Informatiegestuurd optreden is het fundament

Position paper TNO voor het rondetafelgesprek over een strategie ter bescherming van Noordzee-infrastructuur, op 17 mei 2023

Oproep aan de Tweede Kamer

Windmolenparken op zee, internetkabels die ons verbinden met de rest van de wereld; Nederland is in toenemende mate afhankelijk van infrastructuur op de Noordzee. Dat maakt ons land echter ook kwetsbaar voor aanvallen op deze infrastructuur. Complicerende factor is dat het te bewaken gebied enorm is, de middelen schaars zijn en dat verantwoordelijkheden, kennis en informatie over veel verschillende ministeries en bedrijven verdeeld zijn.

TNO roept daarom op om:
1. de krachten te bundelen en samen te werken naar informatie gestuurd optreden;
2. met innovatieve sensoren het risicogebied te monitoren, om sneller in te kunnen grijpen;
3. een centrale databeheersorganisatie met wettelijke basis op de richten (bijvoorbeeld zoals de Geologische Dienst Nederland de data van de ondergrond beheert).

Inleiding

De aanval op de Nordstream pijpleiding heeft duidelijk gemaakt hoe kwetsbaar de onderzeese infrastructuur is. De Noordzee herbergt een enorme hoeveelheid aan kabels, leidingen en windparken die onze energievoorziening, internetverbindingen en daarmee uiteindelijk onze economie en onze welvaart en democratie mogelijk maken. Zoveel vitale infrastructuur op de zeebodem moet tegen sabotage en digitale aanvallen worden beschermd. Dat is echter geen eenvoudige opgave. Vier uitdagingen:

1. **Omvang.** Allereerst is het gebied enorm: het Nederlandse deel van de Noordzee is 58.500 km^2, anderhalf keer het oppervlak van Nederland. In tegenstelling tot op land of in de lucht, zijn er nauwelijks sensoren beschikbaar om actief te monitoren wat er op en onder water allemaal gebeurd. Bovendien zijn de middelen om snel in te kunnen grijpen schaars. In de diepzee van het Caraïbische deel van Nederland is deze opgave zo mogelijk nog complexer.

2. **Governance**. Een tweede complicerende factor is dat de verantwoordelijkheid over de Noordzee en haar infrastructuur belegd is bij zeven verschillende ministeries[i] en een veelvoud aan private partijen, zoals energiebedrijven, energietransport- en leidingbedrijven, zeekabelmaatschappijen, internetproviders en techbedrijven.

3. **Versnipperde informatie**. Om bovenstaande reden is ook de informatie versnipperd. Elk ministerie heeft een eigen set data, maar de bedrijven ook. Delen van data is (om commerciële of AVG-redenen) complex. Dit maakt effectief en tijdig optreden tegen een mogelijke dreiging moeilijk.

4. **Internationale component**. Zowel de infrastructuur als de informatie hebben een internationale dimensie. Een deel van de kabels en leidingen lopen door tussen twee of meerdere landen, soms binnen de EU maar ook daarbuiten. De uitdaging van governance en versnipperde informatie speelt ook in andere landen; soms langs dezelfde lijnen als in Nederland, maar soms ook anders.

Informatiegestuurd optreden is de basis

Informatie die relevant is voor de (beveiliging van) onderzeese infrastructuur kent verschillende lagen:

- **Planning en vergunningverlening**. Deze informatie is wettelijk publiek toegankelijk. TNO verwacht dat deze informatie steeds belangrijker wordt voor internationale en Europese samenwerking op de Noordzee.
- **Ontwerp en installatie**. Technische informatie voor de uitvoering van ontwerp en installatie van de infrastructuur is thans beperkt publiek toegankelijk, maar zal beter beschermd moeten worden. Met de nauwkeurige positie, specifiek maritiemtechnische uitvoering en materialen geef je een potentiële opponent immers een routekaart van je kwetsbaarheid. TNO adviseert daarom deze technische en installatie informatie beter te beschermen.
- **Operationele informatie**. Sensordata (live data) en periodieke informatie (maandelijkse, jaarlijkse survey data) van alle infrastructuur, kabels, leidingen en alle andere bronnen is op dit moment enkel beschikbaar voor overheden en commerciële beheerders op de Noordzee en wordt op ad hoc basis gedeeld. Er is geen totaaloverzicht wat onder water ge beurt. Daarnaast wordt enerzijds data vergaard met zinvolle data maar waar niets mee wordt gedaan, en anderzijds data zinloos wordt vergaard, wat een vals gevoel van veiligheid geeft.

TNO adviseert daarom alle huidige beschikbare operationele *data* centraal samen te brengen in een digitaal representatiemodel van de Noordzee en die naar gevalideerde *informatie* te vertalen. Daarmee creëert Nederland een instrument om met de beperkte middelen informatie gestuurd te kunnen optreden en de ontwikkelingen in de tijd te kunnen weergeven. Alle relevante departementen en bedrijven kunnen hun gegevens inbrengen[ii]. TNO adviseert dit te beleggen in één beheersorganisatie, naar voorbeeld van de Geologische Dienst Nederland die de data van de ondergrond beheert. De centra die (verschillende) overheidstaken voor de Noordzee uitvoeren kunnen hieraan decentraal operationele informatie toevoegen, gebruiken en analyseren.

Aanvullende oplossingsrichtingen

- **Risicogestuurd beschermen**. Bescherming van infrastructuur wordt sterk bepaald door de verwachte dreiging. TNO verwacht dat die onder water qua aantal en soorten zal toenemen, omdat de technologie om onder water te opereren toegankelijker zal worden. Omdat infrastructuur tot wel 100 jaar zou kunnen meegaan, is het nodig te weten hoe de dreiging zich over die periode zal ontwikkelen, zodat men daarop de infrastructuur kan plannen, ontwerpen en installeren. Daarnaast vergen de omvang van te beschermen belangen en de schaarste van middelen een risicogestuurde aanpak op basis van gevalideerde informatie.

- **Governance**. Om dit aan te kunnen is het belangrijk dat de risico's intergouvernementeel, interdepartementaal en interdisciplinair worden vastgesteld. Verkavelen van de risico's over landen, departementen of disciplines leidt tot kwetsbaarheid waar een opponent gebruik van kan maken. Dit vraagt om een andere vorm van governance van de Noordzee: van gebeidsverantwoordelijkheid naar een *system engineering* aanpak.

- **Gelaagde bescherming**. TNO adviseert de bescherming in verschillende schillen op te bouwen. Rondom zeer kritische infrastructuur zal men meer schillen nodig hebben dan ergens anders. Omdat deze bescherming grote investeringen zal vragen, is clustering en redundantie van bepaalde infrastructuur (transformatoren, kabels) nodig.

- **Permanente detectie**. Over tijd zullen nieuwe innovatieve technologieën hun intrede doen die kunnen detecteren of iemand of iets in de buurt van kritieke infrastructuur komt. Dat is belangrijk voor de *attributie* van ongewenste activiteiten. Op dit moment ligt de nadruk op *bovenwater* sensoren zoals satelliet, radar en AIS[iii] informatie, maar ook het aantal en de verscheidenheid van

onderwatersensoren zal toenemen: permanent aangebrachte statische sensoren[iv], dynamische sensoren (sonar van visserij) die toevallig in de buurt zijn en dynamische sensoren (onbemand of autonoom), die met een bepaald doel en taak worden ingezet.

- Connectiviteit. Omdat al deze technologieën in hoge mate interoperabel moeten zijn, is het belangrijk dat de connectiviteit in de nationale informatieketen wordt verbeterd en past bij de vereiste mate van bescherming. Het is ook belangrijk om de connectiviteit van de opponent te kunnen ontzeggen of te verzwakken. Hetzelfde geldt voor navigatie: die moet in de eigen keten robuust zijn en aan de opponent tijdelijk kunnen worden ontzegd.

Contactpersoon: Tim Kreuk, manager Public Affairs (tim.kreuk@tno.nl)

[i] Vanuit de overheid het Ministerie van IenW, Ministerie voor Klimaat en Energie, Ministerie van EZK, Ministerie van Buitenlandse Zaken, Ministerie van Defensie, het Ministerie van J&V, het Ministerie van LNV
[ii] Deze digitale representatie kan op elke informatielaag anders zijn. Vooral bij planning en vergunningverlening is "security by design" essentieel. Om dat goed te doen is het belangrijk dat verschillende scenario's of varianten in één data-omgeving met elkaar kunnen worden vergeleken. Alleen zo kunnen de belangen ten aanzien van economie, klimaat, omgeving en bescherming het beste in balans worden gebracht.
[iii] Automatic Identification System, verplicht voor grote zeeschepen, maar gevoelig voor cyberaanvallen.
[iv] Een voorbeeld hiervan is een passieve fiberoptische sonarketen, ontwikkeld met TNO-kennis, waarmee ongewenste activiteiten onderwater onopvallend kunnen worden vastgelegd.