Waarom ons veiligheidsbeleid rond kritieke maritieme infrastructuur nood heeft aan een inhaalbeweging

Thomas LAMBERT

Korvetkapitein (reservist) Thomas LAMBERT maakt deel uit van de getrainde reserve en is lid van de task force Diplomacy bij Naval Policy Support. Hij is momenteel de Belgische ambassadeur in het Groot-Hertogdom Luxemburg. Voordien bekleedde hij o.m. de functies van diplomatiek adviseur bij de eerste minister, plaatsvervangend ambassadeur in Washington D.C. en bij de Verenigde Naties in New York.

Nos sociétés dépendent dans une large mesure des infrastructures énergétiques et informatiques majoritairement sous-marines qui relient nos pays et nos continents. La vulnérabilité qui en a résulté a reçu beaucoup trop peu d'attention. L'assertivité maritime croissante de la Russie autour de ces infrastructures nous offre l'occasion de nous pencher sérieusement sur cette question. La marine belge doit certainement jouer un rôle à cet égard. Quelques recommandations pour la mise en place de* quick wins*, ou « améliorations rapides ».

Onze welvaart hangt aan een zijden draadje. De blinde vlek ligt onder water: opkomst, belang en beveiliging van onze natte infrastructuur.

Sinds de aanleg van de eerste onderwatertelegraafkabel in 1850 zijn de onderzeese communicatienetwerken sterk uitgebreid en 'vernetwerkt'. Vandaag spreken we over 1 400 000 kilometer datakabels wereldwijd, oftewel driemaal de afstand van de aarde tot de maan. In hoofdzaak gaat het over een 500-tal kabels, waarvan

ruim 200 van strategisch belang. Deze kabels worden doorgaans gelegd en gebruikt door internationale private consortia. Vooral bij de introductie van glasvezelkabels in de jaren ’80 namen deze netwerken een hoge vlucht. Een decennium later nam het aantal zelfs nog meer toe, in een periode waarin de technologische globalisering gelijke tred hield met het incasseren van vredesdividenden na de Koude Oorlog. Vanuit veiligheidsoptiek of met geopolitieke spanningen op de radar was van planning, aanleg en gebruik toen nauwelijks sprake, wel integendeel.

Wereldwijd digitaliseren samenlevingen zeer snel verder en het aantal datakabels zal in elk geval toenemen. Vanuit veiligheidsperspectief heeft dit zowel voor- als nadelen: meer kabels geven betere redundantie, maar ze zijn ook makkelijker te detecteren en te beschadigen.

Het geopolitieke plaatje is intussen drastisch gewijzigd en we bevinden ons aan het begin van een tijdperk van machtspolitiek tussen grote blokken, waarin een hoofdrol is weggelegd voor bestaande grootmachten en aspirant-grootmachten. Dat betekent dat in deze nieuwe wereld de beveiliging, de overtolligheid en het monitoren van deze private netwerken nood hebben aan een grote inhaalbeweging. In de regio van de Stille Oceaan zien we dit nu al het best met de groeiende Amerikaanse inspanningen om datakabels te ontkoppelen van Chinese inbreng. Daar zien we de eerste contouren van een ‘IJzeren Gordijn onder water’, waarbij geprobeerd wordt de Chinese inbreng of potentiële bedreiging tot een minimum te beperken.

Ver buitengaatse energiewinning op de Noordzee nam pas in de jaren ’70 (oliecrisis) een hoge vlucht in de olie- en gassectoren, vooral in Noorse, Britse en Nederlandse wateren. Olie- en gaswinning leverde niet enkel productieplatformen op, maar ook een zeer uitgebreid netwerk aan energieleidingen. Zo worden bijvoorbeeld Noorwegen en het Verenigd Koninkrijk verbonden door de langste gaspijpleiding ter wereld, de ‘Ormen Lange’.

De windsector kende pas een snelle start vanaf het begin van de 21e eeuw en is in het licht van de energietransitie zeker een blijver. Daarbij worden onder Noordzeestaten onderlinge afspraken gemaakt die ook – en dat is nieuw – moeten leiden tot gezamenlijke beveiligingsinspanningen (conclusies van de Noordzeetop Oostende 2023).

We mogen dus stellen dat de Noordzee ondertussen ook een uitgesproken industriële dimensie heeft gekregen. Dit levert kwetsbare en gevoelige infrastructuur op in zowel de traditionele als de nieuwe energiesectoren. Het opblazen van de Nord Stream-pijpleiding in de Baltische Zee leidde in elk geval tot politieke bewustwording over deze kwetsbaarheid. En het gaat wel degelijk om een collectieve kwetsbaarheid: we kunnen immers met wat politieke verbeelding deze infrastructuur ook zien als de *commons* (de 'meent') van de Noordzee-oeverstaten en zelfs van het Europese continent.

Het Belgische deel van de Noordzee (territoriale zee en exclusieve economische zone) is beperkt in oppervlakte. Toch blinkt het uit door een zeer intensief gebruik ervan, dankzij zijn ligging aan de op een na drukste waterweg op deze planeet. Minstens vijf principale datakabels, twee gaspijpleidingen, een elektriciteitskabelverbinding met Groot-Brittannië, meerdere windmolenparken (die tekenen voor bijna 10% van de Belgische energievoorziening), een gaspijpleiding vanuit Noorwegen, gasterminals in Zeebrugge en weldra ook een energie-eiland zorgen ervoor dat de densiteit aan kritische maritieme infrastructuur van strategisch belang is voor ons land en zelfs voor de EU.

De kwetsbaarheden die deze infrastructuur met zich meebrengt worden nauwlettend in de gaten gehouden en gaf ook aanleiding tot de nieuwe wet Maritieme Beveiliging die op 1 januari 2023 van kracht werd. Het veiligheidsdispositief houdt bij ons zeker gelijke tred met de verdere uitbouw van deze maritieme infrastructuur, maar een dergelijk dispositief moet permanent getoetst worden aan evoluerende noden en standaarden. Zo is de toenemende en assertieve Russische aanwezigheid in Belgische, Nederlandse en Britse wateren ondertussen een gekend fenomeen. Er is echter weinig informatie bekend over mogelijke onderwateractiviteiten en/of -observaties van bijvoorbeeld het RFS (*Russian Federation Ship*) *Admiral Vladimirsky* (het intussen breed bekende Russische observatieschip). België is daarbij operationeel en fysiek verbonden met andere, geallieerde Noordzee-oeverstaten en de geldende solidariteit impliceert dat we onze blik ook meer op de hele Noordzee moeten richten vanuit een expeditionair perspectief en in het kader van onze bondgenootschappen. Dat is een zaak van solidariteit en welbegrepen eigenbelang.

Russische activiteiten voor onze kust leveren in de media een snelle connectie op met de indrukwekkende uitbouw van onze infrastructuur rond windenergie. Toch is het niet eens uitgesloten dat de Russische interesse hoofdzakelijk naar datakabels zou gaan. Een vergelijking tussen het vaarpatroon van de *Vladimirsky* en de kaarten van aanwezige datakabels in de Belgische en Nederlandse exclusieve economische zone (EEZ) suggereert zelfs een sterk verband, eerder dan met de windparken.

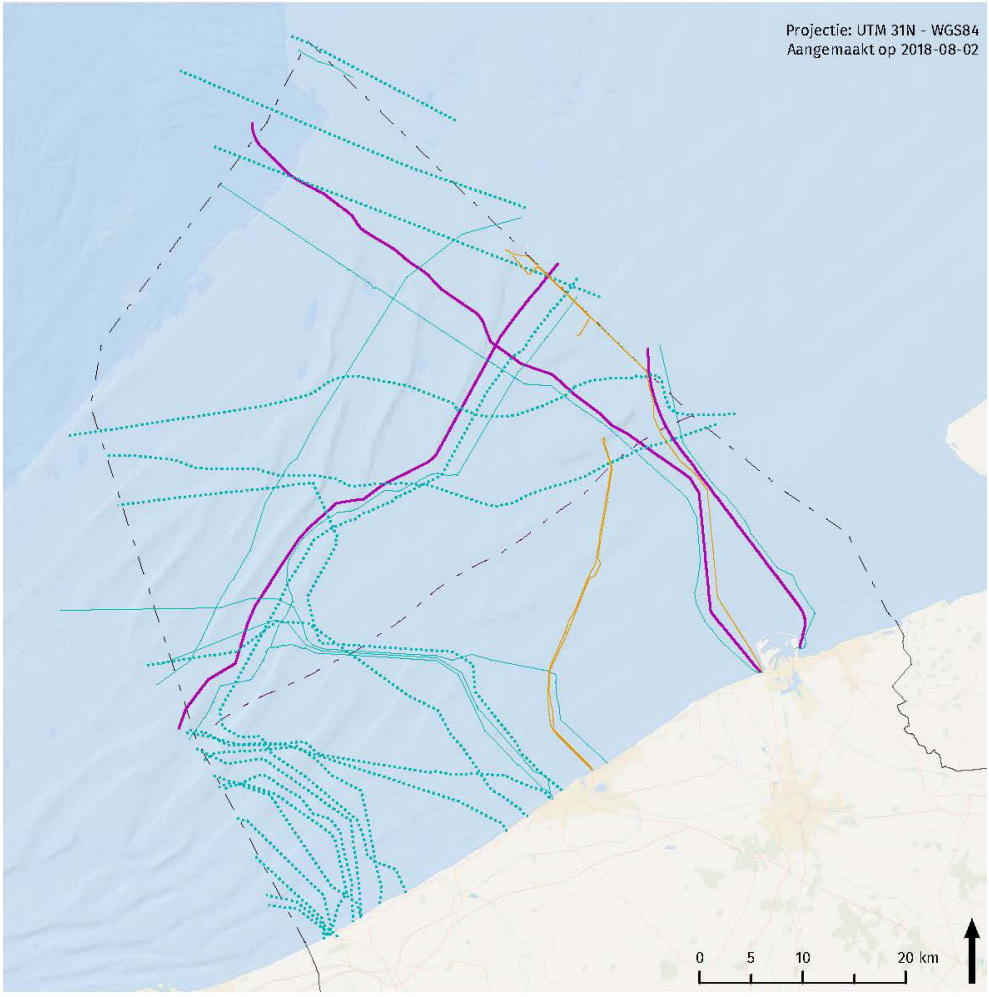
Qua operatieterrein kijken we vooral naar de EEZ, waar een buitenlands schip 'met vreedzame doeleinden' aanwezig mag zijn en waar volledige vrijheid van navigatie geldt, zoals bepaald door artikel 3 van het VN-Zeerechtverdrag.[1] Het in kaart brengen van infrastructuur valt niet onder 'vreedzame doeleinden', maar is zeer moeilijk vast te stellen, laat staan tegen te houden.

De enige middelen die ons echt ter beschikking staan zijn:

1. constante observatie en aanwezigheid, om zo druk te zetten op vermoedelijke observatieactiviteiten + monitoring.
2. diplomatiek reageren. Dat kan in eerste instantie door met diplomatieke démarches te laten weten dat de activiteiten worden geobserveerd, maar in een volgende fase kunnen ook bepaalde sancties worden opgelegd (en in ons geval zal dat via de EU moeten verlopen).
3. een derde reactiemogelijkheid, die in de nabije toekomst moet worden ontwikkeld via het uitvoeren van onderwaterinspecties op en rond deze infrastructuur: de Marine zou, zoals hoger gesuggereerd, relatief eenvoudig de CPV's (*coastal patrol vessels*, kustpatrouillevaartuigen) met 'ogen onder water' kunnen uitrusten; de schepen van het rMCM-programma (*replacement program for mine countermeasures vessels,* de opvolgers van de mijnenjagers) zullen hier sowieso mee zijn uitgerust. Voor bovenwaterinspecties (de constante observatie) zou een toekomstige vliegende dronecapaciteit met adequate sensoren helemaal geen slechte keuze zijn en onze reactiecapaciteit drastisch verhogen.

[1] In territoriale wateren geldt een recht van 'onschuldige doorgang'; een oeverstaat kan voor de navigatie meer beperkingen en modaliteiten opleggen. Voor observatiedoeleinden is het voor een Russisch schip gewoon eenvoudiger en discreter om zich enkel in een EEZ op te houden.

Energie: Kabels & pijpleidingen



Legende

- 12-mijlsgrens
- Belgisch deel van de Noordzee
- Elektriciteitskabel
- Gasleiding
- Telecomkabel (in gebruik)
- Telecomkabel (buiten gebruik)

Bronnen

Basiskaart: ESRI
België: NGI
Maritieme grenzen: Vlaamse Hydrografie
Elektriciteitskabels: Operational Directorate Natural Environment (RBINS)
Gasleidingen, telecom: FOD Volksgezondheid

In elk geval staan we er niet alleen voor: ook buurlanden zoals het Verenigd Koninkrijk (VK) zien de dreiging en nemen maatregelen. Het VK bestelde recent twee schepen, de zogenaamde MROSS (*multi-role ocean surveillance ships*). Deze schepen zullen specifiek worden ingezet met onderwaterdrones, ter observatie en bescherming van de Britse maritieme kritieke infrastructuur. Uit politieke en diplomatieke contacten leren we dat het VK deze schepen ook ziet als platformen voor internationale samenwerking. De expertise die zal worden opgedaan bij de indienstneming en het operationeel inzetten van beide schepen zou ook zeker onze Marine en de Koninklijke Marine erg moeten interesseren.

Seabed warfare (oorlogsvoering op de zeebodem) is in elk geval een nieuwe dimensie die de Marine niet negeert. De internationale realiteit vraagt gewoon dat dit op de radar komt.

De veiligheidsrisico's zijn een groeiende realiteit.

Vanuit operationeel standpunt kan de kritieke maritieme infrastructuur worden opgedeeld als volgt: datakabels, energiekabels (HVDC) en energieleidingen (in essentie olie of gas). Het onderscheid wordt gerechtvaardigd door verschillen in types bedreiging, in kwetsbaarheid, in 'overtolligheid' en rond de vraag welke beveiliging mogelijk en wenselijk is.

Wat betreft de types bedreigingen, kennen datakabels actievedimensies (beschadiging, vernietiging) en passieve dimensies (in kaart brengen, aftappen en aanbrengen van 'slapende' vernietigingsapparatuur). Bij energiekabels of -leidingen is de bedreiging er vooral een van beschadiging of vernietiging. Deze laatste infrastructuur kent ook minder het voordeel van eventuele 'overtolligheid' of redundantie: het omleiden van gas- of oliestromen via andere pijpleidingen is een pak ingewikkelder dan het omleiden van data via doorgaans ruim aanwezige – althans in onze regio – alternatieve capaciteit aan glasvezelkabels. Preventieve en actieve defensie loopt dan ook niet helemaal gelijk voor deze categorieën.

In onze samenleving en economie is de delta tussen een onmiddellijke behoefte aan data en energie versus de benodigde tijd voor herstel van doorgeknipte of beschadigde kabels (kan tot twee weken oplopen) onaanvaardbaar hoog, in het bijzonder voor data. Het is precies deze delta die onze kwetsbaarheid illustreert. In meer dan één sector is dit zelfs extreem tijdsgevoelig. Flitshandel in de financiële sector is een zaak van gefractioneerde seconden en een eventueel gebrek aan back-upcapaciteit via andere kabels en een onderbreking/vertraging van uren of dagen kan dus ernstige economische gevolgen hebben.

Datakabels hebben de diameter van een gemiddelde brandslang. Enkel in zones van 'landval' zijn die kabels versterkt en worden ze onder de zeebodem en onder een laag grind begraven. Verder op zee is dat niet langer het geval en kabelbreuken door menselijke fouten (vissen, ankers slepen, bouwactiviteiten, enz.) of door natuurlijke omstandigheden (onderwaterstormen, seismische activiteiten, schurende bewegingen langs rotsen, enz.) zorgen voor regelmatige breuken. De private consortia achter deze kabels zorgen voor een beperkte, permanente herstelcapaciteit met een klein aantal kabelleggers/herstellers die op stand-by zijn. Hierdoor kan de herstelcapaciteit voor datakabels met een grote praktijkervaring op het vlak van herstellingen relatief snel ingezet worden. Het draagt in elk geval bij tot algemene weerbaarheid (maar niet in eerste lijn via defensieapparaten). In meer perifere EU-gebieden (Noord-Scandinavië, de Azoren, enz.) gelden deze punten natuurlijk in mindere mate.

Voor datakabels bestaan ook weinig of geen andere waardige opties. Satellieten bieden slechts in bijzonder beperkte mate (tot slechts 3% van het dataverkeer in normale omstandigheden) een alternatief en bovendien zijn ze zeer kostelijk. Voor datakabels werkt redundantie nog het best en in de Atlantische kernzone is dat ook een realiteit. Dit is echter minder het geval in perifere gebieden.

Energieverbindingen (olie/gas) zijn daarentegen minder talrijk verspreid, met onderzeese liggingen die rigider zijn en in hoge mate over de gehele lengte qua ligplaats gedocumenteerd zijn. De gemiddelde diameter is ook veel groter en valt (relatief) beter te bereiken. Bij een eventuele beschadiging van dit soort infrastructuur is er hoe dan ook beduidend minder hoge overtolligheid of omleiding via andere pijpleidingen nodig. Een deel van de 'lading' zou in geval van onderbreking zelfs alternatief transport moeten vinden via gespecialiseerd scheepstransport.

Hoe reëel is de bedreiging en overdrijven we die niet?

De vraag 'overdrijven we de bedreiging niet?' kan meteen beantwoord worden met een krachtige 'neen'. Onze digitale samenleving en economie hangen in zeer hoge mate af van energieconnecties en dataverkeer. Zo verlopen dagelijks voor meer dan 11 miljard dollar aan financiële transacties via datakabels, vaker wél dan niet met een maritieme connectie.

De potentiële bedreiging hiervoor komt in hoofdzaak vanuit Russische hoek. Binnen de Russische strijdkrachten opereert het discrete Hoofddirectoraat voor Diepzeeonderzoek (GUGI) met een vloot van een 50-tal gespecialiseerde platformen: 'onderzoeksschepen' zoals de *Vladimirsky* of de *Yantar*, meerdere omgebouwde nucleaire onderzeeërs met gedocumenteerde capaciteiten voor onderwaterwerkzaamheden, kleinere en zeer diep duikende bemande en onbemande tuigen, enz. De investering in en financiering van dit soort capaciteiten loopt in de miljarden euro's. Voor een land met een economie ter grootte van die van de Benelux-landen gaat het om een belangrijke capacitaire en budgettaire inspanning. Of om het nog anders duidelijk te maken: de GUGI-vloot alleen al is talrijker dan het aantal kabelherstellers waarvan hierboven kort sprake was. We kunnen er dus van uitgaan dat de strijdkrachten in Moskou zeer goed weten wat ze hiermee willen aanvangen. De assertieve vaarpatronen van deze schepen tonen dit nog des te meer.

Zo zijn de platformen van de GUGI-vloot zeker sedert 2015 in stijgende mate frequent aanwezig in voor ons gevoelige zones. Het GUGI-schip *Admiral Vladimirsky* was minstens in november 2022 en juli 2023 een opvallende aanwezige in de Belgische en Nederlandse EEZ. De precieze activiteiten zijn niet bekend, maar het schip gebruikte een merkwaardig afwijkend vaarpatroon in de buurt van datakabels en windmolenparken. We mogen aannemen dat de aanwezige infrastructuur daarbij zorgvuldig in kaart wordt gebracht. Of daarbij ook apparatuur ('knipapparatuur' of 'tapapparatuur') wordt of werd aangebracht is minder waarschijnlijk. De mogelijke inzet van ROV's (*remotely operated vehicles*) vanop de *Vladimirsky* is onbekend, omdat het ook niet duidelijk is of het schip over een 'moonpool'[2] beschikt.

[2] Een 'moonpool' is een opening in een schip of werkplatform waarvandaan duikers, materiaal, duikvaartuigen, enz. langs onder het schip kunnen verlaten. Een dergelijke opening is a priori niet of nauwelijks zichtbaar voor externe observaties.

Het feit dat deze infrastructuur privé-eigendom uitmaakt, maakt veiligheid of beveiliging iets moeilijker. Het zijn immers de private bedrijven die in eerste lijn tussenkomen en alarm slaan bij eventueel vastgesteld disfunctioneren, bv. wanneer een datastroom wordt onderbroken of de druk wegvalt in een gaspijpleiding.

Het opblazen van de Nord Stream-gaspijpleiding in de Baltische Zee roept nog steeds vele vragen op. De identiteit van de daders en opdrachtgevers blijft een vraagteken. Het toont wel aan dat de mogelijkheid van sabotage geen fictie is, maar een harde realiteit.

Datakabels breken vaker en doorgaans zonder menselijke kwaadwilligheid. Toch zijn er ook hier enkele recente incidenten die wel degelijk enkel kunnen worden toegewezen aan gerichte, menselijke activiteiten. Noorwegen ondervond dit toen een internetkabel tussen het vasteland en Svalbard brak in januari 2023. Deze kabel bedient een belangrijk grondstation voor satellieten. Eerste conclusies leren ons dat hier door de mens werd ingegrepen.

In november 2021 werd een vier kilometerlang stuk datakabel met militaire sensoren losgerukt, waarna het spoorloos verdween. Dit gebeurde rond de Lofoten (Noorwegen), op een traject dat regelmatig wordt gebruikt door Russische onderzeeërs. Verantwoordelijken werden vooralsnog niet gevonden.

RFS Admiral Vladimirsky -- Foto: Morten Kruger/DR

Op 8 oktober 2023 werden de Balticconnector-gaspijpleiding en twee datakabels in de Baltische Zee ernstig beschadigd. Uit onderzoek blijkt dat dit veroorzaakt zou zijn door een anker dat over tientallen kilometers door het in Hong Kong geregistreerde schip *Newnew Polar Bear* over de zeebodem werd gesleurd. Het onderzoek loopt nog. We mogen echter niet vergeten dat deze pijpleiding ook Finland verbindt met het Europese netwerk van gaspijpleidingen.

Wat doen we eraan?

In België werken vier overheidsdiensten op een geïntegreerde manier samen binnen het Maritiem Informatiekruispunt (MIK) in Zeebrugge: de Marine, de scheepvaartpolitie, FOD Financiën/de douane en FOD Transport/DG Scheepvaart. Elk aspect van de maritieme infrastructuur in het Belgische deel van de Noordzee wordt onderworpen aan een veiligheidsanalyse. De operatoren moeten elk een veiligheidsplan voorleggen aan het MIK en de Nationale Autoriteit voor Maritieme Beveiliging moet dit plan goedkeuren. Naast deze interdepartementale samenwerking heeft de Marine bijzondere relaties aangeknoopt met de offshore sector en Elia die in ons land de elektrische bekabeling beheert. Deze relatie heeft geleid tot wederzijds vertrouwen en doorgedreven samenwerking.

Specifiek voor de Marine worden twee patrouilleschepen ingezet, op roterende basis. De aanschaf van een derde CPV werd onlangs in het vooruitzicht gesteld. Deze schepen zijn bijna permanent op zee in onze zone, maar het ontbreekt hen vooralsnog aan ‘ogen onder water’. Dit probleem zou relatief eenvoudig kunnen worden verholpen mits een lichte dronecapaciteit en/of gesleepte sonarmodule aan boord wordt toegevoegd. Voor het derde schip zou daarom de dekruimte idealiter moeten worden uitgebreid of verlengd.

De toekomstige mijnenbestrijdingsvaartuigen (het rMCM-programma) brengen vanaf 2025 nieuwe capaciteiten naar de Marine. Deze schepen maken een paradigmashift uit voor de mijnenjacht en worden moederschepen voor de inzet van

drones, in de lucht, aan de oppervlakte en onder water. De vraag is of deze platformen niet gebaat zouden zijn bij een relatief lichte capacitaire uitbreiding die – naast de mijnenbestrijding als hoofdtaak – ook het monitoren van onderwaterinfrastructuur zou kunnen omvatten. Het zou ons daarenboven toelaten deze extra capaciteit ook expeditionair in te zetten. Per slot van rekening gaat het om infrastructuur die 'vernetwerkt' is met die van onze buren en bondgenoten: één voor allen, allen voor één.

Ons land is reeds voortrekker bij de opbouw van expertise rond de inzet van onderwaterrobotsystemen voor de mijnenbestrijding via het *Mine Clearance Risk for Europe* (MIRICLE)-project. Het maakt deel uit van het EU-PESCO-project *Maritime semi-Autonomous Mine Countermeasures* (MAS MCM). Hoewel de focus daarbij ligt op mijnenbestrijding, lijkt de stap naar inzet voor het monitoren van infrastructuur niet bijzonder groot.

België besloot recent ook toe te treden tot het EU-PESCO-project voor *critical seabed infrastructure protection* (CSIP) met zes andere EU-lidstaten, waaronder Italië als coördinator. Dit project kijkt ook naar de ontwikkeling van toekomstige technologie ter bescherming van onze natte infrastructuur. De link met het rMCM (*replacement mine countermeasures*)-project (de twaalf toekomstige mijnenbestrijdingsplatformen voor België en Nederland) kan snel worden gelegd en het biedt België de opportuniteit om in BeNeSam (Belgisch-Nederlandse marinesamenwerking)-verband ook de lead te nemen rond een subproject met als doel de maritieme infrastructuur onder water te monitoren.

Conclusies en aanbevelingen

Voor een land als België, en bij uitbreiding de hele EU, is dus de groeiende belangstelling voor de Noordzee als industrieel gevoelige zone van strategisch belang. Onze afhankelijkheid van energie en data via de zee groeit elke dag. En dus ook onze kwetsbaarheid.

Er zijn voldoende precedenten en zelfs incidenten die duidelijk maken dat de bedreigingen reëel zijn en dat minstens één globale speler zijn uitgebouwde capaciteiten daartoe ook effectief inzet.

België neemt zijn verantwoordelijkheid voor veiligheid en beveiliging van deze infrastructuur: op intern wetgevend vlak met o.m. de nieuwe wet Maritieme Beveiliging, via het diplomatiek bijeenbrengen van 'buren en bondgenoten' op een Noordzeetop, door civiele en militaire maritieme capaciteiten te bundelen (in nauwe samenwerking met de private operatoren) via het MIK en het Maritiem Reddings- en Coördinatiecentrum (MRCC), maar ook door de uitbouw van bestaande en toekomstige varende capaciteiten.

> *Gelet op onze niet onbelangrijke verantwoordelijkheden als maritiem logistiek knooppunt op het Europese continent, moet worden bekeken of de capaciteiten van de Marine geen bescheiden verdere uitbouw verdienen door specifieke onderwatermonitoringcapaciteiten in gebruik te nemen. De rMCM-platformen bieden hiertoe de beste gelegenheid, ook om een dergelijke capaciteit expeditionair in te zetten. De PV's lijken zeker gebaat bij de mogelijkheid om een mobiele capaciteit voor onderwaterobservaties (bv. Remus-systemen) aan boord te kunnen nemen. Een derde CPV krijgt hiervoor dus best wat meer dekruimte.*

Minstens in België valt de energie- en data-infrastructuur op zee (windmolens, elektriciteitskabels, datakabels) in de eerste onder de verantwoordelijkheid van de private bedrijven die de infrastructuur in portefeuille hebben en uitbaten. Ondanks de groeiende strategische aard van deze infrastructuur zal dit allicht niet veranderen. Dit betekent ook dat anomalieën in het functioneren van hun systemen eerst zullen vastgesteld worden door deze bedrijven en dus niet noodzakelijk door de betrokken overheden zoals Defensie, de federale politie of de kustwacht

> *Verscherpte preventieve waakzaamheid zal dus ook de private operatoren moeten omvatten, die zowel het recht zullen moeten krijgen als de plicht zullen moeten hebben om opvallende dysfuncties te melden bij een enkele POC zoals het MIK. Daarbij zou de aanbreng van (nog meer) sensoren op de infrastructuur kunnen worden opgelegd of overeengekomen.*

> *De aanstelling van een nationale coördinator voor de bescherming van onze maritieme infrastructuur zou ook coördinatie- en reactieprocessen kunnen versnellen en optimaliseren.*

De Noordzeetop die op het initiatief van België in 2023 bijeenkwam met andere Noordzee-oeverstaten had als hoofddoel werkbare afspraken te maken rond de toekomst van offshore windenergie in de Noordzee, maar ook rond veiligheid en beveiliging van de gezamenlijke en verbonden infrastructuur. Op diplomatiek vlak wordt nu gewerkt aan de opvolging van deze top met de deelnemende landen.

> *Daarbij houdt België het initiatief om eventueel ook te komen tot een permanent en intrageallieerd orgaan dat toezicht kan houden op het 'gemenebest' dat de Noordzee voor ons allen uitmaakt.*

De inhaaloperatie rond beveiliging van onze infrastructuur gebeurt via meerdere platformen: maritieme strategie van de EU, het EU-veiligheidsbeleid, PESCO-projecten, de NAVO, de opvolging van de Noordzeetop, bilateraal met de buurlanden, coördinatie tussen de EU en de NAVO, multilateraal, gesprekken met de relevante industrie en meerdere overheidsagentschappen in België. Ook de *Joint Expeditionary Force* (JEF), een samenwerkingsverband van tien Noord- en Oostzeelanden rond maritieme expeditionaire capaciteit waaraan ons land niet deelneemt, richt zich nu op deze problematiek.

> *Coherentie tussen alle bovenstaande acties is bijgevolg belangrijk, voor alle betrokken landen. Een civiel-militair totaaloverzicht kan best op EU-niveau of op het niveau van de NAVO worden georganiseerd. Voor België zou het slechts een kleine inspanning vergen om ook een waarnemersstatus binnen het JEF te krijgen.*

Trefwoorden: Belgische Marine, kritieke infrastructuur, CPV, rMCM, energie, windmolens