaanderen.

(i) Ten eerste moet Vlaanderen de ontwikkeling van test- en demonstratie-infrastructuur structureel verankeren. Deze infrastructuur fungeert als de brug tussen civiele innovatie en defensieve toepassing en is essentieel om technologische maturiteit te versnellen.

(ii) Ten tweede is een gestroomlijnde governance nodig waarin Defensie, Vlaamse agentschappen en industrie samen prioriteiten bepalen. Door gezamenlijke roadmaps, matchmaking en dual-use calls te organiseren, kan het beleidsproces aanzienlijk versneld worden. De verdere uitwerking van ODIN is hierin al een grote stap voorwaarts.

(iii) Ten derde vraagt de opkomst van omgevingsveiligheid om een nieuwe kennis- en opleidingsarchitectuur. Vlaanderen kan, in samenwerking met Defensie en zijn kennisinstellingen, opleidingen ontwikkelen die civiele en militaire vaardigheden rond omgevingsveiligheid, CBRN, sanering, energiebeheer en crisisrespons integreren.

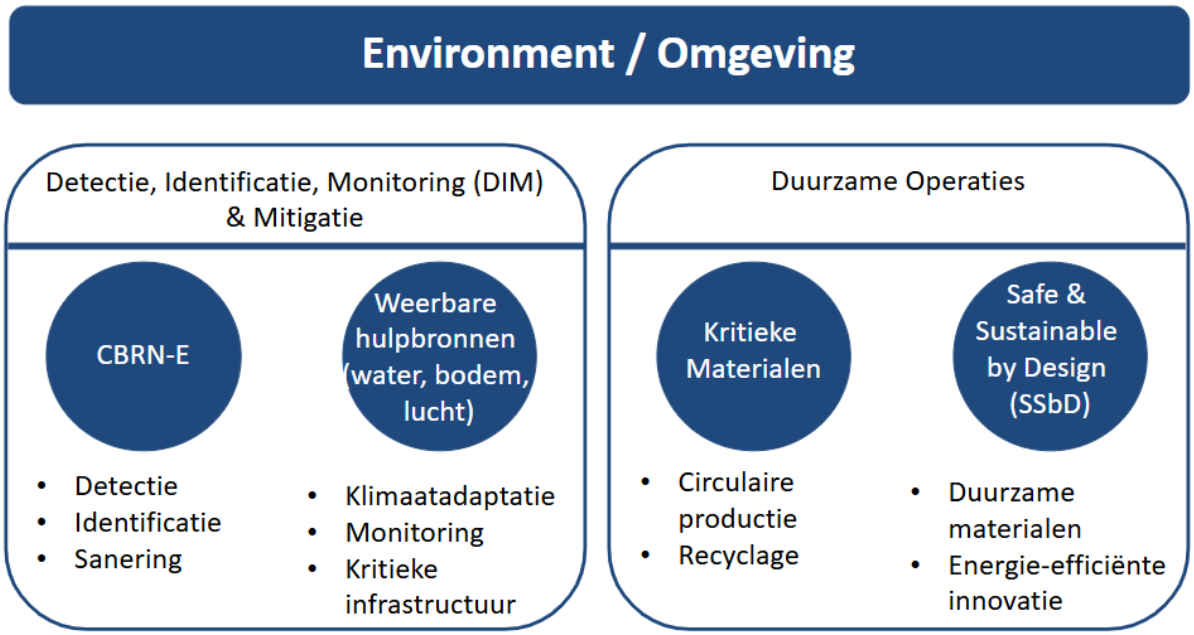
Zo evolueert Vlaanderen van een sterk maar versnipperd innovatielandschap naar een gecoördineerd ecosysteem dat technologie, beleid en veiligheid met elkaar verbindt. Door deze aanpak systematisch uit te rollen kan Vlaanderen zich positioneren als referentieregio voor omgevingsveiligheid en duurzame weerbaarheid binnen Europa.

2.6 Conclusie

De ecosysteemanalyse toont dat Vlaanderen over alle bouwstenen beschikt voor duurzame veiligheid: een robuuste industrie, een sterke kennisbasis en een duidelijk regelgevend kader. Door civiele en militaire innovatieketens te integreren, kan Vlaanderen uitgroeien tot een voortrekker van een nieuw Europees model waarin duurzaamheid, veiligheid en strategische autonomie één geïntegreerde agenda vormen.

3 ROADMAP

De huidige en toekomstige uitdagingen op het gebied van Detectie, Identificatie en Monitoring (DIM) en mitigatie in defensie zijn veelzijdig en cruciaal voor het waarborgen van paraatheid en veerkracht. Enerzijds omvat dit het domein CBRN-e, waarin de ontwikkeling van geavanceerde detectie- en monitorsystemen voor chemische, biologische, radiologische, nucleaire en explosieve agentia centraal staat. Innovaties richten zich op realtime identificatie, opsporing van illegaal transport, robuuste decontaminatie- en mitigatiestrategieën, persoonlijke beschermingsmiddelen, medische tegenmaatregelen en het integreren van menselijke factoren in training en respons. Anderzijds zijn er de uitdagingen rond weerbaarheid van de natuurlijke hulpbronnen (bodem, water en lucht), waarbij technologieën voor early warning, detectie en monitoring van omgevingsbedreigingen, beheersing en verwijdering van vervuiling, duurzaam resource management en bescherming van kritieke infrastructuur essentieel zijn om de weerbaarheid van de omgeving te verhogen op externe schokken. Beide domeinen vragen om integratie van sensortechnologie, data-analyse en modellering, en bieden mogelijkheden voor dual-use toepassingen in landmacht, maritiem en lucht- en ruimtevaartoperaties. Innovaties in deze pijlers kunnen niet alleen militaire paraatheid versterken, maar ook civiele veiligheid verbeteren en de ecologische duurzaamheid van operaties verhogen, door de ontwikkeling van slimme detectiesystemen, omgevingsvriendelijke mitigatieprocessen en adaptieve strategieën voor operationele weerbaarheid tegen zowel CBRN-e incidenten als omgevings-uitdagingen.



Figuur 2 – Eenvoudige weergave van de roadmap Omgeving & Veiligheid. De volledige roadmap is als bijlage achteraan terug te vinden.

3.1 Pijlers

3.1.1 CBRN-e

De onderzoeksuitdagingen voor CBRN-e richten zich op vier hoofdgebieden die cruciaal zijn voor het waarborgen van paraatheid en veerkracht.

1. **Detectie, monitoring en modellering**

   - Ontwikkeling van geavanceerde systemen voor detectie, identificatie en realtime monitoring van CBRN-agentia. Innovaties kunnen gericht zijn op staalafname, nieuwe analytische methodologieën voor snellere detectie, non-targeted chemische karakterisatie voor identificatie van nieuwe en ongekende chemicaliën, off-line en draagbare systemen, high-throughput en automatisering en voorspellende capaciteiten. Nieuwe generatie sensoren, nanotechnologie of lab-on-chip kunnen apart of als multimodaal en geïntegreerd systeem ontwikkeld worden. Drones en robots kunnen dergelijke systemen transporteren voor remote toepassingen. Draagbare sensoren bieden mogelijkheden voor persoonlijke detectie voor militaire of civiele eerstehulpverleners.

   - Gebruik van modellering en simulatie om verspreiding, impact en scenario's te voorspellen. Simulatiemodellen kunnen verspreiding van chemische of biologische stoffen in lucht, water of grond voorspellen. Aan de hand van scenario-analyses en digitale twins kunnen responsstrategieën, voordat incidenten plaatsvinden, getest worden.

   - Ontwikkeling van geavanceerde opsporingstechnieken voor het onderscheppen van illegale transporten en versterking van grenscontrolecapaciteiten gebruik makende van scanners en sensoren voor detectie van verborgen goederen en sporen van explosieven of CBRN-stoffen.

2. **Bescherming van personeel en infrastructuur**

   - Innovatie in persoonlijke beschermingsmiddelen (PBM) voor militair en civiel personeel, met focus op effectiviteit en comfort. Dergelijke innovaties richten zich op effectieve bescherming tegen chemische, biologische en ballistische dreigingen, gecombineerd met lichtgewicht, ademend en modulair ontwerp voor comfort en mobiliteit. Daarnaast worden slimme technologieën zoals sensoren, communicatie-integratie en exoskeletten ingezet om veiligheid, situational awareness en operationele efficiëntie te verhogen.

   - Innovaties op het vlak van monitoring en bescherming van kritieke infrastructuur zoals energiecentrales, watervoorzieningen en communicatienetwerken. Verzekering van de bevoorrading is cruciaal. Contaminatie detecteren en identificeren, bronopsporing in geval van besmetting, voorkomen van cyber aanvallen zijn voorbeelden van cruciale technologische innovaties die bijdragen aan de weerbaarheid en continuïteit van vitale systemen. Dit omvat onder meer de ontwikkeling van geïntegreerde sensornetwerken voor realtime monitoring, AI-gestuurde analyses voor vroegtijdige dreigingsdetectie, communicatiestructuren en cyber-fysieke beveiligingsoplossingen die zowel digitale als fysieke risico's aanpakken. Daarnaast spelen dataplatformen voor snelle informatie-uitwisseling tussen civiele en militaire diensten een sleutelrol in een gecoördineerde respons op incidenten.

3. **Gevaarbeheer en medische tegenmaatregelen**

    - Ontwikkeling van geavanceerde methoden voor decontaminatie, inperking en mitigatie van CBRN-agentia Slimme barrièresystemen, dynamische luchtsluizen en nieuwe filtersystemen zijn enkele voorbeelden om verspreiding te beperken. Geavanceerde materialen (zoals Metal Organic Frameworks), enzymatische en biotechnologische middelen kunnen ingezet worden om toxische stoffen te absorberen en/of af te breken.
    - Onderzoek naar medische tegenmaatregelen, waaronder vaccins, tegengif, behandelingen en diagnostische hulpmiddelen. Opmerking: mogelijke innovaties in dit thema worden uitvoering toegelicht in de Biotech roadmap.

4. **Hybride dreigingen en menselijke factoren**

    - Onderzoek naar hybride dreigingen die militaire en civiele middelen combineren en mogelijke tegenmaatregelen.
    - Integratie van menselijke factoren in training, prestatiemonitoring en technologie voor effectieve respons en veerkracht.

3.1.2 Weerbaarheid van natuurlijke bronnen en bijhorende kritieke infrastructuur

De onderzoeksuitdagingen voor de verhoging van de weerbaarheid van natuurlijke hulpbronnen en hun bijhorende kritieke infrastructuur, zoals bv de waterproductie en waterzuiveringsinfrastructuur, situeren zich op het vlak van mapping-, sensing- en early detectie systemen, prepardness via forecasting modellen en doorrekening van emergency scenario's, opruim- en saneringstechnologieën voor opkomende en specifieke chemische stoffen die vrijkomen bij militaire of andere activiteiten. Dit niet alleen voor de kritieke civiele infrastructuur maar ook die van de militaire bases. Ook onderzoek naar inzet van geavanceerde zuiverings- en waterbereiding bij snelle (de)mobilisatie van eenheden en evaluatie van de geschiktheid van het terrein vanuit de werking van het bodem-watersysteem (wateraanvoer en –afvoer), zijn verder te onderzoeken en te implementeren.

1. **Omgeving- en hulpbronnenbeheer**

    - Geavanceerde detectie en beheersingtechnieken van vervuiling in bodem, water en lucht. Verdere ontwikkeling van sanerings- en beheersingstechnologie voor de verwijdering van opkomende en specifieke chemische stoffen gerelateerd aan oorlogsvoering.
    - Innovaties met betrekking tot het efficiënt gebruik en bescherming van natuurlijke hulpbronnen, inclusief recycling en duurzame praktijken.
    - Bescherming van kritieke infrastructuur tegen omgevings- en andere bedreigingen. Impacts en risicoanalyse van interrupties in energievoorziening op het waternetwerk (uitvallen van pompen, kleppen...), malfunctie van de waterbereidingsketen, contaminatie, cybersecurity. Mapping en scenario analyse met modellen om te evalueren waar best herstelmaatregelen dienen te worden genomen.

2. **Klimaat- en weerbaarheidsstrategieën**
    - Ontwikkeling van adaptieve strategieën om militaire infrastructuur, logistieke ketens en missies te beschermen tegen de gevolgen van klimaatverandering en extreme weersomstandigheden.
    - Versterking van de operationele en ecologische weerbaarheid van militaire sites door duurzame, soevereine energievoorziening, waterbeheer en infrastructuur.
    - Beperking van gezondheidseffecten van omgevings- en klimaatveranderingen op militair en civiel personeel via vroegtijdige detectie, monitoring en aanpassing van operationele procedures.
    - Gebruik van predictive modelling en remote sensing om klimaatgerelateerde risico's en risico's van extreme condities door menselijk handelen en sabotage (contaminatie, droogte, overstromingen, erosie, incidenten in de waterbereiding en waterzuiveringsketen, damdoorbraken) vroegtijdig te identificeren en te mitigeren. Integratie van sensorische metingen (bodem, water, lucht) in modellen om hun predictieve capaciteit te verhogen, gebruik van hybride datagedreven en mechanistische modellen.
3. **Technologische innovatie rond detectie en sanering**
    - Ontwikkeling van geavanceerde detectie- en monitoringsystemen voor realtime opvolging van bodem-, water-, en luchtkwaliteit met toepassingen in risicobeheer en operational support.
    - Innovatie in materialen, processen en systemen om bodem-, water- en luchtkwaliteit te verbeteren.
    - Integratie van technologieën om ecologische duurzaamheid en veerkracht bij defensieoperaties te waarborgen.

De transitie naar Duurzame Defensieoperaties vormt een belangrijke onderzoeks- en innovatieprioriteit voor de komende jaren. Binnen dit domein spelen twee pijlers een cruciale rol: Critical Raw Materials (CRM) en Safe & Sustainable by Design (SSbD).

Bij **CRM** ligt de focus op het waarborgen van een veilige en betrouwbare toeleveringsketen voor schaarse en strategisch belangrijke materialen, zoals zeldzame aardmetalen, lithium en kobalt, gallium, germanium en antimoon die essentieel zijn voor moderne wapensystemen, energieopslag en elektronica. Onderzoek richt zich op recycling en substitutie van kritieke materialen. Innovaties in productieprocessen en materiaalontwikkeling kunnen zowel defensie- als civiele toepassingen ondersteunen, zoals energiezuinige voertuigen, maritieme batterijsystemen of lucht- en ruimtevaartcomponenten met een langere levensduur en lagere omgevings-impact.

De **SSbD**-pijler richt zich op duurzaamheid en veiligheid van materialen en operaties gedurende de volledige levenscyclus van defensiematerieel en infrastructuur. Dit omvat het verbeteren van energie-efficiëntie, het integreren van hernieuwbare energiebronnen, het toepassen van veilig en omgevingsvriendelijk materiaalgebruik en het implementeren van effectief afvalbeheer. Daarnaast worden strategieën ontwikkeld om de ecologische impact van militaire operaties te beperken en de klimaatbestendigheid van infrastructuur en logistieke netwerken te versterken. Dual-use toepassingen zijn hier duidelijk zichtbaar: innovaties in energie-efficiëntie en circulaire materialen kunnen zowel militaire voertuigen als civiele transport- en industriële systemen duurzamer maken.

Het gecombineerde onderzoek naar CRM en SSbD biedt kansen om defensieoperaties te transformeren door technologische innovatie, duurzame inkooppraktijken en samenwerking tussen overheden, industrie en onderzoeksinstellingen. Voor landmacht, maritiem en lucht- & ruimtevaartoperaties betekent dit concreet dat voertuigen, schepen, drones, infrastructuur en ondersteunende systemen niet alleen operationeel robuust en paraat blijven, maar ook minder afhankelijk worden van schaarse grondstoffen, omgevingsvriendelijker functioneren en dual-use voordelen opleveren voor civiele toepassingen.

3.1.3 Critical Raw Materials

De onderzoeksuitdagingen rond kritieke grondstoffen voor defensie kunnen worden samengevat als volgt:

1. **Beveiliging en veerkracht van toeleveringsketens**
    - Waarborgen van een betrouwbare aanvoer van kritieke grondstoffen door de inzet van digital twins voor materiaaltransporten en geavanceerde logistieke modellen. Door transporten te scannen bij vertrek en aankomst, of door slimme sensoren te integreren, kan de integriteit van transporten beter worden gecontroleerd en gegarandeerd.
    - Aanpakken van geopolitieke risico's door diversificatie van leveranciers en strategische partnerschappen om innovatieve technologieën in te zetten en verder te ontwikkelen. Dit versterkt de veerkracht van waardeketens en verkleint de afhankelijkheid van onvoorspelbare markten en producenten met een monopolypositie.
    - Aanleggen en beheren van strategische voorraden en reserves voor crisisbestendigheid. Ontwikkeling van methoden en processen om de operationele inzetbaarheid van strategische materiaalstocks in productieprocessen te verhogen door reductie van onzuiverheden, diversificatie van intermediaire producten, en bewaringscondities te optimaliseren door bijvoorbeeld oxidatieve degradatieprocessen te vertragen.
2. **Efficiëntie en circulair gebruik**
    - Verbetering van het efficiënt gebruik van grondstoffen via innovatieve productieprocessen zoals 3D-printing en andere additieve vormgevingstechnieken. Deze bieden ook kansen op het vlak van lichtgewicht structuren en hieraan gelinkte energiezuinigheid. Ook qua ontwerp van structureel sterke materialen en met betrekking tot impact resistentie bieden deze technieken unieke mogelijkheden in een defensie context.
    - Vermindering van de afhankelijkheid van schaarse materialen door slimme materiaalkeuzes en hergebruik. Recyclage op grondstofniveau is daarbij niet de enige optie: ook herstel en hergebruik van onderdelen bieden nieuwe kansen, ondersteund door AI-gebaseerde beslissingsalgoritmen.

3. **Technologische innovatie**

   - Ontwikkeling van nieuwe materialen, methoden en productietechnologieën om winning, verwerking en gebruik van kritieke grondstoffen te optimaliseren. Selectieve organische, anorganische of hybride sorbenten en/of solventen voor extractie van strategische of kritieke metalen uit een complexe matrices bieden diverse strategische troeven. Ook geavanceerde pyrometallurgische processen zijn cruciaal om bepaalde metalen te herwinnen uit complexe ertsen of rest/afvalstromen.
   - Ondersteuning van defensiecapaciteit via geavanceerde toepassingen en productieprocessen zoals 3D-printing maken het mogelijk om sneller iteratieve ontwikkeling te doen van kritische componenten. De maakindustrie evolueert op dit vlak enorm snel en biedt ook mogelijkheden om productiecapaciteiten snel op te schalen. Bovendien kan een productie snel overgezet worden naar één of meerdere andere locaties in functie van strategische behoeftes.

3.1.4 Safe & Sustainable by Design

1. **Energie en klimaatbestendigheid**

   - Verbeteren van energie-efficiëntie en integratie van hernieuwbare energie in defensie-infrastructuur en -operaties.
   - Versterken van de veerkracht van infrastructuur en activiteiten tegen klimaatverandering en extreme weersomstandigheden.

2. **Materialen en omgevingsbeheer**

   - Ontwikkeling en gebruik van veilige, soevereine materialen bij materieel en infrastructuur. Onderzoek naar de impact van additieven en chemische componenten in textiel en ander materieel op de gezondheid. Ontwikkeling van richtlijnen met betrekking tot veilig ontwerp en gebruik, inclusief verwerking en recyclage op het einde van de levensduur.
   - Implementatie van effectief afvalbeheer, recycling en bescherming van ecosystemen tijdens defensieactiviteiten. Doorgedreven karakterisatie en inventerisatie van afvalstromen voor gerichte recyclage en bescherming van de leefomgeving.

3. **Inkoop, innovatie en samenwerking**

   - Bevordering van inkooppraktijken die voldoen aan omgevings- en rechtelijke normen.
   - Stimuleren van innovatie en samenwerking tussen overheden, industrie en onderzoeksinstellingen voor het aanpakken van duurzaamheidsuitdagingen. Kennis hieromtrent delen op regionaal, nationaal en internationaal vlak.

3.2 Mogelijke Synergieën

Omgeving Roadmap	Synergieën
Maritiem	Maritieme/water omgeving, sensors, havens, logistiek
Space	aardobservatie
AI	environmental sensing, digital twins
Cyber	Cyberbeveiliging van CBRN-e sensornetwerken en digitale infrastructuur, digital twins
Autonomie	Sensortechnologieen
Luchtvaart en Drones	Ultra-materialen, toeleveringsketens, circulair gebruik
Biotechnologie	CBRN-e detectie/monitoring en bescherming
cUAS	Te exploreren
Geo-Intelligence	Sensors, AI, datafusie
Energie	AI en sensornetwerken, autonome energieopwekking

4 BESLUIT

De opmaak van deze Roadmap Omgeving & Veiligheid, uitgevoerd in opdracht van WEWIS Vlaanderen, bevestigt dat Vlaanderen over alle noodzakelijke bouwstenen beschikt om een voortrekkersrol te spelen in de integratie van civiele en defensiegerichte innovatie. Vlaanderen combineert een sterke industriële en wetenschappelijke basis met unieke geografische en economische troeven, wat het tot een strategische hefboom maakt binnen België en Europa.

De analyse toont aan dat Vlaanderen excelleert in domeinen zoals milieutechnologie, chemie, materialen, energie, biotechnologie en sensortechnologie. Deze expertises vormen samen een krachtig fundament voor dual-use innovatie op het raakvlak van milieu, veiligheid en strategische autonomie. Door de bestaande kennis in detectie, sanering, circulaire processen en energiebeheer te koppelen aan defensietoepassingen kan Vlaanderen bijdragen aan een nieuwe generatie oplossingen die duurzaamheid en veiligheid combineren.

De Vlaamse havens en industriële clusters, waaronder de haven van Antwerpen-Brugge en de Noordzeeregio, versterken dit strategisch profiel. Ze fungeren als logistieke knooppunten, energiehubs en testzones voor innovatie, maar zijn tegelijk kwetsbaar voor hybride dreigingen en milieuvervuiling. De bescherming, monitoring en verduurzaming van deze infrastructuren zijn dan ook niet enkel economische prioriteiten, maar strategische veiligheidsdoelstellingen van nationaal en Europees belang.

De verwezenlijking van deze visie vraagt om structurele coördinatie tussen Defensie, Vlaamse beleidsdomeinen, kennisinstellingen en industrie. Door gezamenlijke roadmaps, gedeelde testomgevingen en afgestemde financieringsmechanismen te ontwikkelen, kan Vlaanderen evolueren van een gefragmenteerd innovatielandschap naar een geïntegreerd ecosysteem voor duurzame veiligheid. Daarbij kan Vlaanderen fungeren als brug tussen civiele innovatie en Europese veiligheidsarchitectuur, met een sterke positie binnen programma's zoals het European Defence Fund (EDF), de European Defence Agency (EDA) en REarmEU.

De roadmap benadrukt dat omgeving, energie en grondstoffenbeheer niet langer ondersteunende thema's zijn, maar strategische capaciteiten die de basis vormen van toekomstige weerbaarheid. De bescherming van onze leefomgeving is een veiligheidsvraagstuk geworden dat investeringen in kennis, technologie en samenwerking vereist.

Met deze roadmap schetst Vlaanderen een toekomstgerichte visie waarin veiligheid, duurzaamheid en innovatie één geïntegreerde agenda vormen. Door zijn kennis, beleid en industrie te verbinden, kan Vlaanderen uitgroeien tot een Europese referentieregio voor omgevingsveiligheid, duurzame weerbaarheid en dual use innovatie — een regio waar civiele en militaire vooruitgang elkaar versterken in het belang van een veiligere en veerkrachtigere samenleving.

5 LITERATUURLIJST

1. Nato. (n.d.). *NATO's Chemical, Biological, Radiological and Nuclear (CBRN) defence policy*. NATO. https://www.nato.int/cps/en/natohq/official_texts_197768.htm
2. Nato. (n.d.). Combined Joint Chemical, Biological, Radiological and Nuclear (CBRN) Defence Task Force. NATO. https://www.nato.int/cps/en/natohq/topics_49156.htm
3. EUR-LEX - 52017DC0610 - EN - EUR-LEX. (n.d.). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0610
4. NATO - AMEDP-7.1 - MEDICAL MANAGEMENT OF CBRN CASUALTIES | GlobalSpec. (n.d.). https://standards.globalspec.com/std/13429656/amedp-7-1
5. The EU' climate change and defence roadmap. (n.d.). EEAS. https://www.eeas.europa.eu/eeas/eu-climate-change-and-defence-roadmap_en
6. Water resilience strategy. (n.d.). European Commission. https://commission.europa.eu/topics/environment/water-resilience-strategy_en
7. Nato. (n.d.). NATO releases 2024 Climate Change and Security Impact Assessment Report. NATO. https://www.nato.int/cps/en/natohq/news_227571.htm
8. Enhancing climate security and defence. (n.d.). EEAS. https://www.eeas.europa.eu/eeas/enhancing-climate-security-and-defence_en
9. EU Defence Industry Reinforcement Through Common Procurement Act (EDIRPA). (n.d.). European Commission. https://commission.europa.eu/strategy-and-policy/eu-budget/performance-and-reporting/programme-performance-statements/eu-defence-industry-reinforcement-through-common-procurement-act-edirpa_en
10. The Green Deal Industrial Plan. (n.d.). European Commission. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/green-deal-industrial-plan_en
11. Net-Zero Industry Act. (n.d.). European Commission. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/green-deal-industrial-plan/net-zero-industry-act_en
12. European Critical Raw Materials Act. (n.d.). European Commission. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/green-deal-industrial-plan/european-critical-raw-materials-act_en
13. EU taxonomy for sustainable activities. (n.d.). Finance. https://finance.ec.europa.eu/sustainable-finance/tools-and-standards/eu-taxonomy-sustainable-activities_en

6 BIJLAGE

6.1 Roadmap

vision on technology
for a better world

vito

Roadmap Geo-Intelligence

Vlaamse bijdragen aan een geïntegreerde en veerkrachtige informatiepositie voor veiligheid, defensie en crisisrespons in Europa

Studie uitgevoerd in opdracht van: WEWIS - Vlaanderen
Oktober 2025

vito
Vision on technology for a better world
vito.be

Roadmap Geo-Intelligence

Vlaamse bijdragen aan een geïntegreerde en veerkrachtige informatiepositie voor veiligheid, defensie en crisisrespons in Europa

VITO
Boeretang 200
2400 MOL
Belgium
BTW No: BE0244.195.916
vito@vito.be – www.vito.be
IBAN BE34 3751 1173 5490 BBRUBEBB

SAMENVATTING

Geo-intelligence (GEOINT) vormt de ruggengraat van moderne defensie, veiligheid en crisisrespons. Het domein combineert data uit satellieten, drones, radar en open bronnen met artificiële intelligentie om near-realtime **situational awareness** en **informatie-overmacht** te realiseren. Vlaanderen beschikt over sterke dual use competenties in AI, remote sensing, datafusie en hightech productie, en kan daarmee een strategische rol opnemen binnen de Europese veiligheidsarchitectuur.

België investeert tussen 2026 en 2034 ruim €3,5 miljard in de pijler *Intelligence–Cyber–Influence (ICI)*, met focus op ruimte-inlichtingen, drones, data-infrastructuur en AI-platformen. De geplande *Multi-Domain Operations Cloud* moet 24/7 multisource situational awareness bieden, ook bij GPS-verstoring. Vlaanderen versterkt deze ambitie via samenwerking met ESA, EDA, EDF en NAVO.

Op Europees niveau erkent de *EU Space Strategy for Security & Defence* ruimte als veiligheidsdomein en bevordert het *IRIS²*-programma veilige communicatie en strategische autonomie. De *EDA* en het *EDF* ondersteunen interoperabele GEOINT-standaarden, terwijl de NAVO GEOINT beschouwt als “critical enabler” voor multi-domain operations, met innovatie via *DIANA* en het *NATO Innovation Fund*.

Vlaanderen onderscheidt zich binnen dit ecosysteem door een sterk **downstream-profiel**. De regio telt 138 bedrijven actief in geo-intelligence, waarvan 66 al deelnemen aan Europese of NAVO-programma’s. Strategische Onderzoekscentra zoals VITO bestrijken de volledige keten van sensor tot analyse en validatie, vaak binnen living labs in haven-, kust-, stedelijke en industriële context. Deze nauwe samenwerking tussen onderzoek, industrie en eindgebruikers versnelt de ontwikkeling en adoptie van dual-use innovaties en maakt Vlaanderen tot een betrouwbare partner in Europese waardeketens.

De Vlaamse GEOINT-roadmap richt zich op vier strategische pijlers:

1. **Multisensor-fusie:** integratie van EO-, SAR-, RF-, IR- en hyperspectrale data tot één betrouwbaar operationeel beeld dat situational awareness versterkt.
2. **Edge-intelligentie:** verwerking aan de bron met compacte, energie-efficiënte AI-modellen voor autonome detectie en snelle besluitvorming.
3. **Veilige geodata-infrastructuur:** cyberweerbare, gefedereerde en soevereine datanetwerken die data-integriteit en continuïteit waarborgen.
4. **Besluitvormingsplatformen en digitale tweelingen:** geïntegreerde visualisatie-, simulatie- en analysetools die interoperabiliteit met NAVO- en EU-systemen verzekeren.

Samen vormen deze pijlers een sluitende keten van waarnemen, verwerken, versterken en beslissen. Geo-intelligence evolueert daarmee tot een sleuteltechnologie voor Europese veiligheid, strategische autonomie en weerbaarheid. Vlaanderen beschikt over de kennis, infrastructuur en bedrijven om hierin een voortrekkersrol te spelen. Via triple-helixsamenwerking, living-lab-validatie en gerichte investeringen kan het Vlaams impulsprogramma deze troeven omzetten in operationele meerwaarde, economische groei en een sterke positie binnen de **European Defence Technological and Industrial Base (EDTIB)**.

INHOUDSTAFEL

LIJST VAN AFKORTINGEN

AI	Artificial Intelligence
AIS	Automatic Identification System
ADIV	Algemene Dienst Inlichtingen en Veiligheid
API	Application Programming Interface
CBRN	Chemical, Biological, Radiological and Nuclear
CIS	Communication and Information Systems
DIANA	Defence Innovation Accelerator for the North Atlantic
Defra	Defence-related research or funding
EDA	European Defence Agency
EDF	European Defence Fund
EDIS	European Defence Industrial Strategy
EO	Earth Observation
ESA	European Space Agency
EU	Europese Unie
FPGA	Field-Programmable Gate Array
GEOINT	Geospatial Intelligence
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
ICI	Intelligence–Cyber–Influence
IR	Infrared
IRIS²	Infrastructure for Resilience, Interconnectivity and Security by Satellite
ISR	Intelligence, Surveillance and Reconnaissance
JISR	Joint Intelligence, Surveillance and Reconnaissance
Kmo	Kleine en middelgrote onderneming
LiDAR	Light Detection and Ranging
ML	Machine Learning
NATO / NAVO	North Atlantic Treaty Organization / Noord-Atlantische Verdragsorganisatie
NCIA	NATO Communications and Information Agency
NIF	NATO Innovation Fund
PESCO	Permanent Structured Cooperation
PNT	Positioning, Navigation & Timing
RF	Radio Frequency
SAR	Synthetic Aperture Radar
SOC	Strategisch Onderzoekscentrum
SPS	Science for Peace and Security
STANAG	Standardization Agreement
TRL	Technology Readiness Level
UAV	Unmanned Aerial Vehicle
VLAIO	Vlaams Agentschap Innoveren & Ondernemen

1 VISIE EN CONTEXT

Geo-intelligence bevindt zich op het snijvlak van defensie, veiligheid en technologische innovatie. Het domein omvat het verzamelen, verwerken, analyseren en inzetten van geospatiale data uit diverse bronnen, van satellieten, drones en radar tot open data en signalen uit maritieme, lucht- en cyberdomeinen. Binnen defensie en veiligheid groeit de nood aan betrouwbare, geïntegreerde en near realtime geo-intelligence als fundament voor situational awareness, besluitvorming en respons. Vlaanderen heeft sterke kaarten in dit domein, dankzij bestaande competenties in artificiële intelligentie, remote sensing, datafusie en hightech productie. De uitdaging is om deze sterktes te positioneren in een Europees kader en te benutten voor het versterken van de European Defence Technological and Industrial Base (EDTIB).

1.1 Het strategisch belang van geo-intelligence in defensie

De militaire en veiligheidsrol van Geo-intelligence wordt steeds duidelijker. Waar dit vroeger louter een hulpmiddel was, evolueert dit nu naar een centrale pijler in de moderne veiligheid strategieën. Het is nu een cruciale component van afschrikking, crisisrespons en digitale soevereiniteit.

In Vlaanderen is een sterke dual-use kennisinfrastructuur uitgebouwd, waar zowel civiele als defensietoepassingen samenkomen. De Strategische Onderzoekscentra (SOC's) voeren verschillende programma's rond geo-intelligence en werken actief mee aan projecten binnen NAVO, het European Defence Fund (EDF) en de Belgische Defensie.

Ook VLAIO ondersteunt vandaag al diverse geo-intelligence-gerelateerde initiatieven, met toepassingen in infrastructuurbewaking, klimaatanalyse, crowd monitoring en andere veiligheids- en observatiedomeinen. De resulterende informatie wordt nu al ingezet bij crisissituaties zoals overstromingen en droogte, in samenwerking tussen Defensie en Vlaamse overheidsdiensten.

1.1.1 België en Vlaanderen

Geo-intelligence, of GEOINT, krijgt in België een steeds prominentere rol binnen de defensiestrategie. De **Militaire Strategische Visie Defensie 2025** plaatst GEOINT voor het eerst centraal in de werking van de krijgsmacht. Binnen de nieuwe capacitaire pijler *Intelligence–Cyber–Influence (ICI)* wordt **informatiesuperioriteit** aangeduid als de bepalende factor om op elk niveau, strategisch, operationeel en tactisch, het initiatief te behouden.

Om dat mogelijk te maken, investeert Defensie tussen **2026 en 2034 meer dan € 3,5 miljard** in ICI-capaciteiten. Een belangrijk deel daarvan gaat naar **ruimte-inlichtingen, drones, data-infrastructuur** en **digitale analyseplatformen**. De **Algemene Dienst Inlichtingen en Veiligheid (ADIV)** breidt haar geo-capaciteiten uit met nieuwe satelliet- en dronesensoren, grootschalige datacenters en **AI-systemen** die informatie uit uiteenlopende bronnen, van open data tot geclassificeerde beelden, samenbrengen in één beveiligde omgeving.

Daarnaast werkt Defensie aan een **Multi-Domain Operations Cloud**, een netwerk van datacenters dat grote geospatiale datasets veilig opslaat en in bijna realtime verdeelt over commandoposten en operationele eenheden. AI-gestuurde analysetools filteren die datastromen en leveren direct bruikbare inzichten aan planners, piloten en

marinecommandanten. Tegen **2035** wil België 24/7 beschikken over **multisource situational awareness**, ook in omgevingen waar GPS wordt verstoord of satellieten worden bedreigd.

De **Strategische Visie Defensie 2025**[1] en het **Vlaams Defensieplan 2025**[2] benadrukken dat deze ambities enkel haalbaar zijn door **nauwe samenwerking tussen overheid, industrie en kennisinstellingen**. Vlaanderen beschouwt geo-intelligence als een **sleuteltechnologie** op het kruispunt van **AI, ruimtevaart en veiligheid**, en integreert het in een breder innovatie-ecosysteem. België bouwt bovendien bewust bruggen met **ESA, EDA, EDF en NAVO**, om toegang te krijgen tot gedeelde sensoren, standaarden en opleidingen.

1.1.2 Europese Unie en EDA

Ook op Europees niveau krijgt geo-intelligence een duidelijke strategische invulling. De **EU Space Strategy for Security & Defence**[3] **(2022)** erkent de ruimte als een volwaardig veiligheidsdomein en legt de nadruk op **gemeenschappelijke dreigingsanalyse, weerbaarheid, collectieve actie en dual-use innovatie**. Om de Europese **strategische autonomie** te versterken, lanceerde de EU het **IRIS²-programma**[4]: een eigen satellietconstellatie voor veilige breedband- en command-and-control-communicatie, als Europees alternatief voor commerciële netwerken zoals Starlink.

De **European Defence Agency (EDA)** en het **European Defence Fund (EDF)** spelen een structurele rol in de opbouw van Europese GEOINT-capaciteiten. Het **EDA Capability Development Plan**[5] erkent sinds 2023 *Information Superiority* en *Geo-Intelligence* als prioritaire capaciteitsgaten. De **EDF-oproepen** sluiten daar nauw bij aan en financieren prototypeontwikkeling en interoperabele standaarden. Dankzij deze koppeling vloeien **EDA-standaarden (STANAG)** rechtstreeks door naar EDF-projecten, zodat industriële consortia hun technologieën later naadloos kunnen inzetten binnen EU- of NAVO-missies.

Binnen de **EDA CapTechs** wordt geo-intelligence vanuit verschillende invalshoeken ontwikkeld. Belangrijke domeinen zijn:

- **CapTech 3 – Optronics**, rond elektro-optische dataverwerking, aardobservatie en situational awareness;
- **CapTech 15 – Space**, gericht op ruimtegebaseerde observatie (EO/SAR), PNT en Space Situational Awareness;
- **CapTech 4 – Information (CIS & Networks)**, dat zich richt op datafusie, analyse en visualisatie van (geo)informatie.
- Daarnaast zijn er raakvlakken met **CapTech 8 – Ground Systems** (sensoren op landplatformen) en **CapTech 1 – Technologies & Components** (sensor- en elektronica-bouwstenen).

Het **European Defence Industrial Strategy**[6] **(EDIS, 2024)** en het **EDF** voorzien samen structurele financiering, terwijl de **EU White Paper Readiness 2030**[7] de nadruk legt op weerbaarheid en informatiedominantie, met geo-intelligence expliciet benoemd als *enabling capability*.

1.1.3 NAVO en de internationale context

Ook binnen de **NAVO** is geo-intelligence uitgegroeid tot een onmisbare pijler van moderne defensie. Sinds de **Overarching Space Policy**[8] **(2019)** en de **NATO 2030-agenda**[9] wordt

GEOINT beschouwd als een **‘critical enabler’** voor **multi-domain operations**. De **Joint Intelligence, Surveillance and Reconnaissance (JISR)**-doctrine[10] erkent de nood aan geïntegreerde geospatiale informatie voor effectieve besluitvorming.

In 2025 introduceerde de NAVO een nieuwe **Commercial Space Strategy**, die drie duidelijke doelstellingen formuleert:

1. het systematisch benutten van commerciële oplossingen,
2. het garanderen van ononderbroken toegang tot ruimtedata, en
3. het bewaken van beleidscoherentie tussen de 32 bondgenoten.

Geo-intelligence fungeert daarbij zowel als **afschrikmiddel**, door transparantie en attribution, als **force multiplier**, door de inzet van commerciële en alliantiebrede sensorfusion in *contested space*-omgevingen. Initiatieven zoals **DIANA (Defence Innovation Accelerator for the North Atlantic)** en het **NATO Innovation Fund (NIF)** stimuleren innovatie rond data- en AI-gedreven geospatiale technologieën. Tijdens recente NAVO-toppen benadrukte de **NATO Communications and Information Agency (NCIA)** bovendien het belang van **industriële partnerschappen** om de geospatiale slagkracht van de alliantie verder te versterken.

1.1.4 Conclusie

Geo-intelligence ontwikkelt zich razendsnel tot een sleutelcapaciteit binnen de hedendaagse defensiearchitectuur, van Vlaanderen tot Europa en de NAVO. Het vormt de ruggengraat van informatiesuperioriteit, essentieel voor situational awareness, strategische besluitvorming en multi-domain-operaties. Door de combinatie van technologische innovatie, AI-integratie en internationale samenwerking groeit GEOINT uit tot de verbindende schakel tussen sensoren, data en veiligheid in een steeds complexer geopolitiek landschap.

1.2 Visie op de toekomstige evolutie

In de komende tien jaar zal geointelligence verder evolueren naar een **interdomeintechnologie** die verweven is met maritieme, luchtvaart, cyber en ruimtevaartdomeinen. Deze verwevenheid opent kansen voor nieuwe toepassingen, maar vereist ook nauwe samenwerking en gezamenlijke standaarden. Vlaanderen kan zich profileren als **innovatieve test en validatieregio** waar nieuwe geointelligence capaciteiten worden ontwikkeld, getest en gevalideerd in realistische omgevingen. Daarbij ligt de nadruk op:

- **Innovatiegericht ecosysteem**: triple helixsamenwerkingen die nieuwe technologieën sneller naar de markt brengen.
- **Industrieel versterkingspunt**: Vlaamse bedrijven als betrouwbare partners in Europese waardeketens.
- **Internationale positionering**: Vlaanderen als nichespeler in AIgedreven geointelligence en datagedreven veiligheidstoepassingen, met aansluiting op EDA CapTechs, NAVOinnovatiekaders en andere Europese waardeketens.

De technologische ontwikkeling binnen **geo-intelligence** wordt vandaag aangedreven door enkele duidelijke trends.

Een eerste is de **exponentiële groei van data**. De hoeveelheid sensordata afkomstig van ruimtevaart-, lucht- en maritieme platforms neemt razendsnel toe. Dat creëert een dringende nood aan schaalbare infrastructuren en **AI-gedreven verwerkingsmethoden** om deze datastromen om te zetten in bruikbare inzichten.

Daarnaast evolueert het veld naar een **multisensor- en multimodale aanpak**. Door het combineren van optische beelden, Synthetic Aperture Radar (SAR), LiDAR, hyperspectrale data, AIS- en SIGINT-bronnen ontstaat een veel robuuster informatiebeeld, bruikbaar onder alle weersomstandigheden en in uiteenlopende operationele omgevingen.

De verdere **digitalisering en integratie van artificiële intelligentie** vormen een derde belangrijke trend. Nieuwe foundation models en machinelearningtechnieken maken snelle detectie, classificatie en change detection mogelijk. Tegelijk brengen ze nieuwe uitdagingen met zich mee op het vlak van **uitlegbaarheid, ethiek en veiligheid**.

Voor toepassingen in defensie en veiligheid speelt ook **edge computing** een steeds grotere rol. Verwerking moet dichter bij de sensor plaatsvinden om te voldoen aan de vereisten van **lage latentie en hoge responsiviteit**.

Ten slotte wordt **veilig datadelen** een cruciale voorwaarde voor samenwerking. De **interoperabiliteit en federatieve governance** van data bepalen in grote mate hoe vlot partners, sectoren en landen informatie kunnen uitwisselen en gezamenlijk opereren.

Geointelligence is geen geïsoleerd domein maar een kruispunttechnologie die de effectiviteit en veiligheid van diverse toepassingsdomeinen versterkt. Vlaanderen heeft de troeven om in dit veld een leidende rol te spelen binnen Europa, mits gerichte investeringen, slimme samenwerking en een duidelijk innovatiepad. Het impulsprogramma moet dit potentieel ontsluiten door schaalbare infrastructuur, marktcreatie en talentontwikkeling te stimuleren, en zo bijdragen aan zowel Vlaamse als Europese veiligheid en industriële veerkracht.

2 STAKEHOLDERMAPPING

2.1 Inleiding

De Europese veiligheids- en crisisuitdagingen vragen om permanente, betrouwbare waarneming en verkenning, bescherming van eigen troepen en burgers, detectie van chemische/biologische/radiologische/nucleaire dreigingen op afstand, en een actueel omgevingsbeeld op zee, in de ruimte en aan land. Succes hangt af van drie dingen: **meerdere sensoren slim combineren, de tijd tussen detectie en beslissing verkorten, en robuuste, veilige dataketens die met besluitvormingssystemen kunnen koppelen.**

Vlaanderen biedt hier een uitgesproken downstream-profiel: sterk in **sensorintegratie, datafusie en kunstmatige intelligentie**, verwerking dicht bij de **sensor (edge)** en in de **cloud**, en open standaarden richting **besluitvormingssystemen**. Onze **micro- en nano-elektronica** en fotonica maken compacte, energiezuinige meetapparatuur en rekenmodules mogelijk. Cruciaal is ook de publieke kennisbasis: kenniscentra zoals VITO bestrijken **de hele remote sensing keten**, van aardobservatie-tasking en voorbewerking, over **multisensor datafusie** (optisch, infrarood, hyperspectraal, radar), AI-gestuurde veranderingenkaarten, tot **visualisatie en integratie met operationele systemen**. Dit gebeurt **living-lab-gedreven** (havens, kust, industrie, stedelijk), wat validatie en uitrol versnelt. Tegelijk vertaalt de Vlaamse industrie (**componenten, subsystemen, integratie, data- en softwarehuizen**) deze kennis snel naar producten en diensten die exporteerbaar zijn binnen Europese samenwerkingen. Stakeholders en eindgebruikers (**havens, kritieke-infrastructuurbeheerders, veiligheidsdiensten, civiele bescherming en beleidsmakers**) co-ontwerpen en valideren, waardoor oplossingen sneller operationeel worden.

2.2 De Vlaamse geo-intelligence sector

De Vlaamse **geo-intelligence-sector** telt een brede en diverse groep industriële bedrijven en organisaties. Er is een stevige basis van ondernemingen met vestigingen en tewerkstelling in **Vlaanderen en Brussel**, die actief zijn in uiteenlopende onderdelen van deze technologische waardeketen.

De **mapping** van het ecosysteem werd opgebouwd via een systematische inventarisatie van relevante actoren: bedrijven die actief zijn in de sector, vermeld worden in media of sectorrapporten, of zich hebben gemanifesteerd als **start-ups, scale-ups of innovatieve kmo's**. Ook **middelgrote en grotere ondernemingen** met een bewezen innovatietrackrecord en deelname aan onderzoeksprojecten werden opgenomen.

Een bijkomende groep bedrijven werd geïdentificeerd via **sectorfederaties, speerpuntclusters** en **koepelorganisaties** die actief zijn rond ruimtevaart, data, AI of veiligheid. Daarnaast boden **deelnemerslijsten van thematische events en wetenschappelijke congressen** waardevolle input: zij tonen welke ondernemingen momenteel investeren in of onderzoek doen naar geo-intelligence. Ook de **Strategische Onderzoekscentra (SOC's)** bleken een belangrijke bron van informatie, gezien hun nauwe samenwerking met innovatieve bedrijven binnen hun onderzoeksnetwerken.

De samenstelling van de mapping is **niet statisch** en zal regelmatig moeten worden bijgewerkt naarmate het inzicht in de sector groeit en nieuwe spelers opduiken. Sommige bedrijven zullen verdwijnen, andere zich verder ontwikkelen of heroriënteren.

Om de focus te behouden, werden enkel bedrijven opgenomen die een **duidelijke innovatieve rol** vervullen of promoten. Zeer kleine ondernemingen of éénmansvennootschappen met louter een adviserende functie werden niet meegenomen, tenzij ze een aantoonbare rol spelen binnen grotere projecten of samenwerkingen.

Omdat het onderscheid tussen maatschappelijke zetel en effectieve tewerkstellingsplaats vaak moeilijk te maken is, werden ook **Brusselse bedrijven** opgenomen. Veel ondernemingen hebben immers vestigingen in beide regio's en functioneren binnen dezelfde Vlaamse innovatiecontext. Bedrijven met meerdere locaties of dochterondernemingen zijn samengebracht onder één merknaam, die dus meerdere vennootschappen kan vertegenwoordigen.

In totaal werden **138 bedrijven** geïdentificeerd. Een aanzienlijk aantal is actief in meerdere technologiedomeinen, waarvan **geo-intelligence** er één is.
De verdeling binnen de belangrijkste technologische clusters toont volgende cijfers:

- **Sensors & on-board dataverwerking:** 90 bedrijven
- **Edge computing & autonome verwerking:** 67 bedrijven
- **Weerbare en robuuste datainfrastructuur:** 44 bedrijven
- **Samenwerkende data-infrastructuren:** 60 bedrijven

Veel ondernemingen bestrijken meerdere onderdelen van de geo-intelligence-keten. Van deze groep zijn **66 bedrijven** betrokken bij lopende **DIANA-, NIF-, SPS-, EDF-, PESCO- of Defra-projecten**. De **samenwerking met Defensie** of binnen **dual-use toepassingen** is dus nu al sterk aanwezig. Dit illustreert het aanzienlijke **groeipotentieel** en de stevige basis van **innovatieve kmo's** in Vlaanderen.

Vlaanderen positioneert zich duidelijk als een **actieve speler in geo-intelligence-technologieën**. Dat onderscheidend vermogen komt voort uit strategische beleidskeuzes, nauwe samenwerking tussen **industrie, overheid en kennisinstellingen**, en een reeks **gerichte innovatie-initiatieven**.

Binnen het Vlaamse ecosysteem vinden we bedrijven die letterlijk de **volledige keten** afdekken: van **"het oog" (de sensor)** tot **"het inzicht" (de analyse)**. Aan de bron staan spelers die **camera's en sensoren** ontwikkelen voor gebruik in de ruimte of op drones, van optische en infraroodcamera's die haarscherpe beelden leveren tot radars en **hyperspectrale scanners** die zelfs door wolken of rook heen details detecteren.

Andere bedrijven bouwen aan **satellietsystemen en communicatienetwerken** die data betrouwbaar naar de grond sturen. Steeds vaker wordt die data **on-board of aan de rand (edge)** verwerkt, zodat enkel relevante informatie wordt doorgestuurd en beslissingen sneller kunnen worden genomen.

Een onmisbare schakel in dit geheel is **Positioning, Navigation & Timing (PNT)**. Vlaamse bedrijven leveren hier robuuste **ontvangers en timingoplossingen** die zorgen dat data nauwkeurig geolokaliseerd en getimestamped blijft, ook in situaties waarin **GPS-signalen worden verstoord**.

2.3 Lessen en opportuniteiten uit het stakeholderlandschap

De Vlaamse **geo-intelligenceketen** wordt gedragen door een sterk netwerk van **onderzoekspartners, industriële spelers en eindgebruikers**, die elk een essentiële rol vervullen in de ontwikkeling en toepassing van nieuwe technologieën.

De **onderzoeksinstellingen** focussen op **methodiekinnovatie, standaardisatie, validatie** en het verhogen van technologische maturiteit. Ze zorgen bovendien voor de **opleiding van gespecialiseerd talent** dat het ecosysteem versterkt. De **industrie** bestrijkt het volledige traject van **componenten en subsystemen** tot **systeemintegratie, data- en softwarediensten, operaties en ondersteuning**. De **eindgebruikers en beleidsactoren**, waaronder havens, logistieke spelers, beheerders van kritieke infrastructuur, veiligheidsdiensten en regulatoren, brengen **operationele eisen, data en validatiecriteria** aan en helpen succesvolle innovaties op te schalen.

De samenwerking tussen deze actoren krijgt vorm via **living labs**, waar technologieën in reële omgevingen worden getest en verfijnd. Door te werken met **gedeelde prestatie-indicatoren** en **open standaarden** ontstaat een omgeving die bijdraagt aan **Europese interoperabiliteit** en versnelde innovatie.

Uit de stakeholdermapping komen duidelijke inzichten naar voren:

1. **Ecosysteem boven silo's:** de grootste waarde ligt in de volledige keten – van sensor tot beslissing – gedragen door samenwerking tussen onderzoek, industrie en eindgebruikers.
2. **Dual-use versnelt innovatie:** civiele en defensietoepassingen delen dezelfde bouwstenen; hergebruik verkort de tijd tot inzet en versterkt exportkansen.
3. **Verwerking dicht bij de sensor** verhoogt robuustheid en vermindert vertraging en bandbreedtegebruik.
4. **Datakwaliteit en standaarden** zijn belangrijker dan modelcomplexiteit: herkomst, annotatie en governance bepalen de operationele waarde.
5. **Betrouwbare positionering en cyberweerbaarheid** vormen onmisbare basisvoorwaarden.
6. **Living-lab-validatie** in haven-, stads-, industriële of kustomgevingen verkleint adoptierisico's en versnelt certificatie.
7. **Open architecturen** houden systemen vervangbaar, uitbreidbaar en interoperabel.

Vlaanderen profileert zich als **partner van keuze** voor **downstream geo-intelligence**: (i) multisensor-integratie, (ii) datafusie en AI, (iii) verwerking dicht bij de sensor, (iv) interoperabiliteit en (v) living-lab-validatie. Het ecosysteem combineert **sterk onderzoek** met **innovatieve industrie** en **operationele stakeholders**, waardoor nieuwe technologieën snel inzetbaar worden.

Vlaamse spelers vormen zo een complementaire schakel naast Europese hoofdaannemers en ruimtevaartpartners, met **schaalbare, datagedreven oplossingen** en **snelle operationele adoptie**. De mapping bevestigt een solide basis aan **bouwstenen, informatiesystemen, platformcapaciteit** en **test- en validatiefaciliteiten**, precies wat nodig is voor moderne toepassingen in **waarneming, verkenning, bescherming, aardobservatie-gestuurde crisisrespons** en de **detectie van CBRN-dreigingen op afstand**.

3 ROADMAP

3.1 Inleiding

Geo-intelligence (GEOINT) heeft de voorbije jaren een stormachtige ontwikkeling doorgemaakt, mede door de zogeheten **lagebaanrevolutie** in de ruimtevaart. De lage aardbaan is vandaag volledig *open for business*: het ontwikkelen en exploiteren van satellieten is niet langer het exclusieve domein van overheden of defensie, maar ook **bedrijven en kennisinstellingen** kunnen er hun innovatieve ideeën realiseren.

Tegelijk breidt **data-acquisitie** zich uit tot een veel breder spectrum van bronnen. Niet alleen satellieten, maar ook **luchtvaartuigen, drones, maritieme platforms, grondgebonden sensornetwerken en mobiele systemen** leveren een explosieve groei aan observatiegegevens. Deze combinatie van ruimte-, lucht-, zee- en landgebaseerde waarnemingen creëert een **ongekende rijkdom aan data**, die de basis vormt voor moderne geo-intelligence-toepassingen.

Geo-intelligence speelt een steeds belangrijkere rol in het monitoren en begrijpen van onze omgeving, van de open zee tot stedelijke gebieden en binnenlandse waterwegen.

Op zee en in het mariene milieu kan GEOINT worden ingezet om zowel **ecologische als veiligheidsaspecten** te bewaken. Naast satellietwaarnemingen leveren ook **sensoren op schepen, boeien en autonome drones of vaartuigen** waardevolle gegevens. Zo kan men **waterkwaliteit opvolgen**, **olielekken detecteren en analyseren**, **rivier- en kanaalstructuren in kaart brengen** en **de verspreiding van plasticvervuiling monitoren**. Geo-intelligence biedt bovendien krachtige middelen in de strijd tegen **illegale visvangst en andere verboden activiteiten op zee**.

Ook op het land en in stedelijke contexten heeft GEOINT tal van toepassingen. Sensoren en beeldanalyse maken **monitoring en herkenning van structuren en materialen** mogelijk. De verzamelde data vormt de basis voor **driedimensionale stadsmodellen** en **digital twins**, die beleidsmakers ondersteunen bij **voorspellingen en simulaties** van nieuwe maatregelen. Met zulke modellen kunnen bijvoorbeeld **energieverbruikspatronen** op stadsniveau worden onderzocht, of de **'materialenvoorraad'** van gebouwen en infrastructuur worden geïnventariseerd in het kader van **de circulaire economie** en **de Europese Critical Raw Materials-agenda**.

Voor zowel militaire als civiele gebruikers blijft de essentie hetzelfde: zij willen **snel en betrouwbaar inzicht** in wat er gebeurt, niet morgen, maar binnen **minuten of zelfs seconden** na een gebeurtenis. De informatie moet efficiënt worden verwerkt, met **minimale belasting van infrastructuur, bandbreedte en rekencapaciteit**. Alleen de relevante data mag worden doorgestuurd, en de systemen moeten **robuust blijven functioneren**, zelfs bij storingen of aanvallen. Die storingen kunnen onschuldig zijn, zoals slecht weer of netwerkbeperkingen, maar ook kwaadaardig, zoals **jamming, spoofing of cyberaanvallen**. Bovendien is het cruciaal dat de verschillende systemen **vlot interopereren en autonoom samenwerken**, zonder dat menselijke tussenkomst telkens nodig is.

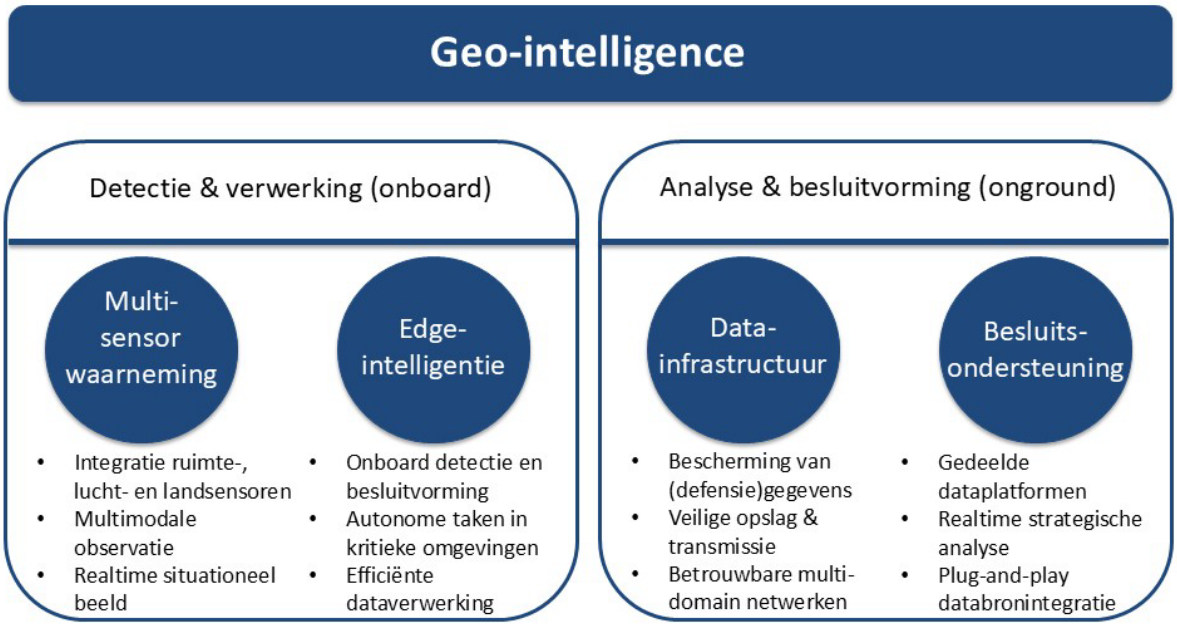
In wezen vormt geo-intelligence de **sensorlaag van geopolitiek**: ze vertaalt enorme hoeveelheden ruwe pixels en signalen in **strategische kennis, diplomatieke hefboomkracht en tactische voorsprong**. Om die rol te behouden in een wereld van **contested space, elektronische verstoring en AI-gedreven camouflage**, is blijvende **investering in technologische vernieuwing** noodzakelijk, met name in **edge-AI, multisensor-integratie en robuuste infrastructuren**.

3.2 Overkoepelende doelstellingen

Tijdens de **geo-intelligence-roadmapoefening** zijn een aantal **cruciale defensienoden en technologische uitdagingen** geïdentificeerd. Ze weerspiegelen de groeiende behoefte van Defensie aan **snellere, betrouwbaardere en beter geïntegreerde informatievoorziening** in een **steeds complexere en meer betwiste operationele omgeving**. De roadmap richt zich op het ontwikkelen van oplossingen die deze noden rechtstreeks ondersteunen en zo bijdragen aan een **sterkere Vlaamse en Europese informatiepositie**.

1. **Persistente waarneming.** Continu zicht op zee, land, lucht en vanuit de ruimte, over dag/nacht en alle weersomstandigheden. Complementaire sensoren en slimme taakplanning verminderen blinde vlekken en verhogen de kans op vroege detectie.
2. **Strategische autonomie/soevereiniteit.** Zeggenschap over kritieke technologie (sensoren, algoritmen), data en infrastructuur. Open interfaces en soevereine cloud/edge-opties maken samenwerken mogelijk zonder afhankelijk te worden.
3. **Real-time inzichten (lage vertraging).** In plaats van achteraf rapporteren, onmiddellijk alarmeren en bijsturen. Dit vraagt verwerking dicht bij de bron (edge), efficiënte datadoorstroom en modellen die geoptimaliseerd zijn voor snelheid én betrouwbaarheid.
4. **Veerkracht in verstoorde omgevingen.** Operaties moeten doorlopen bij cyberaanval, jamming, uitval of congestie. Redundantie, self-healing en failsafe autonomie zorgen dat de keten gecontroleerd degradeert in plaats van te stoppen.
5. **Multidomein-integratie voor beslissingsvoorsprong.** Data uit ruimte, lucht, zee en land samenbrengen in één coherent beeld met zichtbare herkomst en betrouwbaarheid, gekoppeld aan simulatie en besluitvorming, zodat we van “zien” naar **vooruitkijken en handelen** gaan.

3.3 Roadmap



Figuur 1 - Eenvoudige weergave van de roadmap Energie & Veiligheid. De volledige roadmap is als bijlage achteraan terug te vinden.

De roadmap werd opgebouwd op basis van de volgende structuur:

- De **visie en het doel** dat we nastreven ('Mission')
- **Focus**: welke problemen en uitdagingen lossen we op?
- **Bouwstenen**: wat willen we doen binnen het toepassingsgebied? Welke concrete innovatiedoelen/technologische ontwikkelingen willen we bereiken?
- Welke **projecten** (innovatiekansen) zouden er binnen het toepassingsgebied mogelijk zijn (dit is louter ter inspiratie en niet-limitatief)

3.3.1 Focuslaag: Onboard

Pijler 1 en 2 ("Onboard") richten zich primair op de sensorkant van de keten: hoe ruwe observaties uit uiteenlopende bronnen (ruimte, lucht, zee, land) sneller, robuuster en coherenter verwerkt kunnen worden. Waar Pijler 1 focust op multibron-fusie en situationeel overzicht, legt Pijler 2 de nadruk op autonome, realtime verwerking dicht bij de bron, met algoritmen die domeinvariatie en onzekerheid aankunnen.

3.3.1.1 Pijler 1: Multibron-sensing en fusie voor situationeel overzicht

3.3.1.1.1 Scope

Deze pijler richt zich op de **integratie van heterogene sensoren** over verschillende platformen — van satellieten en luchtvaartuigen tot UAV's, maritieme systemen en grondgebonden installaties — en op de ontwikkeling van **geavanceerde datafusie-algoritmen** die daaruit één **real-time, context-rijk en betrouwbaar operationeel beeld** genereren.

De focus ligt op het **combineren van complementaire sensormodaliteiten** (zoals EO, SAR, RF, IR en hyperspectraal) met referentiedata en contextuele informatie, zodat zowel strategische als tactische besluitvorming in alle defensiedomeinen ondersteund wordt.

3.3.1.1.2 Belangrijkste onderzoeks- en ontwikkelingsprioriteiten

- **Integratie van sensoren over platformen heen.** Een eerste prioriteit is de ontwikkeling van **interoperabele sensorarchitecturen** die data uit ruimte-, lucht-, maritieme, UAV- en grondsystemen naadloos samenbrengen. Daarvoor is een sterke focus nodig op de **harmonisatie van sensoruitvoer**, met gestandaardiseerde dataformaten, kalibratieprotocollen en uniforme tijd- en ruimtereferenties. Ook het integreren van **bestaande en opportunistische sensoren** — zoals stertrackers, GNSS-ontvangers en RF-antennes — biedt kansen om de **dekking en betrouwbaarheid** van observaties verder te vergroten.

- **Fusie over verschillende sensortypes (cross-modality fusion)**. Een tweede prioriteit is het ontwikkelen van **geavanceerde AI- en machine-learningtechnieken** die gegevens van uiteenlopende sensoren en platformen kunnen samenvoegen tot één consistent geheel. Hierbij spelen **fysisch geïnformeerde en onzekerheidsbewuste modellen** een sleutelrol: ze houden rekening met sensorkarakteristieken, ruis en betrouwbaarheid, waardoor beslissingen kunnen worden genomen op basis van **meetbare zekerheid**.

- **Realtime en edge-capabele verwerking**. Een derde pijler richt zich op de ontwikkeling van **lichte, energie-efficiënte fusie-algoritmen** met lage latentie, die geschikt zijn voor verwerking **aan boord of aan de rand (edge)**. Hierbij hoort ook de implementatie van **closed-loop-taakplanning**, waarbij sensoren zichzelf autonoom kunnen heroriënteren of herconfigureren op basis van gefuseerde inzichten — een cruciale stap richting **autonome detectie en besluitvorming**.

- **Multidomein- en multibroncoherentie**. Tot slot is er nood aan een **nauwe afstemming tussen sensordata en contextuele of referentie-informatie**, zoals kaarten, bathymetrie, weerdata, AIS-signalen of terreininformatie. Door data uit verschillende domeinen te integreren tot één **coherent en geo-gelokaliseerd operationeel beeld**, ontstaat een betrouwbaar fundament voor samenwerking over **missie-, organisatie- en landsgrenzen** heen.

3.3.1.1.3 Strategische impact

Deze pijler maakt **persistente, betrouwbare en nauwkeurige situationele bewustwording** mogelijk door de **complementaire sterktes van diverse sensoren en platformen** te benutten.

Ze ondersteunt zowel **strategische autonomie** als **operationele voorsprong**, doordat besluitvormers tijdig toegang krijgen tot **contextuele en gevalideerde inlichtingen** — ongeacht de herkomst, het domein of de omstandigheden. Daarmee vormt deze pijler de technologische basis voor **snellere detectie, nauwkeuriger besluitvorming en efficiënter gebruik van middelen** binnen de moderne defensie- en veiligheidsarchitectuur.

3.3.1.2 Pijler 2: Realtime edge intelligentie: algoritmen voor autonome verwerking

3.3.1.2.1 Scope

Deze pijler richt zich op het ontwikkelen van **intelligente platformen** die data **aan de bron** kunnen verwerken en interpreteren. Door **AI-gestuurde detectie, classificatie en besluitvorming** rechtstreeks *onboard* uit te voeren, kunnen systemen sneller en betrouwbaarder reageren, ook in **tactische of tijdelijk ontkoppelde omgevingen**. De focus ligt op **autonome taakuitvoering**, **lage-latentie-verwerking** en **bandbreedte-efficiëntie**, zodat missies kunnen doorgaan, zelfs wanneer communicatie of infrastructuur verstoord is.

3.3.1.2.2 Belangrijkste onderzoeks- en ontwikkelingsuitdagingen

- **AI-architecturen voor beperkte en veeleisende omgevingen**. Ontwikkeling van **compacte, energie-efficiënte en robuuste AI-modellen** die kunnen draaien op ruimte-, lucht- en maritieme platformen met beperkte rekencapaciteit. De nadruk ligt op **modeloptimalisatie, kwantisatie en compressie**, zodat algoritmen performant blijven bij lage latency en beperkte hardware.

- **Autonome detectie, classificatie en besluitvorming**. Het ontwerpen van **zelfredzame AI-modules** die onafhankelijk detecties analyseren, prioriteren en daaruit acties afleiden, bijvoorbeeld automatische her-taakstelling of waarschuwing

bij afwijkingen. Zo evolueren platformen van dataverzamelaars naar **autonome observatie-eenheden** die in realtime waardevolle inlichtingen genereren.

- **Closed-loop taakplanning en adaptieve missiesturing**. Ontwikkeling van **gesloten regelkringen** tussen detectie, analyse en actie, waarbij de sensorplanning dynamisch wordt aangepast op basis van de actuele informatiewaarde. Dit verhoogt de efficiëntie en laat sensoren zelf bepalen waar en wanneer verdere observatie nodig is.

- **Veilige, energie-zuinige en stralingsbestendige hardware**. Ontwerp van **low-power, radiation-hardened rekenhardware** (zoals FPGA's en AI-accelerators) die bestand is tegen extreme omstandigheden en langdurig autonoom kan functioneren. De hardware-laag vormt zo een betrouwbare basis voor edge-AI in kritieke missies.

- **Latentiereductie voor tijdskritische toepassingen**. Verbetering van **end-to-end reactietijd** voor ISR- en crisisresponsscenario's door verwerking dichter bij de sensor te brengen, data-stromen te optimaliseren en communicatie-overhead te minimaliseren.

3.3.1.2.3 Strategische impact

Deze pijler vergroot de **tactische wendbaarheid, reactiekracht en overlevingskansen** van operationele platformen. Door beslissingen lokaal en onmiddellijk te nemen, vermindert de afhankelijkheid van externe infrastructuren en wordt **missiecontinuïteit gegarandeerd**, zelfs in **verstoorde omgevingen**. Realtime edge-AI vormt zo een **krachtvermenigvuldiger** voor de Belgische en Europese defensie, met directe impact op **situational awareness, autonomie en veerkracht** in het veld.

3.3.2 Focuslaag: Onground

Pijler 3 en 4 ("Onground") verplaatsen het zwaartepunt naar de grond: de veilige en soevereine infrastructuur om grote, heterogene geodata betrouwbaar te beheren en distribueren (Pijler 3), en de integratie tot bruikbare besluitvormingsomgevingen en digitale tweelingen (Pijler 4). Samen zorgen deze twee lagen ervoor dat de rijkere sensorgegevens daadwerkelijk doorstromen naar operators, analisten en besluitvormers in een reproduceerbare en interoperabele workflow.

3.3.2.1 Pijler 3: Veilige, veerkrachtige en soevereine geo-datainfrastructuur (beheer & verwerking)

3.3.2.1.1 Scope

Deze pijler richt zich op het uitbouwen van een **robuuste, soevereine en cyberweerbare geodata-infrastructuur** die het volledige traject ondersteunt van **dataverzameling tot verspreiding van inlichtingen**. Het gaat om de veilige verwerking van **ruimtelijke en sensorgebaseerde data** — afkomstig van satellieten, drones, schepen, grondstations en externe partners — en om het garanderen van **integriteit, beschikbaarheid en vertrouwelijkheid** binnen **gefedereerde, multidomein- en internationale omgevingen**. Zo vormt deze pijler de **digitale ruggengraat van geo-intelligence**, waarin geografische

informatie veilig kan worden gedeeld, gecombineerd en benut voor defensie-, veiligheids- en crisisresponsdoeleinden.

3.3.2.1.2 Belangrijkste onderzoeks- en ontwikkelingsprioriteiten

- **Gefedereerde en modulaire geodata-architecturen met lokale autonomie**. Ontwikkeling van **schaalbare, modulaire infrastructuren** die grote hoeveelheden geodata kunnen beheren, verwerken en delen over meerdere locaties en partners. Deze infrastructuren ondersteunen **gedistribueerde operaties**, met lokale verwerkingscapaciteit zodat gegevens ook beschikbaar blijven bij netwerkuitval of beperkte connectiviteit. Ze moeten toelaten om **nationale en bondgenootschappelijke geodatabronnen te federeren**, op basis van **beleidsgestuurde toegangscontrole** en **veiligheidsniveaus per datacategorie**.

- **Cyberweerbaarheid en continuïteit van geo-informatiesystemen**. Bescherming tegen **cyberaanvallen, datacorruptie en systeemdegradatie** is cruciaal om operationele kaartlagen en sensorgegevens betrouwbaar te houden. Daarom wordt ingezet op **redundante, zelfherstellende en veerkrachtige infrastructuren** die cruciale geodata blijven leveren, zelfs bij fysieke schade of verstoring van communicatielijnen. De nadruk ligt op **mission continuity**, altijd toegang tot de noodzakelijke geo-informatie, ongeacht de omstandigheden.

- **Datasoevereiniteit en governance voor geodata** Versterking van **nationale zeggenschap over strategische geodata-assets**, inclusief inlichtingen- en referentielagen. Dit omvat **transparante datalinages** (herkomst en bewerking van geografische datasets), **audittrailmechanismen**, en naleving van **defensie- en privacyrichtlijnen**. Daarnaast worden **gestandaardiseerde geotaxonomieën en vocabularia** ontwikkeld om gegevensuitwisseling tussen nationale, Europese en NAVO-partners te vereenvoudigen zonder soevereiniteit op te geven.

- **Hoogperformante geopijplijnen en datafluxen**. Ontwikkeling van **real-time verwerkingspijplijnen** voor de enorme datastromen uit EO-, SAR-, hyperspectrale en andere sensoren. Deze pijplijnen ondersteunen **streaming analytics**, **lage-latentie-disseminatie** en koppeling aan **geografische beslissingssystemen**. Zo kunnen operationele gebruikers op elk moment beschikken over **actuele, geolokaliseerde en betrouwbare informatie** — essentieel voor situational awareness en crisisrespons.

3.3.2.1.3 Strategische impact

Deze pijler waarborgt dat de **geo-informatiesystemen van Defensie** veilig, veerkrachtig en **soeverein** blijven onder alle omstandigheden. Ze vormt de **basis voor betrouwbare, schaalbare en missie-kritieke geodata-operaties** over verschillende domeinen en partners heen.

Door **datasoevereiniteit te koppelen aan cyberweerbaarheid** versterkt Vlaanderen en België hun rol als betrouwbare bron en beheerder van **strategische geografische informatie**. Dit is cruciaal voor de **informatieovermacht, weerbaarheid en autonomie** van de defensie- en veiligheidsinfrastructuur in Europa.

3.3.2.2 Pijler 4: Integratie voor besluitvorming en digitale tweelingen

3.3.2.2.1 Scope

Deze pijler richt zich op de ontwikkeling van een **gedeeld, uitbreidbaar en soeverein grondplatform** dat **multisource-geodata en inlichtingenstromen** integreert tot één samenhangend beeld. Het platform ondersteunt zowel **realtime operationele besluitvorming** als **strategische planning**, en biedt **rolspecifieke interfaces, visualisaties en analysetools** voor uiteenlopende gebruikers — van operatoren tot beleidsmakers. Een modulaire en open architectuur maakt het mogelijk om **nieuwe databronnen, sensoren en AI/ML-analyses** eenvoudig te integreren, zodat het systeem mee evolueert met veranderende missievereisten.

3.3.2.2.2 Belangrijkste onderzoeks- en ontwikkelingsprioriteiten

- **Geïntegreerde inlichtingen- en geodatafusie**. Ontwikkeling van methoden voor het **aggregeren, harmoniseren en koppelen van data** uit uiteenlopende bronnen: sensoren, databanken, externe partners en open data. Het platform moet zowel **gestructureerde als ongestructureerde informatie** ondersteunen, met **ruimtelijke en temporele afstemming** als kernprincipe. Zo ontstaat één **uniform en actueel situational picture** dat bruikbaar is in alle domeinen.

- **Rolgebaseerde besluitvormingsondersteuning**. Uitbouw van **dashboards, waarschuwingen en visualisaties** die zijn afgestemd op de specifieke noden van gebruikers, van operationele eenheden tot strategische leiding. Het systeem ondersteunt **plug-and-play-integratie van AI/ML-analyses** en **beslissingsondersteunende modules**, zoals **predictieve analyses** en **what-if-simulaties** die helpen om alternatieve scenario's te verkennen vóór actie wordt ondernomen.

- **Digitale tweelingen en simulatieomgevingen**. Ontwikkeling van **realtime digitale tweelingen** van operationele en geografische omgevingen, die gebruikt kunnen worden voor **planning, training en besluitvorming**. Door **live data te koppelen aan simulatiemodellen**, kunnen beslissingen worden getoetst aan actuele omstandigheden en automatisch worden bijgestuurd wanneer de situatie verandert. Deze koppeling versterkt het adaptief vermogen van commandovoering en crisisrespons.

- **Interoperabiliteit en uitbreidbaarheid**. Ontwerp van een **open, modulaire architectuur** op basis van **gestandaardiseerde interfaces (API's)** en **open standaarden**, zodat integratie met **bestaande, NAVO- en bondgenootsystemen** mogelijk blijft. De architectuur moet voldoende flexibel zijn om **nieuwe missiedomeinen, datatypen en analysemethoden** te ondersteunen zonder herontwerp van de kerninfrastructuur.

3.3.2.2.3 Strategische impact

Deze pijler versterkt de **informatiepositie en slagkracht** van Defensie door besluitvormers te voorzien van een **coherent, realtime operationeel beeld** en **geavanceerde plannings- en analysetools**. Ze maakt **snellere en beter onderbouwde beslissingen** mogelijk, verhoogt de **voorspellende capaciteit** en bevordert **samenwerking en interoperabiliteit**

over missies, domeinen en partners heen. Daarmee vormt dit geïntegreerde platform een **cruciale schakel tussen waarneming en actie**, en tilt het de geo-intelligenceketen naar een niveau van **anticiperende besluitvorming** en **strategische wendbaarheid**.

3.3.2.3 Samenhang tussen pijlers (ketenwaarde)

In samenhang creëren de vier pijlers een **sluitende geo-intelligenceketen**:

1. **Waarnemen** – sensoren registreren de wereld in hoge resolutie, dag en nacht, onder alle omstandigheden.
2. **Verwerken** – edge-AI zet ruwe data om in eerste inzichten, met minimale vertraging.
3. **Versterken en beveiligen** – robuuste infrastructuren bewaren, verrijken en beschermen geodata over meerdere domeinen en partners.
4. **Beslissen en handelen** – geïntegreerde platformen ondersteunen besluitvorming, simulatie en actie in realtime.

Elke pijler kan autonoom functioneren, maar hun ware kracht ligt in de **interactie**: data die veilig doorstroomt van sensor tot besluit, algoritmen die leren uit feedback, en infrastructuren die standhouden onder druk.

3.4 Mogelijke synergieen

Geo-Intelligence Roadmap Synergieën	
Maritiem	Detectie, identificatie, sensorfusie en AI, dataintegratie, intelligente sharing, situational awareness
Space	Space-gebaseerde aardobservatie, Space situational awareness
AI	Sensorfusie, edge compute, data and ICT infrastructuur
Cyber	Security and resilience built-in for software- and hardware-based defense technology
Autonomie	Veerkrachtige, autonome missies met hybride vloten van drones/UXV's
Luchtvaart en Drones	Sensoriek en sensorfusie
Biotechnologie	Sensors en monitoring
cUAS	AI detectie, multi-sensor integratie, visuele en elektro-optische identificatie, RF-signatuurherkenning en gedragspatronen , autonome tracking
Omgeving	Environmental monitoring
Energie	AI en sensornetwerken, autonome energieopwekking

4 CONCLUSIE

De **Europese Unie** en de **NAVO** maken van geo-intelligence een strategische prioriteit, met nadruk op **24/7 multisource-waarneming**, **beslissingsvoorsprong**, **interoperabiliteit** en **weerbaarheid** in een omstreden ruimte- en cyberdomein. Via programma's zoals **EDF**, **EDIS**, **DIANA** en het **NATO Innovation Fund** worden middelen vrijgemaakt om **dual-use innovaties** versneld te vertalen van demonstratie (TRL 5–7) naar operationele inzet (TRL 8–9).

Binnen dit kader positioneert het **Vlaams impulsprogramma voor defensie** zich als een **strategische hefboom** om Vlaamse kennis, industrie en infrastructuur te mobiliseren. Vlaanderen beschikt over sterke troeven langs de hele geo-intelligenceketen: van **aardobservatie, datafusie en edge-AI** tot **geodata-infrastructuren en digitale besluitvorming**.

De regio telt **138 actieve bedrijven**, waarvan **66** reeds deelnemen aan Europese of NAVO-programma's — ondersteund door **living labs** (haven, kust, stedelijk, industrie) die snelle validatie en opschaling mogelijk maken.

De roadmap toont waar Vlaanderen het verschil kan maken:

- **multisensorwaarneming en edge-verwerking** voor persistente situational awareness,
- **soevereine en cyberveilige geodata-infrastructuren** die aansluiten op Europese standaarden,
- en **interoperabele besluitvormingsplatformen en digitale tweelingen** voor gezamenlijke operaties.

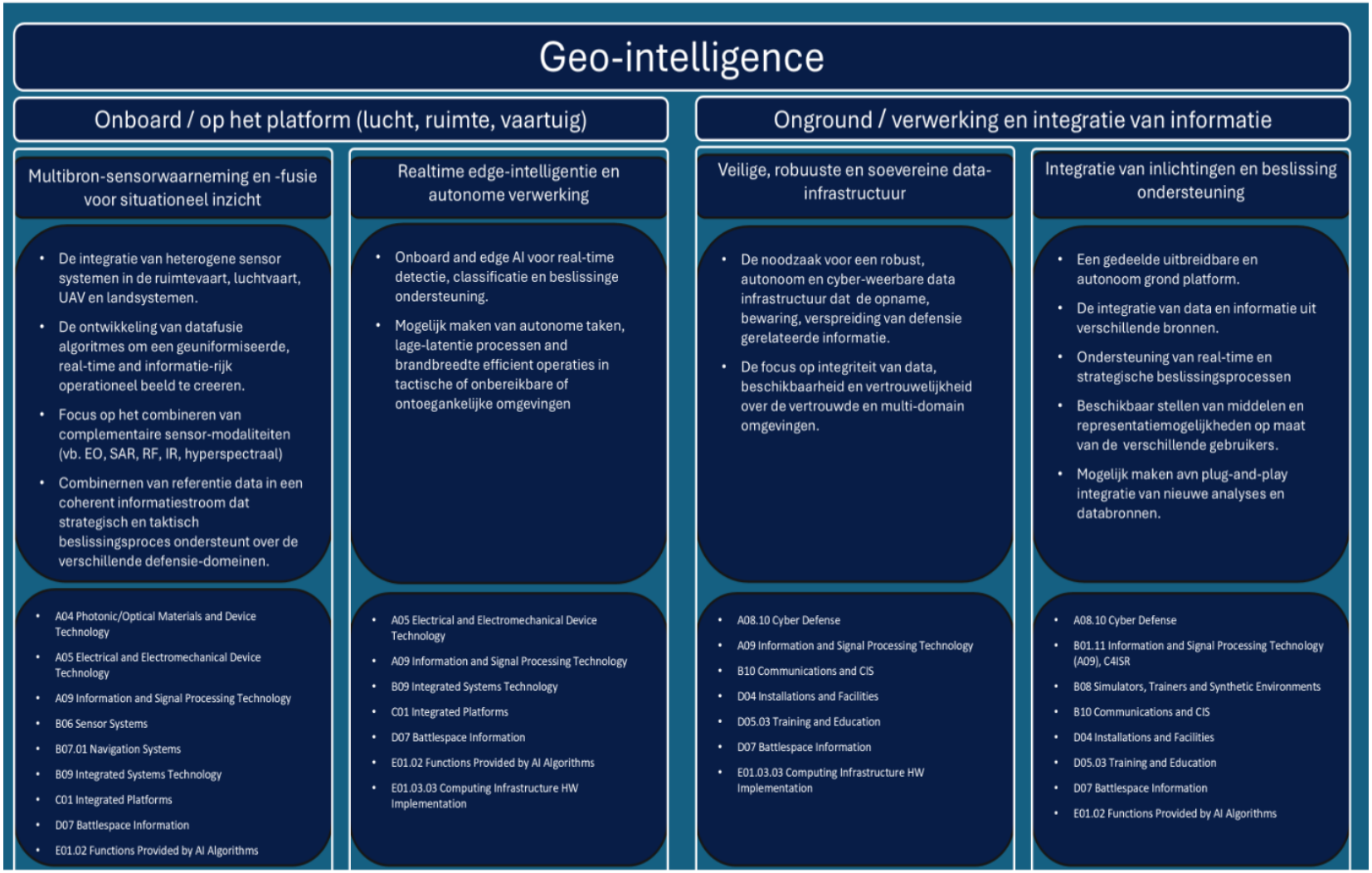
Het momentum is gunstig: EU en NAVO creëren de middelen en markten, terwijl Vlaanderen via zijn impulsprogramma de **brug kan slaan tussen onderzoek, industrie en defensie**. Door **triple-helixsamenwerking** rond concrete use-cases en **gerichte investeringen** in validatie en standaardisatie kan Vlaanderen zijn technologische voorsprong omzetten in **operationele meerwaarde, economische groei** en een **vaste positie in de Europese geo-intelligence-keten**.

5 LITERATUURLIJST

1. Actualisering van het STAR-plan voor Defensie: Strategische Visie 2025. (2025, July 18). News.Belgium. https://news.belgium.be/nl/actualisering-van-het-star-plan-voor-defensie-strategische-visie-2025
2. Vlaams defensieplan. (n.d.). Vlaanderen.be. https://www.vlaanderen.be/vlaamse-regering/beslissingen-van-de-vlaamse-regering/vlaams-defensieplan
3. EU Space Strategy for Security and Defence. (n.d.). Defence Industry and Space. https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en
4. IRIS2. (n.d.). EU Agency for the Space Programme. https://www.euspa.europa.eu/eu-space-programme/secure-satcom/iris2
5. https://defence-industry.eu/the-2023-eu-capability-development-priorities/
6. The European Defence Industrial Strategy. (n.d.). Innovation for Place-based Transformation. https://place-based-innovation.ec.europa.eu/publications/european-defence-industrial-strategy_en
7. Readiness Roadmap 2030. (n.d.). Defence Industry and Space. https://defence-industry-space.ec.europa.eu/eu-defence-industry/readiness-roadmap-2030_en
8. Nato. (n.d.). NATO's overarching space policy. NATO. https://www.nato.int/cps/en/natohq/official_texts_190862.htm
9. CIPR -. (n.d.). https://ec.europa.eu/newsroom/cipr/items/713800/en
10. UK Ministry of Defence. (2023). Joint Doctrine Note 1/23 Intelligence, Surveillance and reconnaissance. https://assets.publishing.service.gov.uk/media/641c27e15155a200136ad4df/JDN_1_23_ISR_web.pdf

6 BIJLAGES

6.1 Roadmap



vision on technology
for a better world

vito

Biotechnology for defense

Orientation roadmap for Flanders

October 2025

VIB vzw
Suzanne Tassierstraat 1 – 9052 Ghent – Belgium
info@vib.be
www.vib.be

Contents

Introduction

In an era marked by geopolitical instability, climate change, pandemics, and hybrid warfare, biotechnology has emerged as a critical enabler of resilience and security. From countering Chemical, Biological, Radiological, and Nuclear (CBRN) threats to ensuring the availability of life-saving medicines and enhancing soldier health, biotech is reshaping defense capabilities. As NATO and the European Union (EU) adapt to these evolving challenges, Flanders is positioning itself as a hub for innovation and industrial leadership in defense-related biotechnology and is strategically located in the heart of Europe.

Vision: Biotechnology as a Strategic Enabler

Biotechnology offers transformative potential across multiple defense domains. It enables rapid detection and neutralization of CBRN agents, supports the decentralized production of critical therapeutics and enhances human performance and recovery on or off the battlefield. The convergence of biotech with digital technologies, such as AI and synthetic biology, is accelerating innovation and creating dual-use solutions that benefit both military and civilian sectors.
The EU and NATO have recognized the strategic importance of biotechnology [1][2]. The European Defense Agency (EDA) CapTech CBRN and Human Factors initiative, for example, supports collaborative research to close capability gaps in CBRN defense and human performance enhancement [3]. Similarly, the EU's CBRN Centres of Excellence (CoE) initiative fosters international cooperation to mitigate CBRN risks and promote a global culture of safety [4].

1. Defense Against CBRN and Other Battlefield Hazards

CBRN threats remain a top priority for European and NATO defense planning. The proliferation of dual-use technologies, the risk of state and non-state actors deploying biological agents, and the increasing complexity of hybrid warfare demand robust countermeasures.
The EU's CBRN CoE initiative created 15 years ago, active in over 60 countries across 8 regions, exemplifies a comprehensive approach to risk mitigation through training, governance, and international collaboration [4][5]. The EDA's CapTech CBRN & Human Factors program focuses on technologies such as detection and identification systems, personal protective equipment, and medical countermeasures [3].
Belgium contributes to NATO's CBRN Centre of Excellence and hosts several biotech firms and research institutions specializing in biopharma, healthcare, biosurveillance, diagnostics and decontamination. The country's strategic location, scientific expertise and range of pilot facilities make it a key player in European CBRN preparedness.
Pandemic preparedness and anti-microbial resistance (AMR) strategies are of particular interest in the context of CBRN. Whether to address highly resistant infections after battlefield trauma or to combat biological warfare, solutions need to be developed in peace time, for use in crisis. The question is not if but when another crisis of the scale of the COVID-19 pandemic will hit us. AMR is **rapidly rising** as a cause of death, and the immunosuppression associated with high-stress conditions – such as battlefield trauma- is a known predisposing factor for infections caused by ESKAPE pathogens. These include *Enterococcus faecium*, *Staphylococcus aureus*, *Klebsiella pneumoniae*, *Acinetobacter baumannii*, *Pseudomonas aeruginosa* & *Enterobacter* species.[6][7].

2. Biomanufacturing of Critical Medicines, Materials, and Food

In a world increasingly vulnerable to supply chain disruptions, rising geopolitical tensions and environmental degradation, the **ability to produce essential goods such as medicines, materials, and food** —through biotechnology has become essential to ensure national resilience. The COVID-19 pandemic highlighted the importance of having domestic capabilities for producing vaccines and therapeutics. **Biomanufacturing platforms** such as mRNA synthesis, cell-based production, and modular bioreactors enable rapid, localized responses to health emergencies. Belgium has world-class expertise and infrastructure in pharma-logistics (e.g. at Zaventem) and in (bio-)manufacturing of (bio-)pharmaceuticals, which both are critical during crisis response.

The availability of pilot biomanufacturing facilities is a key enabler of innovation in this domain and provides also **an 'emergency' capacity** that can be called upon by the military in times of crises. These infrastructures bridge the gap between laboratory research and industrial-scale production, allowing for process optimization, regulatory validation, and rapid scale-up. The EU's Biomanufacturing Industrial Alliance [8] and initiatives under HERA (Health Emergency Preparedness and Response Authority) [9] emphasize the need for such infrastructure to ensure strategic autonomy.

Through **synthetic biology and precision fermentation**, biotech enables sustainable production of high-performance materials, including bioplastics, bio-based textiles, and advanced composites. These materials are critical for defense applications such as lightweight armor, protective gear, and stealth coatings.

In conflict zones or disrupted environments, conventional food supply chains may collapse. Biotechnology approaches such as precision fermentation, cellular agriculture, and algae-based systems could **provide nutrient-dense, shelf-stable food** for both deployed military personnel and civilian populations.

Belgium is home to several pilot-scale and industrial biomanufacturing hubs, including the Walloon BioPark, BioTech Lane Ghent and the other Flanders' biotech clusters. These sites support not only biopharmaceutical production but also research into bio-based materials and food systems. The country has seen significant investments in clinical manufacturing of advanced therapy medicinal products (ATMPs), making it a key player in the European landscape. Belgium's integration of academic, industrial, and defense stakeholders positions it as a European leader in resilient biomanufacturing.

3. Advanced Health Technologies

Modern warfare places immense physical and psychological demands on personnel. Advanced **health technologies**—including wearable/implantable biosensors, regenerative medicine, neurotechnology, predictive modeling for personalized treatment/diagnostics/training and mission assignment, and autonomous/AI-enabled technologies that support telemedicine/remote robotic surgery, trauma triage, assisted medevac and care—are vital for maintaining operational readiness and long-term health.

The EDA's Human Factors Strategic Research Agenda highlights the importance of human performance monitoring, customized training, and integration of wearable technologies [3]. These innovations not only enhance soldier resilience but also contribute to broader health system modernization.

Belgian universities and startups are at the forefront of developing wearable health monitors, AI-driven diagnostics, and rehabilitation technologies. The country's integration of academic research with defense needs could support EDA's research agenda and NATO's goal of enhancing human capability through innovation.

Challenges and Gaps of Biotech for Defense

Although Belgium has a solid scientific foundation and significant industrial assets, Flanders stands out as a dynamic hub of biotech excellence, with globally recognized research institutions, innovative companies, and a strong entrepreneurial spirit. To fully harness biotechnology for defense and security, Flanders, and Belgium more broadly, faces strategic challenges that also present unique opportunities for growth, collaboration, and leadership within NATO and the EU.

1. Strengthen coordination across a rich innovation ecosystem

Flanders hosts a vibrant biotech ecosystem, complemented by strong clusters in Wallonia and Brussels. However, the full potential of these regional strengths is not yet fully realized due to limited interregional coordination. By fostering stronger collaboration across regions, Belgium can build integrated innovation pipelines that serve both civilian and defense needs, unlocking synergies and accelerating dual-use innovation. Flanders, with their proactive innovation culture, are well-positioned to lead such efforts.

2. Defense-Oriented R&D Funding

While Flanders has historically invested modestly in defense-related R&D compared to its peers, recent developments signal a promising shift. The region's strong foundation in civilian biotech offers a unique opportunity to extend innovation into dual-use and defense-specific applications. Encouragingly, new government investments in defense are beginning to open up fresh avenues for collaboration, technology translation, and capability development. To fully realize this potential, it is essential to align these new funding streams with targeted mechanisms—such as defense innovation grants, challenge-based procurement, and public-private partnerships. These instruments can catalyze the translation of academic and industrial biotech research into deployable solutions for NATO and EU missions. Additionally, tailored incentives should be developed to address concerns about publication and risk mitigation strategies with regards to contamination or confidentiality.

3. Scaling up Pilot-Scale Infrastructure and embracing digitalization

Flanders benefit from advanced biotech incubators and industrial facilities, but there is a shortage of pilot-scale biomanufacturing infrastructure specifically designed for defense-relevant applications. Investing in modular, digitalized, multi-use pilot facilities—potentially co-funded by EU or NATO innovation programs would enhance crisis response capabilities and support allied operations. Flanders' strong digital innovation ecosystem offers a solid foundation to lead in this area, especially in domains like biologics, bio-based materials, and food resilience.

4. *Regulatory and Security Constraints*

Biotech innovation for defense frequently deals with sensitive data, dual-use technologies, and complex ethical considerations. Although Belgium's regulatory framework is strong for civilian use, defense applications require more agile and secure protocols. Developing a specialized regulatory track for defense biotech—aligned with EU and NATO standards— would streamline approvals while ensuring safety and compliance. Flanders' experience in navigating complex regulatory landscapes can be an asset in shaping this evolution.

5. Talent Pipeline and Skills

Flanders' universities and research centers produce world-class biotech talent. To meet the interdisciplinary skills needed for defense innovation (e.g., bioinformatics, biodefense, systems engineering), new dedicated training programs, internships, and fellowships in defense biotech should be developed—possibly in collaboration with NATO's Defense Innovation Accelerator for the North Atlantic (DIANA). These initiatives could make biotech in defense a more attractive and impactful career path for young scientists, positioning Flanders as a leader in cultivating mission-driven talent.

Stakeholder mapping: Flemish strengths in Biotech

Given the major needs and developments in defense biotech, VIB has conducted a stakeholder mapping at the national level in Belgium, which were then used to identify the Flemish strengths and areas for future development for defense. The result includes information and data compiled and curated from public information and private databases (including Pitchbook Financial Database).

In total, 700+ companies and organizations in Belgium were identified within the broader biotech definition, excluding public academic research institutes. Among these, 134 companies and organizations have business activities that are highly relevant for the Impulse Program. Flanders stands out at a national level for its high concentration of Biotech, Medtech, pharmaceutical companies and organizations with direct relevance to the defense sector, as 79 (59.0%) of these are based in Flanders, 44 (32.8%) are based in Wallonia and 9 (6.7%) are based in Brussels region [Figure 1]. From the list of companies and organizations based in Flanders, we identified six broader technological categories that are highly relevant for the impulse program, which are:

1. **Diagnostics** (11 entities): these include companies developing diagnostic equipment & tools (including IVD), and those providing diagnostic services
2. **Facilities** (10 entities): incubators, pilot plants, biomanufacturing sites and service providers (including CDMO), and packaging facilities for biotech products
3. **Medtech** (27 entities): monitoring equipment, medical supplies, surgical devices, therapeutic devices and materials (e.g. for drug delivery, wound dressing), and other Medtech devices and supplies (e.g. exoskeleton, healthcare delivery, brain-machine interface, organ preservation, rehabilitation, prosthetics)
4. **Other equipment and devices** (7 entities): these include R&D equipment/kits/products, manufacturing equipment for therapeutic and Medtech products, decontamination equipment/method, and water/food/air monitoring and/or decontamination systems
5. **Planetary and industrial biotechnology** (9 entities): biotech and agtech companies that develop/produce products other than human drugs (e.g. ag-food, nutraceutical, veterinary care (non-therapeutic) products, environmental (cleantech), and biomaterials
6. **Therapeutics** (14 entities): pharma, biotech, and API/excipient/formulation/platform tool companies that produce/develop vaccines, monoclonal antibodies, nanobodies, drugs and drug substances for human or veterinary use

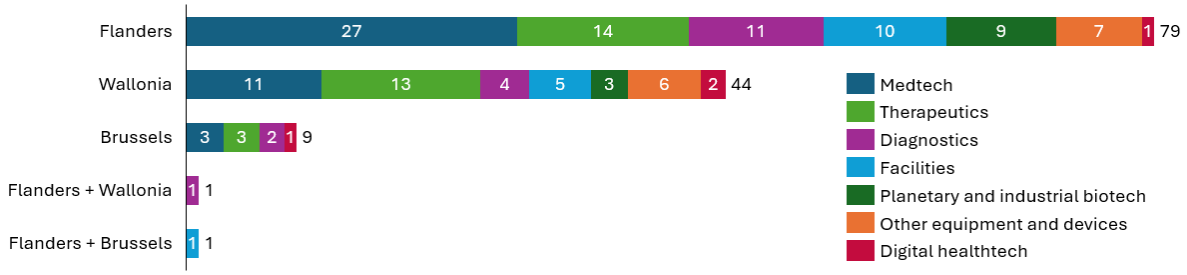


Figure 1. Regional distribution and technological categories of the mapped Belgium companies and organizations relevant for the Biotech EDT for the Impulse Program.

Observations:

- Flanders demonstrates particular strength in Biotech with 79 entities identified. The top three technological subcategories in terms of number of entities are Medtech (27), Therapeutics (14), and Diagnostics (11

Digital Healthtech companies and organizations that are relevant for biotech in defense is under-represented in Flanders

- In Flanders, Gent has a relatively larger share of Impulse Program-related biotech entities (here defined as having >15% of all Flemish entities) with a particular strength in the following technological subcategories: Planetary and industrial biotechnology (55.6%; 5/9 of all Flemish entities), Facilities (36.4%; 4/11 of all Flemish entities), Diagnostics (25%; 3/12 of all Flemish entities), and Medtech (18.5%; 5/27 of all Flemish entities).
- Antwerp has a relatively large share of entities in Other equipment and devices (28.6%; 2/7 of all Flemish entities) and Diagnostics (16.7%; 2/12 of all Flemish entities).
- Leuven's entity make-up per Impulse Program-related technological category is more balanced, but Therapeutics stands out (21.4%; 3/14 all Flemish entities). Leuven also hosts the only one Impulse Program-relevant Digital healthtech company in Flanders.
- There are also four pharmaceutical companies located near Zaventem international airport (Zaventem, Machelen, and Vilvoorde), all of which are multinational companies: Roche diagnostics, Abbott, Pfizer, and Novartis, with Pfizer and Novartis also maintaining sites in Puurs.
- SMEs (classified based on company employee <250) account for 93/134 (69.4%) identified companies in Belgium, and the share is the highest in Flanders: 62/79 (78.4%) [Figure 2]. Since biotech startups and SMEs are key drivers for high-risk technological development, their agility enables them to compete for and propose innovative projects within the Impulse Program.

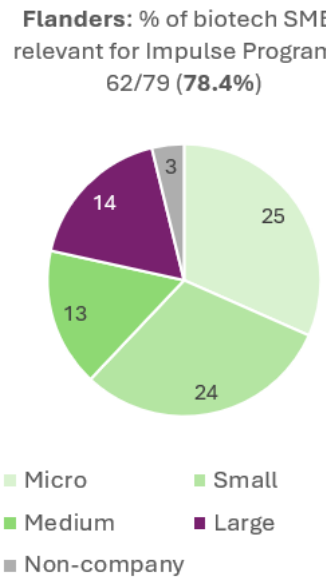


Figure 2. Composition of company sizes in Flanders, for companies relevant for Biotech EDT for the Impulse Program. Company sizes are based on the EC Directive (EU 2023/2775 of 17 October 2023) [10] and VLAIO [11], but excluding criteria on balance sheet and annual turnover.

Roadmaps for Biotechnology

The roadmap is the result of combining the above mapping of the Belgian Biotech ecosystem relevant for defense and the analysis of defense needs (conducted through desk research and interviews with key Defense stakeholders).
It is structured around three strategic priorities/domains:

- **Defense against CBRN** and other battlefield hazards
- **Biomanufacturing**
- **Advanced military health** and **technologies**

each with associated building blocks.
The first domain, Defense against CBRN threats and other battlefield hazards, is subdivided into: (1) **detection, identification, and monitoring (DIM)** of CBRN threats; (2) CBRN **modeling and simulation**; (3) **medical countermeasures** (MCM) for CBRN and battlefield hazards, and a fourth building block related to **protection of food and water supply** from CBRN threats, as also outlined in the roadmap of Environment and Geo-intelligence. Within the domain of CBRN threats, the Biotech roadmap will primarily focus on biological threats.
The second domain, Biomanufacturing includes: **Biomanufacturing of medicines**, and **advanced materials and food**.
The third domain, Advanced military health and technologies, comprises: **Data driven health & readiness optimization**, **advanced medical response**, and **human performance enhancement** technologies.

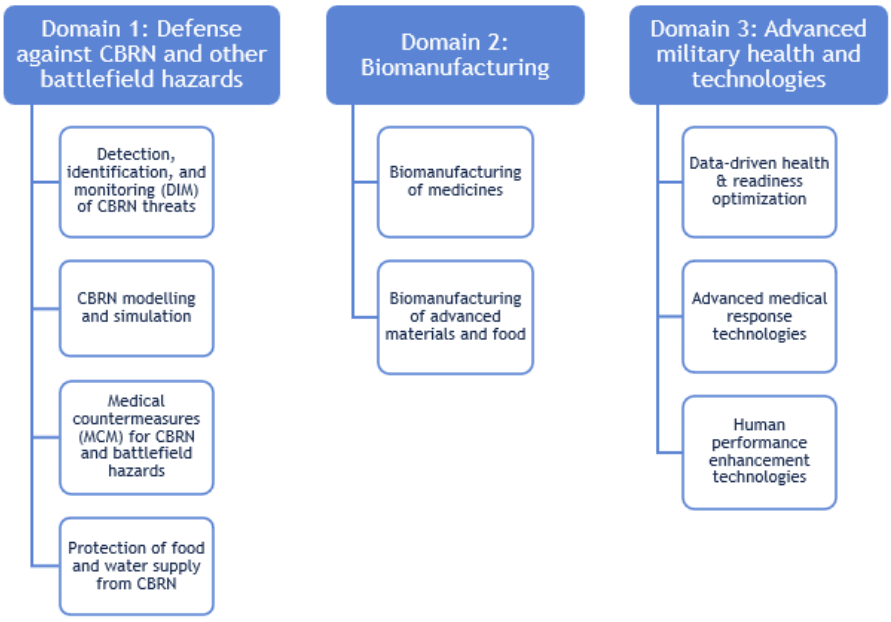


Figure 3. Breakdown of the domains included in the Biotech roadmap

The roadmap encourages industry and academia to develop deployable technologies within 5–10 years, with a focus on delivering mid-to-high TRL solutions that can be integrated into EU and NATO defense systems.

Domain 1: Defense against CBRN and other battlefield hazards

CBRN threats present complex challenges that demand urgent and strategic responses. They can result in mass casualties and long-term health consequences and impact military operations.
These threats may arise from deliberate actions such as terrorism or warfare, industrial accidents, or natural occurring outbreaks, and they carry severe consequences for public health, national security, and the environment. This domain encompasses two pillars and three interconnected building blocks for the first pillar, each addressing a critical aspect of protection against CBRN. The first three focus on core capabilities the **detection**, **identification** and continuous **monitoring** (DIM) of hazardous agents. The use of **modeling** and **simulation** to anticipate threat scenarios, track contamination spread and refine response strategies. The development and deployment of **medical countermeasures** such as vaccines, therapeutics, and antidotes are needed to reinforce operational readiness and enable a rapid response. The second pillar highlights the unique vulnerabilities of **food and water systems**, emphasizing the need for tailored protective measures to safeguard these essential resources against contamination and disruption.

Pillar 1: CBRN situational awareness and countermeasure ecosystem

CBRN situational awareness and countermeasure ecosystem

What	**Detection, Identification, and Monitoring (DIM) of CBRN threats** enables early discovery, confirmation, and ongoing surveillance. As the first line of defense, it supports fast situational awareness and decision-making for pathogens, biological toxins, and hazardous substances—whether used in conflict, terrorism, or arising naturally. This includes air monitoring systems	**CBRN modelling and simulation** supports analysis of threat dispersion, impact, and evolution. It includes plume modelling, exposure estimates, and predictive tools for strategic and operational planning	**Medical countermeasures (MCM) for CBRN and battlefield hazards** include drugs, vaccines, devices to prevent, mitigate or treat the effects of CBRN exposure, AMR ,as well as conventional battlefield injuries, encompassing, prophylactic agents (vaccines and prophylactic drugs), post-exposure agents(antivirals, antibiotics, antidotes, cytokine therapy)
Why	• To initiate targeted health interventions such as quarantine, vaccination, prophylaxis • Tu guide military operations such as mission oriented protective measures (MOPP) level changes • To support forensic attribution, treaty enforcement and post-incident recovery • Trigger timely decontamination protocols for both equipment and personnel, helping limit further exposure, environmental spread, and enabling the safe continuation of mission-critical activities.	• To anticipate and limit human exposure • To test the effectiveness of protective measures. • To support tactical planning and resource allocation • To simulate CBRN release scenarios for training and preparedness	• To preserve operational effectiveness of military personnel in contaminated areas • To limit spread through early treatment and prophylactics • To fill critical treatment gaps especially for category A agents • To counter emerging synthetic and bioengineered treats **Focused on:** Category A: High priority (Anthrax, botulism, plague, smallpox, tularemia, Filoviruses, Arenaviruses), etc. Category B: Moderately easy to disseminate (Brucellosis, Epsilon toxin of C. perfringens, Q-fever, Ricin toxin, food safety threats, etc. Category C: Emerging threats such as Nipah and hantavirus
How	**Existing capabilities:** Detection: Fieldable biosensors, environmental surveillance for water/soil/air testing and POC detection kits using antigen or nucleic acid methods, bioaerosol detectors, and radiation detection systems Identification: Lateral Flow Assay, PCR/qPCR, next generation sequencing, ELISA and western blot, high through-put labs, biosensors Monitoring: Fixed air monitoring stations, radiation monitors, real-time aerosol monitors, zoonotic and wastewater surveillance **Emerging tools/needs:** Multiplexed biosensors, Lab-on-a chip microfluids, CRISPR-based detection, synthetic biology-based biosensors, nanotechnology-enhanced assays, AI driven outbreak predictive tools, wearable pathogen sensors	**Existing tools:** Epicast, FluSurge, GLEAM for spread of infectious diseases, pandemic modelling platforms to integrate into response system (ATP-45, GIS based tools, CBRN information management, simulation **Emerging tools/needs:** AI and machine learning integration, sensor driven modelling systems	**Existing** prophylaxis, therapeutics and supportive care • Vaccines: Anthrax, smallpox, Ebola • Broad spectrum antimicrobials and antivirals: plague, anthrax, tularemia, etc. • Monoclonal antibodies: Ebola, anthrax • Antitoxins: Botulinum • Phage therapy: Personalized therapies against certain bacteria (*Staphylococcus aureus*, *Pseudomonas*,...) • Advanced delivery systems for battlefield use **Emerging** tools/needs: mRNA vaccines, next-generation biologics, toxin neutralizers, platform technologies (viral vectors), broad spectrum antivirals ->Use of **synthetic biology** and **AI** to target drug delivery and combat infectious disease threats and AMR and should comply with the EU- and Belgian biosafety and biosecurity regulations

VIB vzw
Suzanne Tassierstraat 1 – 9052 Ghent – Belgium
info@vib.be
www.vib.be

Building Block 1: Detection, Identification, and monitoring (DIM of CBRN threats)

In modern defense strategy, rapid **Detection**, precise **Identification** and sustained **Monitoring**- collectively known as **DIM**- form the backbone of an effective CBRN protection framework. These capabilities enable early warning, informed decision-making and coordinated response under high-stress, high-risk conditions. While current systems offer foundational tools for threat awareness, they are largely reactive, fragmented and ill-equipped for the complexity and speed of modern and emerging hazards. A transformational shift is needed to embrace technologies that provide **real-time intelligence, predictive analysis** and **global interoperability**. At present, detection is primarily conducted through fixed ground sensors, portable manual instruments, and basic field kits. These tools often lack integration with digital command infrastructures and show diminished effectiveness in remote or hostile environments. Identification typically relies on time-consuming lab-based techniques, with rapid tests offering only moderate accuracy and a limited scope. Many operations still depend on transporting physical samples to specialized laboratories, creating delays and reducing operational agility. Monitoring, meanwhile, remains static and periodic—centered around environmental scanning and event-specific surveillance—with minimal predictive capabilities and inefficient data sharing among agencies. Flanders already has particular strengths in this field. Biocartis' Idylla™, a point-of-care, highly adaptable and connected device was developed and proven fully fieldable, even in BSL-3 level outbreaks (in mobile labs). In addition, miDiagnostics, a spin-off from Imec, has developed ultra-fast, silicon based diagnostic technology that enables decentralized, high-throughput testing at the point of care.

Future needs demand an ecosystem of intelligent, mobile, and adaptive DIM systems such as rapid point-of-care diagnostic capabilities that can identify pathogens and resistance profiles (AMR) directly in the field to enable targeted antibiotic therapy.

This building block focuses on the biological aspects of CBRN threats, whereas the remaining elements are described in the in the roadmap for Environment and Geo-Intelligence.

Thematic Objectives – Project Opportunities:

- **Autonomous and Intelligent Detection:** Develop and deploy AI-powered, mobile sensor networks capable of autonomously detecting anomalies in real time across diverse operational environments.
- **Rapid and Precise Identification:** Develop miniaturized, field-deployable molecular diagnostic and sequencing platforms integrated with cloud-based agent libraries and AI-driven interpretation to enable rapid, point-of-care detection of AMR and emerging pathogens at the tactical edge.
- **Continuous Monitoring and Forecasting:** Develop dynamic, continuously updating data systems integrated with advanced geo-mapping, contamination forecasting, and live operational dashboards to enable real-time monitoring of personnel, infrastructure, and environmental conditions.
- **Secure and Interoperable Platforms:** Develop secure, interoperable architectures and collaborative interfaces for DIM systems that enable multinational threat tracking and information sharing without data fragmentation.

Building Block 2: CBRN modeling and simulation

CBRN modeling and simulation serve as vital enablers to model and simulate the dispersion, impact and evolution of CBRN threats. The available digital tools allow defense stakeholders to replicate complex threat scenarios in virtual environments, anticipate contamination, dispersion patterns, and test the effectiveness of protective measures under varying conditions. Advanced models incorporate environmental variables, agent behavior, troop movements and infrastructure layouts to generate actionable insights for preparedness without exposing personnel to real-world hazards. Simulations also facilitate training, mission rehearsal, and inter-agency coordination by providing immersive, consequence driven scenarios.

Thematic Objectives – Project Opportunities:

- **Advanced CBRN Modeling and Simulation:** Integration of AI with CBRN modeling platforms and real-time sensor data to enhance predictive capabilities and enable dynamic, up-to-date threat assessments.

Building Block 3: Medical Countermeasures

Medical countermeasures (MCMs) for Biological threats within the CBRN landscape are essential for mitigating the health impact of intentional, accidental, or naturally occurring outbreaks. Biological threats are categorized by the Centers of Disease Control and Prevention (CDC) into Categories A, B and C (outlined in Figure 4) based on the severity, transmissibility, and potential public panic. **Category A** agents, such as anthrax, smallpox, and botulinum toxin, pose the highest risk due to the ease of dissemination and high mortality. **Category B** agents, including ricin and Q fever, are moderately easy to spread with lower lethality, while **Category C** encompasses emerging pathogens like Nipah virus and hantaviruses. Addressing these threats requires a layered approach utilizing vaccines for prevention (e.g. anthrax, smallpox), antibiotics to combat bacterial agents, and monoclonal antibodies/nanobodies for targeted immediate protection. Additionally, antivirals, antitoxins and phage therapy broaden the therapeutic arsenal. AMR poses a growing threat to military operations by undermining the effectiveness of standard prophylactic and therapeutic measures for combat-related infections. Deployed personnel often operate in austere environments where empirical use of broad-spectrum antibiotics, limited access to laboratory diagnostics and exposure to regions with high AMR prevalence, favors the emergence and spread of multidrug-resistant pathogens. This not only increases morbidity, mortality and evacuation rates but also places a significant logistical and operational burden on military medical services. Phage therapy, which utilizes bacteriophages to selectively target and destroy antibiotic-resistant bacteria, is currently experiencing a resurgence in clinical and research settings as a complementary or alternative solution. As biological threats evolve, emphasis must be placed on platform technologies capable of accelerating the development and deployment of broad-spectrum countermeasures. Together, these innovations strengthen preparedness by enhancing therapeutic precision and operational resilience in high-pressure scenarios.

Critically, all phases of medical countermeasure development and deployment must comply with stringent EU and Belgian biosafety and biosecurity regulations, ensuring that products are scientifically sound, ethically managed, and fit for emergency or accelerated use without compromising public trust.

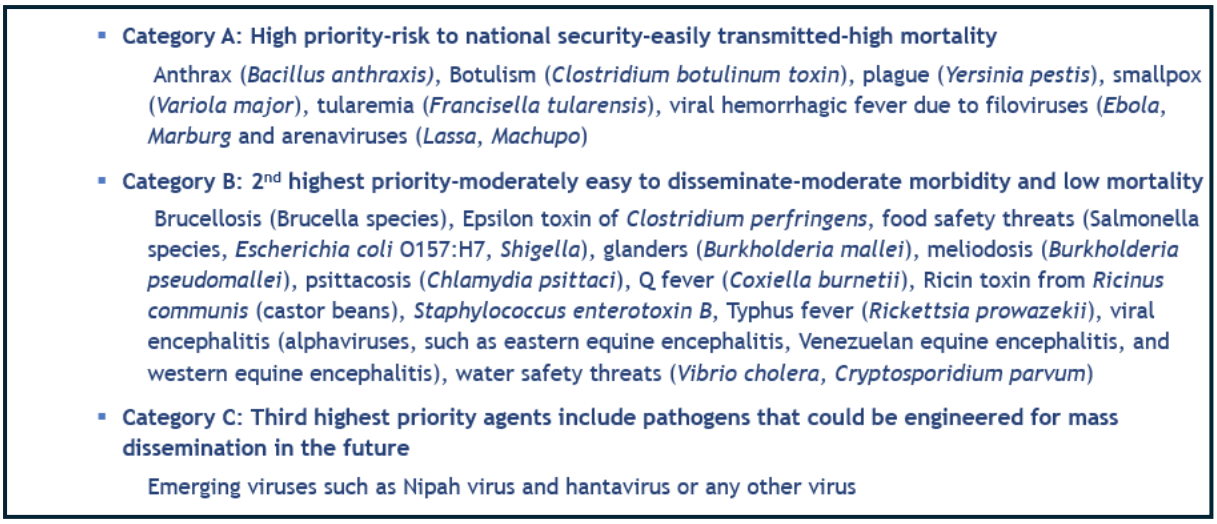
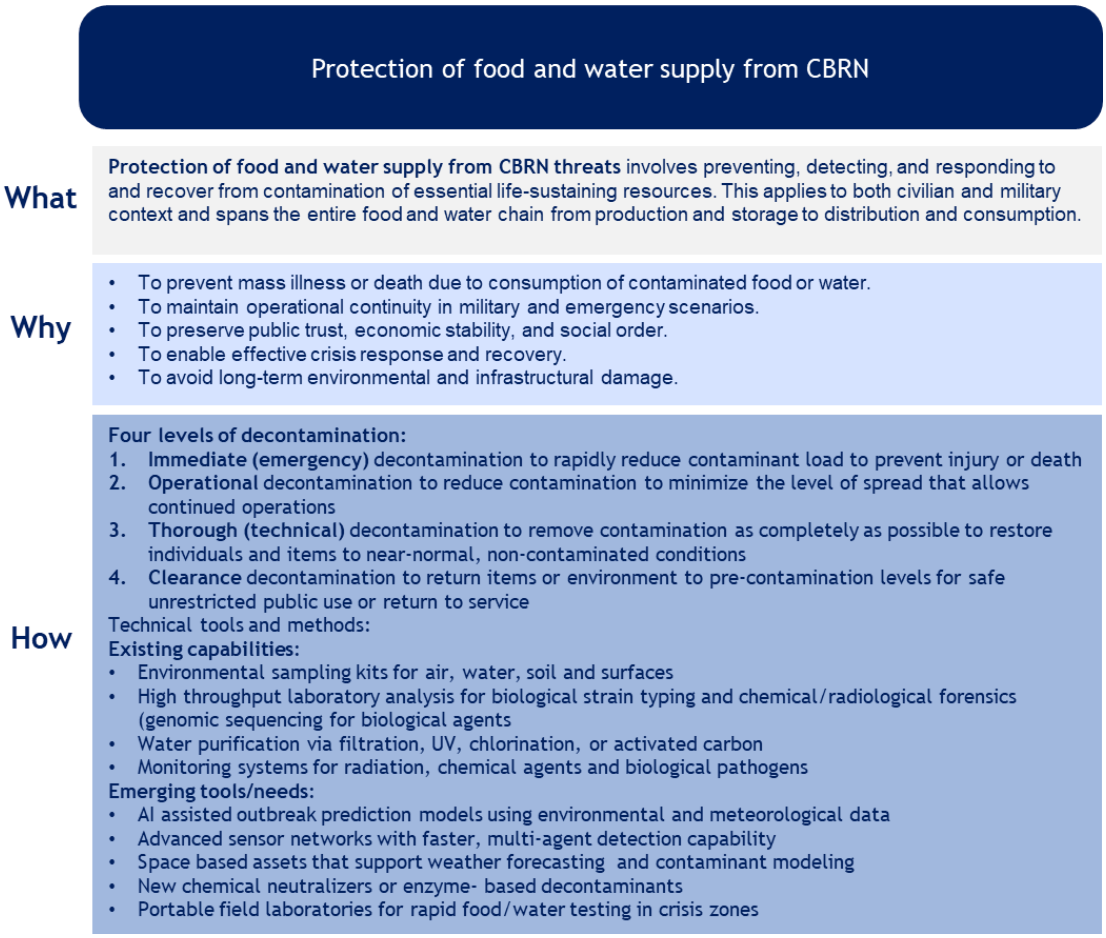


Figure 4. CDC list of Bioterrorism agents/diseases

Thematic Objectives – Project Opportunities:

- **Platform technologies:** Develop a comprehensive arsenal of next-generation medical countermeasures — including biologics, small molecules, modular synthetic biology-based therapeutics, and advanced delivery systems — to enable rapid, scalable, and cost-effective prophylaxis and treatment against emerging pathogens.
- **Tools to Address Emerging Challenges:** Development of innovative technologies to combat AMR.
- **AI Enhanced Drug Development and Therapeutic Precision**: Integrate artificial intelligence to accelerate therapeutic discovery and optimize personalized treatment pathways through enhanced candidate screening and precision drug targeting.

Pillar 2: Protection of food and water supply from CBRN



Protection of food and water resources from CBRN is vital to maintaining public health and continuity of life in both civilian and military contexts. Contaminants can be introduced deliberately or inadvertently, requiring rigorous surveillance, preparedness, and response protocols. Currently, protection is enabled through tools such as portable contamination detectors, spectrometry equipment, bioassay kits, and surface sampling technologies, alongside monitoring systems coordinated by agencies like the Federal Agency for the Safety of the Food Chain (FASFC) and Sciensano. In the event of exposure or contamination, decontamination must be swift and systematic, applying the four recognized levels: **Immediate** (emergency) decontamination to rapidly reduce contaminant load to prevent injury or death, **Operational** short term decontamination to minimize the level of spread that allows continued operations, **Thorough** (technical) cleaning to restore full functionality and safety and **Clearance** (complete) decontamination including verification processes to certify the area and resources are hazard-free. These processes ensure the safe restoration of food and water systems while maintaining public trust.

Thematic Objectives – Project Opportunities:

- **Advanced Detection and Monitoring:** Develop and deploy AI-enabled, real-time sensor systems for rapid detection and identification of CBRN threats in food, water, and the environment, with multi-agent monitoring capabilities.

- **Adaptive Response and Decontamination:** Develop autonomous robotic systems integrated with predictive contamination modeling to rapidly mitigate and contain CBRN threats in affected environments.
- **Smart Packaging:** Development of smart packaging technologies that detect contamination and provide real-time alerts.

Domain 2: Biomanufacturing

Pillar 1: Biomanufacturing of Medicines

Recent global crises have strongly exposed the fragility of supply chains for critical medicines. The European Union is actively working to mitigate these risks by bolstering supply chain resilience and enhancing its strategic autonomy in health [11]. This involves reducing dependency on external sources for Active Pharmaceutical Ingredients (APIs) and finished medical products. The need for sovereign manufacturing capabilities is particularly acute in conflict scenarios, where disruptions can have severe consequences.

	Biomanufacturing of medicines	
What	**Production of critical medicines** has been transformed by biomanufacturing, which enables the development of complex and highly effective therapies. This includes a wide range of biopharmaceuticals such as antibodies, vaccines, cell and gene therapies (C&GT), and therapeutic proteins like peptide hormones and enzymes.	**Pilot facilities** for development of medicines are essential to strengthening EU's health resilience. Recognizing vulnerabilities in global supply chains, it's important to secure access to critical capabilities across all stages—from sourcing raw materials and active pharmaceutical ingredients (APIs) to the production of medical products.
Why	• Supply resources might be compromised in crisis, endangering health & lives due to shortages. CMA identified 200 critical medicines • Substitute or adjust medicines with equivalent treatments for fast and efficient production • COMEDS & MHWG lists of critical medicines in combat zones and times of pandemic (pain meds) • Obtain fast response plan by a network of R&D, local production, logistics & storage (EU critical medicine act)	• Reduce external manufacturing dependencies of APIs from outside the EU for both drug substances and drug products, essential for resilience and strategic autonomy • Obtain non-profit biomanufacturing capacity and experts to rapidly accelerate critical innovations & fill gaps in supply chain. • Reduce technological risks and optimize to obtain efficient, robust, flexile, cost-efficient and less prone to contamination production processes
How	**Existing:** advanced biotech R&D in vaccine and pharmaceutical drug development and production, clinical trial capabilities, highly educated experts **Needs:** • New anesthetics and anti-inflammation medicines • New antibiotics to address shortages • Build & expand domestic API production capacity • Advanced formulations (eg increased stability, optimized drug dosing, multi-dosing, …) • National incentives for new medication (e.g. vouchers/subsidies/tax breaks for off-patent or non-commercial vital medicines) • EMA standards fast-track national regulatory approval mechanisms for critical medicines • Inventory, dispersed storage and distribution systems (cold chain logistics) to prevent shortages • Partnerships with EU countries to share technology and resources	**Existing:** MSAT expert groups, small-scale productions of proteins, viral vectors, antibodies, pre-run cGMP process development, pharma & biotech companies **Needs:** • Manufacturing capacity, including non-profit pilot-scale operations, advanced bioreactors, purification technology and quality control by cGMP standards ensuring proper design, monitoring, and control to guarantee drug identity, strength, purity, and quality • A biomanufacturing ecosystem: network of R&D, biomanufacturing facilities, service, legal, supply chain and logistics companies • Advance MSAT through cutting-edge process innovations such as AI/ML-driven digital twins, flexible biomanufacturing tech and 'Open' production hosts • Advanced Manufacturing Technologies that improve drug quality, address shortages of medicines, & speed up time-to-market e.g., 3-D printing

Building Block 1: Production of critical medicines

Both the EU's Critical Medicines Alliance (CMA) and NATO's Committee of the Chiefs of Military Medical Services (COMEDS) have identified lists of essential medicines, including anaesthetics, antibiotics, and anti-inflammatory drugs, that are vital during emergencies [13]. However, many of these medicines are not commercially viable for continuous production in Europe.

This vulnerability is dangerously amplified for antibiotics due to the escalating threat of AMR. The war in Ukraine, provides a stark, real-world illustration of this crisis in action. On modern battlefields, conditions such as blast-contaminated wounds, long evacuation chains, overwhelmed hospitals, and disrupted labs drive heavy empirical use and misuse of broad-spectrum antibiotics [14]. This environment creates an intense selective pressure for highly resistant Gram-negative bacteria, leading to complex wounds and bloodstream infections that are incredibly difficult to treat. The WHO warns that without reinforced infection prevention, microbiology capacity, and antibiotic stewardship, conflict zones risk becoming reservoirs that export AMR to other health systems.

The urgent need for novel antibiotics to combat these emerging superbugs runs directly into a a **significant market failure**. Because any newly approved antibiotic would be prudently reserved for "last resort" use to preserve its effectiveness, the business case for private investment is fundamentally unworkable. To stimulate their development and manufacturing, especially by startups and SMEs, national incentives are indispensable. Solutions such as government-backed vouchers, subsidies, label extensions, or tax breaks for off-patent medicines are essential to ensure we are prepared for future health crises.

Thematic Objectives – Project Opportunities:

- **Rapid Response Platforms:** Develop flexible platforms for the rapid production of vaccines and biotherapeutics against emerging health threats.
- **Critical Medicine Equivalents:** Develop substitutes or adjusted formulations for critical medicines (antibiotics, anesthetics and anti-inflammatory drugs) to ensure equivalent treatments, improve stability, and optimize dosing.
- **Secure Supply Chains and Storage:** Foster EU-wide collaboration and strategic partnerships with Contract Development and Manufacturing Organizations (CDMOs) to create robust supply chains and secure storage capacity.
- **National fast track regulatory approval mechanisms:** Obtain a national regulatory framework according to EMA standards must be set out to obtain fast response and regulatory approval for critical medicines.

Building Block 2: Pilot facilities

Building a **resilient biomanufacturing ecosystem** necessitates a concerted effort to overcome existing hurdles. There is a tangible need to de-risk the development of innovative biotherapeutics early in the innovation chain. Furthermore, research groups and small companies often lack the capacity to produce materials at a sufficient scale for Phase I/II clinical trials. Compounding this is an acute shortage of highly skilled personnel specialized in Manufacturing Science and Technology (MSAT).

Advanced biotech R&D is fundamental to strengthening Europe's health security. This requires investment in **pilot production facilities that are compliant with Current Good Manufacturing Practice (cGMP) standards**, as defined by the European Medicines Agency (EMA) and U.S. Food

and Drug Administration (FDA) [15]. Such facilities are essential for developing and scaling up APIs for complex therapies, including antibodies, vaccines, and cell and gene therapies (CGTs).
The integration of cutting-edge technologies is transforming the pharmaceutical landscape such as, AI-driven design and digital twins to accelerate drug development and optimize manufacturing processes, 3D printing allowing on-demand production and personalized medicine, and 'Open' production hosts to obtain production free of IP restraints.
Initiatives like the EU Health Emergency Preparedness and Response Authority (HERA) and the forthcoming EU Biotech Hub aim to create a supportive regulatory and investment framework to boost European Biomanufacturing [8][16] in Belgium, with its strong academic and industrial base in advanced biotech for vaccine and pharmaceutical drug development and production, clinical trial capabilities and highly educated experts, is uniquely positioned to play a key role within this EU-wide ecosystem.

Thematic Objectives – Project Opportunities:

- **Pilot Facilities:** Establish cGMP-compliant pilot facilities for the development, testing, and production of APIs and complex biologics.
- **Advanced Technology Integration:** Integrate AI, digital twins, and 3D printing to address medicine shortages, improve quality, and accelerate time-to-market.
- **Talent Development:** Launch hands-on cGMP training programs for highly educated profiles to bridge the MSAT talent gap.
- **Biomanufacturing ecosystem building:** set up a network of universities, biomanufacturing (pilot) facilities, R&D, service, legal support, supply chain and logistic companies to obtain a resilient biomanufacturing ecosystem.

Pillar 2: Biomanufacturing of Advanced Materials and food

Defense and advanced industries, e.g., aerospace, automotive, renewable energy systems, etc. that require materials with tailored properties, such as exceptional strength-to-weight ratios, flexibility, self-repair capabilities, and biodegradability. Traditional manufacturing is often energy-intensive, polluting, and rigid. Biotechnology, particularly synthetic biology, offers a paradigm shift towards sustainable and high-performance materials.

Biomanufacturing of advanced materials and food		
What	**Advanced Materials** engineered through synthetic biology by reprogramming the genetic code and re-engineering organisms, materials with customized properties such as enhanced strength, durability and biodegradability can be designed.	**Food Technologies** can be used to develop more nutritious, functional foods and meal replacements which are essential. Probiotics can help maintain gut microbiota balance, enhance immune resilience, and reduce complications following antibiotic use or radiation exposure
Why	• To improve durability and performance of military equipment: stronger, lighter, self-healing, less toxic, next-gen PPC, stable in extreme conditions, faster to manufacture e.g., ELMs, dynamic camouflage,... • Overcome logistic problems through local produced materials, such as bio-energy sources trough waste, self-healing gear, etc. • Optimize and scale bioprocesses to accelerate the DBTL cycle	• Overcome food and water logistics to the battlefield by local production, lightweight biodegradable packaging • Soldiers often meet inadequate macronutrient intake (carbohydrates & proteins) and have signs of dehydration • Support gut health, boosting the immune system, resilience against diseases, maintain gut microbiome integrity and immune homeostasis through probiotics
How	**Existing**: biocatalysis and enzyme engineering, metabolic engineering, bioprocess design, smart & functional materials. **Emerging tools:** • Lightweight, high-strength fibers, bioplastics • Extreme environment equipment (space/ desert/artic); extremophilic gene expression; production of extremozymes/stabilizing proteins; engineered cellular resilience • In-situ construction/repair in remote areas, smart adaptive infrastructure, living sensors, on-demand material generation, self-healing polymers/materials • AI/ML to optimize bioprocesses to accelerate the DBTL cycle and portable biosynthesis systems to produce local bio-energy • Camouflage by microbes producing pigments/ reflectins; genetic circuits for environmental sensing; bio-inspired structural coloration	**Existing:** freeze dried food & packaging replacements, prebiotics, probiotics, food production through bioprocesses, pilot plants, performance-enhancing foods **Emerging tools**: • Local food production through small-scale bioprocessing in extreme and hostile environments, including space • Development of probiotics reducing secondary infections, gastrointestinal complications, and systemic inflammation • Functional foods & individual nutritional packages for optimal intake, performance -enhancing and gut health, including vitamins, minerals, prebiotics, ... • Advanced individual hydration solutions for rapid rehydration in different weather conditions (linked to wearables)

Building Block 1: Advanced Materials

By engineering the genetic code of microorganisms, scientists can program them to produce materials with novel functionalities. This includes bioengineered fibers stronger than steel, lightweight composites, and adaptive materials for applications such as next-generation Personal Protective Equipment (PPE), self-healing gear and coatings and dynamic camouflage that responds to the environment.

Computational tools are essential for accelerating innovation. Artificial Intelligence (AI) and Machine Learning (ML) can rapidly optimize bioprocesses and shorten the Design-Build-Test-Learn (DBTL) cycle, leading to more efficient and robust production.
Furthermore, the development of portable biosynthesis systems offers a major logistical advantage. These systems could enable the on-demand, in-field production of essential resources like biofuels, biocomposites, and repair materials, significantly reducing the reliance on vulnerable supply lines.

Thematic Objectives – Project Opportunities:

- **Lightweight, Durable materials:** Develop bio-based materials for defense, aerospace, and automotive applications.
- **Living Materials & In-situ repair:** Create materials for on-demand construction and repair in remote areas, smart adaptive infrastructure, and living sensors.
- **Bio-inspired camouflage:** Engineer microbes to produce pigments or reflective proteins for dynamic camouflage systems.
- **Bio-based coatings:** Produce protective and functional bio-coatings with properties like anti-fouling or corrosion resistance.
- **Process optimization:** Use AI/ML to accelerate the DBTL cycle and develop portable biosynthesis systems for local resource generation.
- **Circular economy:** Design materials and processes focused on circularity, emphasizing reuse and complete biodegradability.

Building Block 2: Biomanufacturing of Food

In crisis situations, remote deployments, or combat zones, access to fresh, nutritious food is severely limited. Disruption of food supply chains is a common tactical problem. As a study on Belgian soldiers demonstrated, standard rations can lead to significant loss of body mass and fail to meet macronutrient recommendations, with suboptimal hydration also being prevalent [17]. There is a growing demand for functional foods that actively support physical and mental resilience under stress.

Biotechnology enables the development of innovative food solutions tailored for extreme conditions:

- Formulations that support gut health are critical, as a healthy microbiome is directly linked to a stronger immune system, enhanced resilience against disease, and improved physical performance and recovery [18]. This can be achieved by incorporating probiotics and prebiotics.
- Sustainable and nutrient-dense proteins can be produced from plant-based, insect-based, or microbial fermentation platforms.
- The creation of mobile or deployable food production units can provide fresh nutrition in operational contexts.

Thematic Objectives – Project Opportunities:

- **Resilience-Enhancing foods:** Develop functional foods and meal replacements that boost immunity, gut health, and cognitive performance.
- **Targeted probiotics:** Create probiotic supplements designed to reduce secondary infections, gastrointestinal issues, and systemic inflammation in high-stress environments.

- **Advanced hydration:** Design personalized hydration solutions for rapid rehydration, ideally linked to wearable sensors monitoring physiological status.
- **Mobile food production:** Create containerized, mobile units for producing fresh food (e.g., through hydroponics or fermentation) in the field.
- **Extreme environment nutrition:** Design specialized food solutions for military, space, or disaster relief operations.
- **Smart packaging:** Innovate packaging with integrated sensors to monitor food safety, freshness, and nutrient integrity.

Domain 3: Advanced military health and technologies

Modern military operations increasingly demand sustained physical and psychological performance under extreme conditions. Personnel must be capable of enduring long deployments, operating in hostile environments, and making rapid decisions under stress. Yet, current health and medical systems in defense remain largely reactive, fragmented, and insufficiently personalized.
The focus domain of **Advanced military health and technologies** addresses this gap by enabling a proactive, data-driven, and ethically grounded approach to military health and performance. It encompasses three strategic building blocks:

1. **Data-driven health & readiness optimization**
2. **Advanced medical response**
3. **Human performance enhancement**

Together, these building blocks aim to prevent incapacitation and improve readiness, improve battlefield medical care, and safely enhance human capabilities.

Data-driven health & readiness optimization Advanced medical response Human performance enhancement			
What	**Data-driven health & readiness optimization** to enhance performance and health (both physical and psychological) and to prevent injury & disease for military personnel. This include durable, self-powered wearables or other easy-to-use biosensors that provide (near) real-time data for AI-assisted predictive analysis and tailored health, nutrition, and medical advice.	**Advanced medical response** technologies encompass a range of emerging physical health intervention technologies for military personnel, addressing physical injury, infection prevention, pain, and psychiatry care. These technologies also support trauma triage, assisted medevac and care—particularly through automated systems and AI-assisted digital health platforms.	**Human performance enhancement** technologies include both biotechnological and non-biotechnological interventions that enable military personnel to operate beyond normal limits by improving mobility, fatigue endurance, and decision-making in complex environments. The use of these technologies must be strictly grounded in moral, ethical, and legal principles.
Why	• To optimize military personnel selection, training, and operational performance, while preventing incapacitation from overtraining • To enable tailored plans and decisions regarding vaccination, medication, nutrition, training, rehabilitation, and mission assignment	• To improve the survival chance of wounded military personnel • To enable remote healthcare delivery in hostile environments • To support rapid decision-making for high-volume triage and personalized medical interventions	• Opportunity to equip military personnel to withstand extreme physical and mental demands • Ethical considerations: the long-term effects of human enhancement technologies (e.g. neural implants) on physical and psychological health remain largely unknown
How	**Existing capabilities:** Health monitoring: wearables (e.g. watch, suit, earplug, electro encephalograph headset) & implantable biosensors for real-time & near real-time collection of physiology & biomarker data **Emerging tools:** Health monitoring: development of more durable, self-powered, and AI-embedded devices (including wearables, implantable, and imaging-based devices) that integrate multiple streams of real-time and secured physiological, cognitive, and biomarker data for predictive modeling and personalized interventions Predictive modeling: AI-assisted and secured models, including digital twins, for simulations that optimize medical treatment outcomes and guide training, rehabilitation, and mission assignment of military personnel based on individual health and readiness data, as well as operational conditions	**Existing capabilities:** Physical health intervention: advanced bionic prosthetics Trauma triage, assisted medevac and care: medical drones **Emerging tools:** Physical health intervention: low latency, secure, and AI-assisted remote robotic surgery; non-pharmacological wound care/infection prevention; novel treatments for non-compressible hemorrhage; 3D tissue printing and tissue engineering; biomarkers to predict organ transplantation success rate; novel pain management drugs; auto-injected, personalized resuscitative fluids, blood, or freeze-dried plasma; multi-omics and data models for drug development for traumatic brain injury, sepsis, infection and psychiatric conditions (e.g. PTSD) Trauma triage, assisted medevac and care: autonomous medical drones; AI technology to assist with high-volume triage decisions; AI-assisted wearables and telemedicine platforms to provide secured (real-time) biometric data for (AI-assisted) expert medical advice	**Existing capabilities:** Physical enhancement technologies: exoskeletons (e.g. Onyx by Lockheed Martin) Training systems: AR and VR systems for training, simulation, real-time assistance, or accelerated recovery (e.g. MOVElab) Ethical considerations & guidelines: The six principles for the responsible use of BHE outlined in NATO's BHE strategy (2024), including lawfulness, safety and security, human agency, informed consent, and sustainability **Emerging tools:** Specialized devices & pharmacological tools that enhance cognition, strength, or other capabilities, which include brain-machine interface for controlling external devices, neuro implants to modulate neural activity, pharmacological metabolic enhancers, multi-omics & data models for drug development aimed at enhancing tissue & physiological performance

Building Block 1: Data-driven health & readiness optimization

Military personnel face risks of overtraining, stress-induced injury, and undetected (mental) health deterioration during operation. Current monitoring systems—such as smartwatches or chest straps—offer limited insight and lack integration across physiological, cognitive, and biochemical domains. This building block aims to transform health management from reactive to predictive, using real-time data and AI to guide personalized interventions. In particular, the monitoring and biological basis of sleep is an attractive domain for early detection of mental conditions or neurodegenerative diseases.

Durable, self-powered biosensors and wearables

Existing wearables in defense settings are often fragile, power-dependent, and limited to basic metrics like heart rate or sleep. For example, photoplethysmography sensors used in commercial devices are unreliable under motion or extreme temperatures—conditions common in military operations.

Emerging biosensors, such as flexible epidermal patches and implantable devices, can detect biomarkers like cortisol, lactate, and glucose. When integrated with nanomaterials, energy harvesting systems, and secure communication protocols, these wearables can operate autonomously and withstand harsh environments.

Defense applications include continuous monitoring of fatigue, hydration, infection risk, and psychological stress. The key unmet need is multi-modal sensing with embedded AI (also refer to the section “Time-series based sensing”, Impulse Program Roadmap on Artificial Intelligence) for on-device analysis.

AI-assisted predictive modeling and personalized health recommendation

Current health systems in defense are fragmented and reactive, offering limited insight into individual readiness and mission-specific health risks. Statistical models and generic platforms fail to account for operational stressors, environmental exposure, and cognitive load.

Emerging solutions combine AI-driven predictive modeling with personalized health platforms to simulate health trajectories and deliver tailored recommendations for timely interventions, also described in “Building Block 1.3: Time-series based sensing (incl. health & biosensors)” of the Orientation Roadmap on Artificial Intelligence Digital twins—virtual replicas of individuals—can guide decisions on training, rehabilitation, and deployment by integrating physiological, cognitive, and environmental data. These systems require multi-source data ingestion, context-aware reasoning, and secure interoperability with defense infrastructure (also refer to the section “Building Block 4.3: Simulations and training” of the Orientation Roadmap on Artificial Intelligence).

In parallel, such platforms can deliver dynamic recommendations on vaccination, nutrition, and fatigue management based on real-time biosensor inputs. The key technological gap is interoperability across devices, data standards, and operational systems.

Thematic Objectives – Project Opportunities:

- **Biosensors for Health Monitoring:** work towards improved durability, self-powered, and AI-embedded devices (including wearables, implantable, and imaging-based devices) that integrate multiple real-time and secured physiological, cognitive, and biomarker data and securely transfer these to command systems.
- **AI-assisted Predictive Modeling Systems**: design AI-assisted predictive modeling (including digital twins) and personalized health platforms that source data from

individual health, readiness and operational conditions to guide adaptive training programs, mission-specific health planning, and early warning systems.

Building Block 2: Advanced medical response

Battlefield medicine faces critical challenges: delayed care, limited access, and high casualty rates in the first hour post-injury. Traditional systems rely heavily on human medics and evacuation logistics, which are often compromised in high-intensity or remote operations.
This building block focuses on innovative technologies that improve the speed and quality of medical response, including advanced medical solutions, automated systems for remote healthcare delivery, and AI-supported digital health platforms.

Advanced medical solutions

Current battlefield interventions—such as tourniquets and basic resuscitation kits—are insufficient for complex injuries like non-compressible hemorrhage or traumatic brain injury. Advanced prosthetics and tissue engineering are emerging but lack battlefield-grade resilience and personalization. Technologies such as low-latency robotic surgery, auto-injected resuscitative fluids, and 3D bioprinting offer transformative potential. However, challenges remain in miniaturization, autonomy, and integration with field systems.

Automated systems for remote healthcare delivery

Medical drones are increasingly used for supply delivery, but their role in casualty evacuation and remote care is underdeveloped. Limitations include airspace control, payload capacity, electromagnetic radiation on the field (potential target) and lack of real-time medical decision support.
Autonomous drones equipped with biometric sensors and AI can perform triage, deliver care supplies, and evacuate wounded personnel. Real-world examples like the DP-14 Hawk show promise but lack integration with triage algorithms and battlefield data.

AI-supported digital health platforms for operational support

The current digital health platforms for battlefield use are also fragmented and lack real-time integration with biometric data. Civilian telemedicine systems are not optimized for multi-casualty, high-stress scenarios.
AI-supported platforms can process sensor data, environmental inputs, and medical history to guide triage and treatment. The key unmet need is real-time, secure, and scalable decision support.

Thematic Objectives – Project Opportunities:

- **Innovative Physical Health Interventions:** defense applications include trauma care in armored vehicles, rapid wound closure and advanced wound care, and personalized drug delivery. Projects should focus on deployable medical systems that combine automation, AI, and bioengineering for frontline use. These can include but not limited to:
    - Low latency, secure, and AI-assisted remote robotic surgery
    - Non-pharmacological wound care/infection prevention
    - Novel treatments for non-compressible hemorrhage
    - 3D tissue printing and tissue engineering

  - Biomarkers to predict organ transplantation success rate
  - R&D of novel pain management drugs and new technologies addressing AMR
  - Auto-injected personalized resuscitative fluids, blood, or freeze-dried plasma
  - Multi-omics and data models for drug development for traumatic brain injury, sepsis, infection and psychiatry e.g. PTSD
- **Trauma Triage, Assisted Medevac and Care:** develop technologies with applications in the following areas:
  - **Autonomous medical drones** that integrate biometric sensors and AI to perform autonomous casualty extraction, drone-assisted diagnostics, and remote care in denied environments. Projects should aim to develop integrated drone-care ecosystems with secure data links and battlefield-grade autonomy.
  - **AI technology to assist high-volume triage decisions**
  - **AI-supported wearable and telemedicine platforms** for secured and real-time remote diagnostics and expert medical advice via encrypted channels. Projects should focus on AI-driven platforms that integrate wearables, drones, and command systems for seamless battlefield care.

Building Block 3: Human performance enhancement

Military personnel often operate under extreme physical and cognitive demands. Enhancing mobility, endurance, and decision-making can significantly improve mission success. However, such enhancements must be pursued responsibly, with full respect for ethical and legal standards.

This building block explores biotechnological and non-biotechnological interventions to safely extend human capabilities, guided by NATO's six principles for responsible use: lawfulness, safety and security, human agency, informed consent, accountability, and sustainability.

Exoskeletons and mobility enhancers

Exoskeletons like Lockheed Martin's Onyx reduce fatigue and injury during load-bearing tasks. However, current systems are bulky, energy-intensive, and not mission-adaptive.

Emerging designs focus on lightweight, modular systems with AI-driven motion assistance. Integration with soldier biometrics and mission parameters is still missing.

Neurotechnology and cognitive enhancement

Brain-machine interfaces (BMIs) and neuro implants offer potential for enhanced decision-making and stress resilience. Civilian systems lack robustness, security, and contextual adaptability for combat use.

Real-time modulation of neural activity could support fatigue countermeasures, threat detection, and multitasking. However, ethical concerns and long-term health effects must be addressed for their responsible use.

Pharmacological enhancers and metabolic modulators

Pharmacological tools—such as metabolic enhancers and neuroprotective agents—can extend endurance and accelerate recovery in extreme operational settings. Yet, current options often impair cognition or lack mission-specific targeting. Defense needs safe enhancers tailored to individual physiology and operational demands.

Belgium's biotech sector, rich in SMEs and academic spin-offs, developing pharmacological enhancers are well-positioned to lead innovation. To incentivize companies, regulatory

incentives could include a defense-specific fast-track approval pathway, modeled after EMA's PRIME scheme, and expanded R&D tax credits for SMEs developing strategic health solutions. Real-world gaps—such as inadequate cold-weather endurance treatments—highlight the need for multi-omics-guided drug development and real-time monitoring integration.

Thematic Objectives – Project Opportunities:

- **Specialized Devices:** these include
  - **Exoskeletons and other mobility enhancers** provide mobility support in physical-demanding terrains, fatigue reduction during patrols, and injury prevention in logistics. Projects should develop adaptive light-weight exoskeletons with real-time feedback and mission-specific configurations.
  - **Brain-machine interfaces** and **neuro implants** that provide cognitive load balancing, neural feedback for decision support, and AR/VR-assisted training. Projects should align with NATO's ethical principles and focus on secure, reversible Neurotechnologies.
- **Pharmacological Enhancers and Metabolic Modulators:** using multi-omics-guided drug development and real-time monitoring integration to develop deployable, ethically compliant pharmacological solutions, supported by streamlined regulation and targeted funding.

Conclusion

The convergence of biotechnology and defense represents a pivotal opportunity for Flanders to not only enhance its national security but also to solidify its position as a global biotechnology innovation leader. This roadmap has outlined how biotechnology can offer transformative solutions to modern defense challenges, moving beyond theoretical concepts to tangible applications. From developing next-generation countermeasures against CBRN threats to securing critical medicines supply chains and optimizing the health and performance of military personnel, the potential is immense.

Leveraging a World-Class Ecosystem

This ambition is not merely aspirational; it is grounded in a uniquely robust and vibrant biotech ecosystem that is already a cornerstone of the nation's economy. Belgium's foundation is built upon:

A Complete Value Chain: The country hosts a dense network of world-class academic institutions, dynamic accelerators, and powerful industry clusters. This is complemented by a full spectrum of commercial players—from agile startups and innovative SMEs driving disruptive research, to established, large-scale industrial giants with global reach.

Resilient Biomanufacturing: This integrated ecosystem is the critical engine for building a sovereign and resilient biomanufacturing capability. By controlling the production of essential medical countermeasures, advanced biomaterials, and other critical supplies, Belgium can position itself as a key European enabler, reducing strategic dependencies on volatile global markets and reinforcing the continent's collective security.

The Path Forward: A Call for Coordinated Action

Realizing this vision requires a deliberate and coordinated national effort. The foundational elements are in place, but they must be strategically aligned and mobilized towards defense objectives. This requires several key actions:

Targeted Investment and Public-Private Partnerships: Unlocking these potential demands targeted, long-term investment that encourages high-risk, high-reward innovation. Fostering dedicated public-private partnerships will be essential to bridge the "valley of death" between promising research and deployable, field-tested solutions.

Regulatory and Strategic Agility: A cohesive national strategy must be implemented to intentionally bridge the gap between civilian innovation and defense requirements. This involves creating clear, agile regulatory pathways for dual-use technologies and ensuring that regional strengths are harmonized with overarching federal defense goals, as well as with key EU and NATO priorities.

Empowering Innovators: It is crucial to break down silos between academia, industry, and the Ministry of Defense. By creating dedicated platforms for collaboration and specifically empowering SMEs—the primary drivers of disruptive technology—Belgium can accelerate the development cycle and ensure a continuous pipeline of cutting-edge solutions.

By taking these decisive steps, Belgium can harness its formidable biotech sector to become an indispensable hub for defense biotechnology within Europe and the transatlantic alliance. This is more than an industrial strategy; it is a commitment to ensuring national security, bolstering strategic autonomy, and building a future where Belgian innovation safeguards both its armed forces and its civilian population against the complex threats of tomorrow.

References

[1] **European Commission**. (2025). *New European Biotech Act: Which Way Forward?* European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772866/EPRS_BRI%282025%29772866_EN.pdf
[2] **NATO**. (2024). *Summary of NATO's Biotechnology and Human Enhancement Technologies Strategy*. https://www.nato.int/cps/en/natohq/official_texts_224669.htm
[3] **European Defense Agency**. (n.d.). *CapTech CBRN and Human Factors*. https://eda.europa.eu/what-we-do/all-activities/activities-search/captech-cbrn-and-hf
[4] **European Commission**. (n.d.). *EU CBRN Centres of Excellence*. https://cbrn-risk-mitigation.network.europa.eu/eu-cbrn-centres-excellence_en
[5] **European Commission.** (2025). *15 Years of International Cooperation through the EU CBRN Risk Mitigation Centres of Excellence Initiative*. https://cbrn-risk-mitigation.network.europa.eu/news-1/eu-cbrn-coe-publishes-anniversary-booklet-marking-15-years-international-cooperation-2025-05-28_en
[6] **Mende et al. (2022).** *Multidrug-Resistant and Virulent Organisms Trauma Infections: Trauma Infectious Disease Outcomes Study Initiative*. Military Medicine, 187, S2:42-51. doi: https://doi.org/10.1093/milmed/usab131
[7] **Antimicrobial Resistance Collaborators.** (2022). *Global burden of bacterial antimicrobial resistance in 2019: a systematic analysis*. Elsevier Ltd. doi: https://doi.org/10.1016/S0140-6736(21)02724-0
[8] **European Commission.** (2024). *Commission Launches New Biotech and Biomanufacturing Initiative*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1570
[9] **European Commission.** (n.d.). *Health Emergency Preparedness and Response (HERA)*. https://health.ec.europa.eu/health-emergency-preparedness-and-response-hera_en
[10] **Crowe**. (2024). *Changes to European rules governing the size of companies*. https://www.crowe.com/be/spark/insights/wijziging-europese-groottecriteria
[11] **VLAIO**. (n.d.). *Definition of enterprise size*. https://www.vlaio.be/en/subsidies/green-investment-subsidy/who-can-submit-application-green-project-invitation/definition
[12] **European Commission.** (2024). *Communication on Boosting Biotechnology and Biomanufacturing in the EU*. https://research-and-innovation.ec.europa.eu/document/download/47554adc-dffc-411b-8cd6-b52417514cb3_en
[13] **European Medicines Agency (EMA).** (2024). *Union list of critical medicines*. https://www.ema.europa.eu/en/human-regulatory-overview/post-authorisation/medicine-shortages-availability-issues/availability-medicines-during-crises/union-list-critical-medicines
[14] **World Health Organization** (WHO). (2024). *Statement – Renewed focus on health critical as Ukraine approaches third winter amid full-scale war*. https://www.who.int/europe/news/item/12-09-2024-statement--renewed-focus-on-health-critical-as-ukraine-approaches-third-winter-amid-full-scale-war
[15] **U.S. Food and Drug Administration (FDA).** (2024). *Current Good Manufacturing Practice (CGMP) Regulations*. [Online]. Available: https://www.fda.gov/drugs/pharmaceutical-quality-resources/current-good-manufacturing-practice-cgmp-regulations
[16] **European Commission.** (2024). *Commission launches public consultation on the EU Biotech Hub*. https://europa.eu/youreurope/business/running-business/developing-business/biotech/index_en.htm
[17] **De Bry, W., et al.** (2020). *Dietary Intake, Hydration Status, and Body Composition of Three Belgian Military Groups*. Military Medicine, 185(7-8), e1175–e1182. doi: https://doi.org/10.1093/milmed/usaa061
[18] **Ma, L., et al.** (2023). *Psychological Stress and Gut Microbiota Composition: A Systematic Review of Human Studies*. Neuropsychobiology, 82(5), 247–260. doi: https://doi.org/10.1159/000533131