BLAUWE CLUSTER

INNOVATIEROADMAP

Maritieme beveiliging

APRIL 2026

KONINKLIJK HOGER INSTITUUT voor DEFENSIE
Samen voor #sterkgroeien VLAIO
FLANDERS INVESTMENT & TRADE

Structurele partners

Inhoud

1. Technologiedomeinen

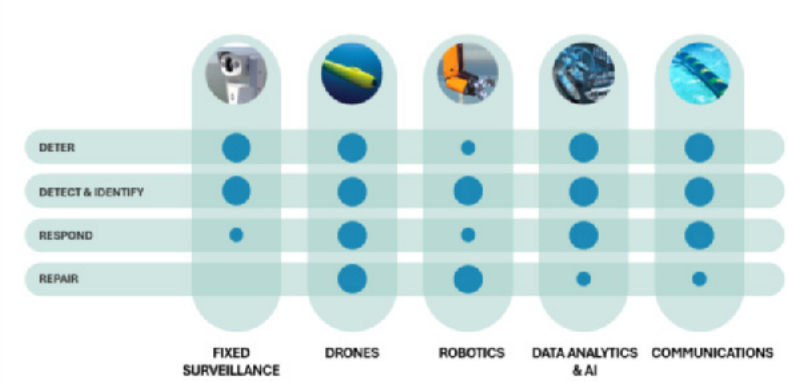
Het ecosysteem voor maritieme veiligheid en defensie is veelzijdig en sterk in opmars. Het steunt op een stevige basis van overheid en marine, gecombineerd met een intensieve samenwerking tussen onderzoeksinstellingen en innovatieve bedrijven. Vooral de wisselwerking tussen kennisinstellingen en kmo's vormt een motor voor vernieuwing: er worden technologische oplossingen ontwikkeld die zowel defensie-specifieke toepassingen als dual-use technologieën mogelijk maken, met toepassingen in havens, offshore energie en maritieme veiligheid en defensietoepassingen.

Ons land 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 we internationaal erkend worden 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** staan we 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.

Daarnaast wordt sterk ingezet op **predictieve AI-toepassingen**, **digital twins**, **sensornetwerken** en **dual-use robotica**. Deze niches hebben een hoog innovatiepotentieel en kunnen uitgroeien tot technologische specialisaties.

Om het innovatieve potentieel tastbaar te maken, kunnen we het maritieme 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 we vandaag in huis hebben. Samen vormen ze het fundament waarop België zijn rol als toonaangevende speler in maritieme veiligheid, defensie en dual-use technologie verder kan uitbouwen.



1.1 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.

Enkele 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.

1.2 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.

Enkele 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.

1.3 Geautomatiseerde systemen en robotica

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.

Enkele 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. pereren in lucht-, zee-, onderwateromgevingen.

1.4 Communicatiesystemen

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

Enkele 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.

1.5 Data-analytics en artificiële intelligentie

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

Enkele 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.

2. Innovatieroadmap maritieme beveiliging

Maritieme beveiliging 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.

MARITIEME BEVEILIGING

DETER

Toegang ontmoedigen

Het verhinderen van ongeautoriseerde of vijandige toegang tot systemen, infrastructuur en strategische zones – zowel in civiele als militaire context. Conceptueel, fysiek, digitaal.

- Continue patrouille en perimeterhandhaving (oppervlakte, lucht, onderwater) – mix van platformen, Nood aan integratie van sensoren in lucht, oppervlak en onderwater om blinde zones te vermijden.
- Ontmoedigen en afschrikken via zichtbare en onzichtbare aanwezigheid (autonome systemen, surveillance), door het opwerken van fysieke en digitale barrières.
- Digitale verdedigingscapaciteit tegen spoofing, jamming en datamanipulatie wordt cruciaal. Opzetten van veerkrachtige, weerbare IT & OT-systemen met redundantie.

DETECT & IDENTIFY

Vroegtijdige opsporing van afwijkingen en verdachte activiteiten boven, op en onder het water

- Detectie: Multidimensionale detectie van dreigingen onder, op en boven water via vaste en mobiele sensoren (radar, sonar, drones, onderwaterrobotica), detectie van digitale sabotage of elektromagnetische storingen.
- Identificatie: Sensorfusie en AI-patroonherkenning zijn cruciaal voor vroegtijdige en autonome identificatie.van afwijkend gedrag, objecten en digitale dreigingen (data uit gecombineerde sensornetwerken (radar, lidar, sonar, camera's, ...), AI gestuurde patroonherkenning, interoperabele systemen)
- Data-integratie tussen civiele, industriële en militaire sensornetwerken, AI-modellen die getraind zijn op tactisch relevante afwijkingen.
- Onderwaterdetectie optimaliseren door het wegwerken van akoestische ruis en het inzetten van mobiele sensoren.
- Intelligence sharing voor het verbeteren van situational awareness en verkorte responstijden.

RESPOND & REPAIR

Snelle en gecoördineerde inzet van middelen bij incidenten of in conflictomstandigheden, snelle repair in geval van incidenten

- Readiness: Snel inzetbare (autonome) responsmiddelen (drones, UUVs, robotica) voor tactische acties zoals mijnendetectie, interceptie of sabotagerespons.
- Execution: verbeterde coördinatie tussen autonome systemen in lucht, wateroppervlak en onderwater (swarm-operaties)
- AI-ondersteunde commandovoering en realtime datafusie (mens-machine teaming en multi-agent operaties in complexe dreigingsscenario's).
- Repair: mobiele herstelcapaciteit op zee (bv. autonome inspectie-/herstelrobots), redundante infrastructuur en digitale resilience voor kritieke systemen
- Cybersecurity: detectie en herstel bij aanvallen (bv. spoofing, datamanipulatie), security-by-design en failover-mechanismen
- Civiel-militaire coördinatie & communicatie en interoperabele protocollen (op uniforme wijze analyseren en interpreteren) voor snelle respons én herstelling.

2.1 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. Belgische 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 Belgische spelers in op behoeften 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).

2.2 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.

2.3 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.

2.4 Repair – herstel van systemen, infrastructuur en operationele capaciteit

Repair is een kritische component binnen maritieme beveiliging: 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.

3. Innovatiekansen

3.1 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 voor vroege detectie van vijandelijke onderwateractiviteit, mijnendetectie.

3.2 Drones en autonome vaartuigen (UAV's, USV's, UUV's)

Autonome vaartuigen en drones vormen een nieuwe generatie inzetmiddelen die het maritieme domein in drie dimensies kunnen bestrijken: door de lucht (UAV's), op het water (USV's) en onder water (UUV's). 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:

- UAV's: boven water – verkenning, patrouille, inspectie, logistiek
- USV's: op water – perimeterbewaking, mijnendetectie, responsplatform
- UUV's: 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: 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.

3.3 Geautomatiseerde systemen en robotica

Geautomatiseerde systemen en robotica richten zich op het versterken van maritieme beveiliging 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.

3.4 Communicatie 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.

3.5 Data-analytics en artificiële intelligentie

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.

3.6 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.

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.

3.7 Samenwerking

Samenwerking tussen stakeholders is een essentiële pijler in de verdere uitbouw van de maritieme beveiligingsindustrie. 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.

4. Conclusie

De Noordzee en onze 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.

De roadmap 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.

Deze innovatieroadmap vormt de basis waarop toekomstige projecten kunnen worden gebouwd – als hefboom voor innovatie, veiligheid en economische groei.

Deze publicatie zou niet mogelijk zijn geweest zonder de waardevolle inbreng, expertise en betrokkenheid van de bedrijven, onderzoeksinstellingen en overheidsinstanties binnen het netwerk van De Blauwe Cluster. Hartelijk dank voor jullie tijd, openheid en bijdrage aan dit document.

Auteurs:
Eveline Buyck (red.).

Gelieve als volgt naar deze publicatie te verwijzen:
De Blauwe Cluster (2026). Innovatieroadmap martieme beveiliging.

De Blauwe Cluster
Bluebridge
Wetenschapspark 1
B-8400 Oostende

T +32 50 26 75 15
www.blauwecluster.be