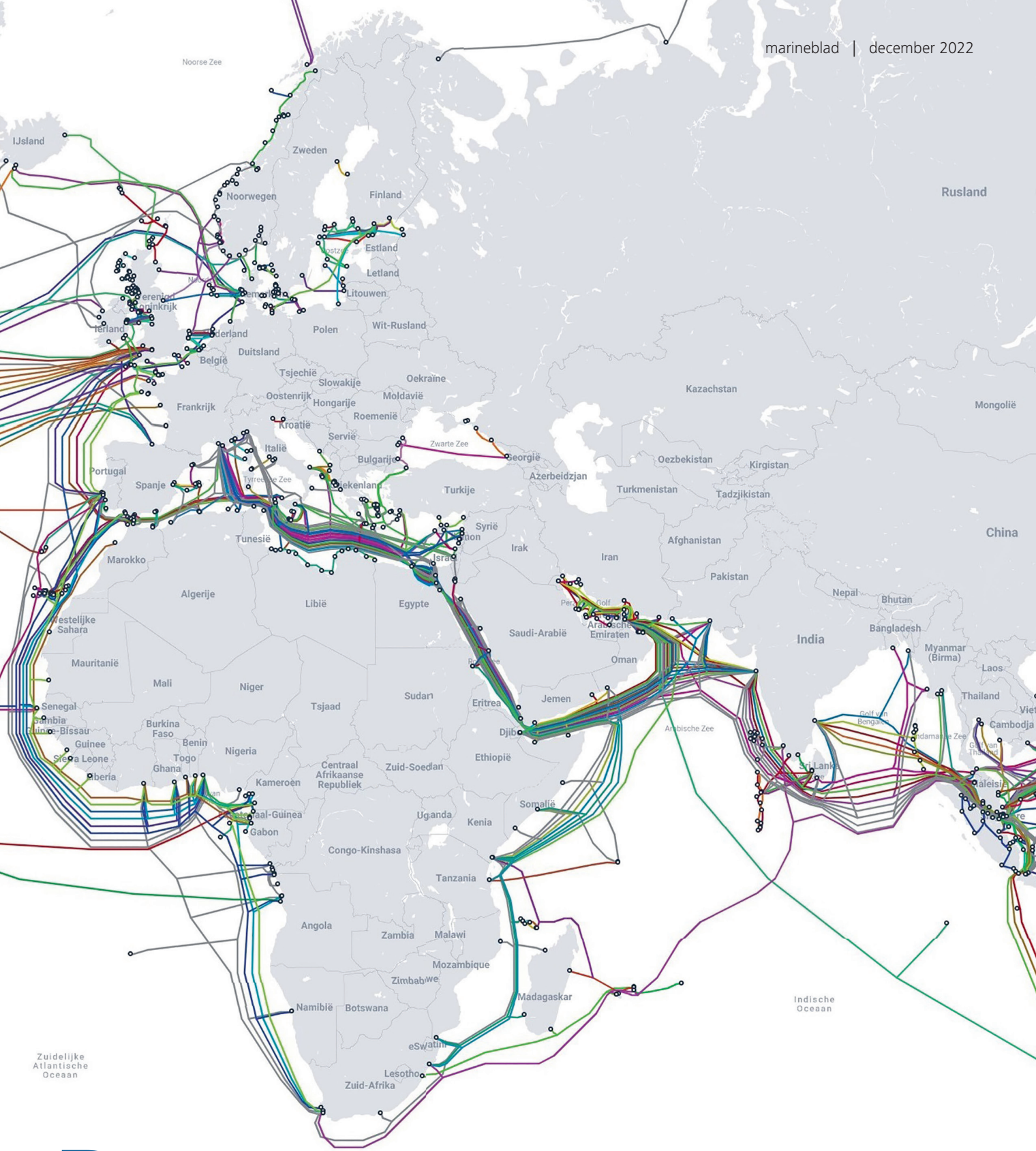
KTZ (LD) mr. dr. Martin Fink

Uitdagingen in de diepte

Juridische achtergronden bij de bescherming van onderzeese kabels en pijpleidingen

Het onderwerp onderzeese kabels en pijpleidingen en het *Nord Stream*-incident van afgelopen september brengt een aantal actuele thema's bij elkaar. In hoeverre het voorval in verband staat met de oorlog in Oekraïne is slechts gissen, maar de brug naar het andere actuele thema van *hybrid warfare* is snel gemaakt.

Overzicht van onderzeese kabels (Teleography)



Deze activiteiten dwingen ook Nederland, in het bijzonder in de maritieme dimensie, dit aandacht te geven. Ten eerste vanwege het steeds intensievere gebruik van de Noordzee en de groeiende afhankelijkheid van het exploiteren van natuurlijke bronnen in zee. Een zorg die het *Hague Centre for Strategic Studies* (HCSS) vorig jaar nog in het rapport *The High Value of The North Sea* schetste. Ten tweede omdat de onderzeese infrastructuur, waar data en grondstoffen doorheen vloeien, een achilleshiel is. De aantasting ervan kan ontwrichtende gevolgen voor de samenleving teweegbrengen. En dat brengt ons bij het cyberdomein als actueel thema. Dit domein is op zijn beurt weer afhankelijk van onderzeese infrastructuur. Zowel een cyberoperatie tegen de data die door de kabel stroomt als een fysieke kabelbreuk tast dit alles aan.

Waar zoveel onderwerpen en invalshoeken bijeen komen, zijn antwoorden op veel vragen niet makkelijk te formuleren. Die vragen reiken van detailvragen over middelen en capaciteit en de rol van verschillende veiligheidspartners, tot en met meer filosofische kwesties zoals de vraag of een betere bescherming van maritieme infrastructuur gepaard moet gaan met inperking van de vrijheden van de

Het gaslek in de *Nord Stream* 2-pijpleiding gezien vanaf een Deense F-16, 25 september 2022 (Danish Defence)

zee. Deze bijdrage stipt enkele juridische punten aan over de bescherming van onderzeese kabels en pijpleidingen, met als doel een eerste kader te scheppen waarbinnen de discussie over bescherming ervan kan plaatsvinden. Deze bijdrage begint met drie veiligheidsperspectieven en uitdagingen en gaat vervolgens kort in op de achterliggende kaders.

Drie veiligheidsperspectieven

In het huidige debat over de bescherming van onderzeese kabels en pijpleidingen spelen tenminste drie veiligheidsperspectieven of -invalshoeken een rol. In de eerste plaats een perspectief waarin de fysieke bescherming van onderzeese infrastructuur tegen ongelukken of moedwillige beschadiging centraal staat. Ongelukken worden veroorzaakt door bijvoorbeeld ankers of sleepnetten.
Bij moedwillig beschadigen is het oogmerk divers, zoals diefstal of daden met een meer terroristisch oogmerk. In juridische zin gaat het naast het uitbaten van rechten kabels en pijpleidingen te mogen leggen in zee en eventuele strafrechtelijke reacties door een staat om civielrechtelijke aansprakelijkheid. Iemand moet immers voor de schade opdraaien.

Naast dit 'normale' beschermingsregime, focust de huidige discussie over de bescherming van onderzeese infrastructuur zich op interstatelijke veiligheid. Bij deze invalshoek hebben we te maken met spanningen tussen staten door activiteiten - direct of indirect - die de staatsveiligheid kunnen aantasten. Een voorbeeld is kabelspionage. Sabotage van kabels of pijpleidingen met de nodige gevolgen kan daar ook een voorbeeld van zijn. Doorgaans blijven deze zogenaamde hybride dreigingen onder de lat van het interstatelijk geweldsverbod. In de media lezen we berichten dat Russische vaartuigen rondhangen in de buurt van kabels, hetgeen andere staten zorgen baart.[1] En dat het Russische oceanografisch onderzoeksschip *Yantar,* net als het *USS Jimmy Carter,* de benodigde capaciteiten bezit om dergelijke acties uit te voeren.[2] In juridische zin gaat dit over het recht toepasselijk op interstatelijke verhoudingen, dat in het ultieme geval tot interstatelijk geweldgebruik kan leiden.
In de derde plaats kan er sprake zijn van een lopend gewapend conflict, waarin oorlogvoerende partijen het aanvallen of gebruiken van onderzeese kabels en pijpleidingen onderdeel van de militaire strategie maken. Voordeel op de tegenstander wordt dan behaald door deze communicatie, informatie en grondstoffen te ontnemen of door heimelijk mee te luisteren. Het juridische kader is

> 'Een kabel of pijpleiding heeft geen vlag of nationaliteit waardoor staten zich aangesproken kunnen voelen'

in dit geval vooral het oorlogsrecht, dat de regels tijdens een gewapend conflict bepaalt tussen partijen, maar ook tussen partijen en neutralen.
Wie dus de vraag stelt tegen welke dreigingen onderzeese infrastructuur moet worden beschermd, moet dit relateren aan verschillende invalshoeken. Wat 'bescherming' en 'bedreiging' betekent is daarmee niet eenduidig. Dit zal onder meer resoneren in de 'wie-doet-wat'-vraag en welke bevoegdheden er zijn. En naast de drie invalshoeken die hier zijn genoemd, zijn er mogelijk meer te noemen, waaronder rampen- en calamiteitenbestrijding op zee.

Uitdagingen

Deze veiligheidsperspectieven hebben tal van uitdagingen. Ik noem er hier drie.

Who dunnit and why?

De dreigingsdiversiteit in het huidige veiligheidslandschap maakt het lastig te bepalen om welk veiligheidsperspectief het nou eigenlijk gaat. Het is daarmee moeilijk invalshoeken - en de reactie erop - uit elkaar te houden. Is het een eenvoudige visser die zich toevallig bij een onderzeese kabel ophoudt of kabeldiefstal pleegt, een visser die in werkelijkheid heimelijk acties uitvoert in opdracht van een staat,[3] of een schip van of onder controle van een staat in oorlog die acties onderneemt tegen de tegenstander door middel van kabelspionage of het vernietigen van een kabel dat ook andere landen raakt? Zoals *gray zone* wetenschapper Arsalan Bilal stelt in de *NATO Review*: 'The [second] defining characteristic of hybrid warfare relates to ambiguity and attribution.'[4] Het is moeilijk te achterhalen wie en waarom: *who dunnit and why?*

Bedrijfsrisico en staatsbelang

Ten tweede is staatsbetrokkenheid een complex vraagstuk. Onderzeese infrastructuur behoort doorgaans toe aan (een veelheid van) private commerciële bedrijven en is niet van een staat.[5] Er bestaan bedrijven die de infrastructuur monitoren, en er zijn kabel- en pijpleidingreparateurs. Bovendien is de infra gelegd in maritieme zones van verschillende staten. Normaliter zal een staat vooral betrokken zijn bij het uitbaten van de rechten kabels en pijpleidingen te mogen leggen en bij het opleggen van straffen. Het beschadigen van onderzeese infrastructuur zou mogelijk ook kunnen leiden tot aantasting van - of in het ergste geval een aanval op - vitale belangen van de staat. Maar dat is niet vanzelfsprekend. Naast dat lastig te bepalen is wanneer dat het geval is, is een andere vraag welke staat dat dan precies is: door wiens wateren de infra loopt, de staat onder wie het bedrijf valt, of de staat die afhankelijk is van de inhoud van de kabel of pijpleiding en de effecten van breuk ondervindt? Een kabel of pijpleiding heeft geen vlag of nationaliteit waardoor staten zich aangesproken kunnen voelen. Hier speelt dus het issue wanneer het commerciële belang van bescherming van onderzeese infrastructuur samengaat met het staatsbelang, waardoor objecten – bijvoorbeeld meer preventief – beschermd moeten worden.

Maritime meets cyber

Een derde uitdaging is dat onderzeese kabels en pijpleidingen het maritieme- en cyberdomein samenbrengt: de fysieke kabel op of in de bodem van de oceaan en de data die door de kabel stroomt. Het maritieme domein richt zich vooral op de fysieke bescherming van kabels en pijpleidingen, maar zegt niets over de inhoud ervan, of over kabels en pijpleidingen als inzet van interstatelijke spanningen of oorlogvoering. Een cyberoperatie zal de data of grondstoffenstroom raken, net zo goed als een fysieke kabel- of pijpleidingbreuk dat doet. Hoewel een fysieke kabelbreuk waarschijnlijk niet wordt beschouwd als een cyberoperatie of -aanval, liggen de gevolgen vooral ook in het digitale domein. De ernst zit vooral in de gevolgen die de samenleving mogelijk kunnen ontwrichten. In de context van de drie veiligheidsperspectieven is de vraag of een incident alleen vanuit de fysieke kant moet worden beschouwd of dat mogelijk sprake is van een (indirecte) cyberoperatie of aanval.

Het ingewikkelde van rechtsmacht op zee

Er bestaat regelgeving over onderzeese kabels en pijpleidingen. Al in 1884 kwam ter bescherming van onderzeese kabels de *Convention for the Protection of Submarine Telegraph Cables* tot stand. Het VN-Zeerechtverdrag (UNCLOS) kent voorts bepalingen over onderzeese kabels en pijpleidingen en heeft een gedeelte van de 1884 Conventie overgenomen. In essentie bepaalt het VN-Zeerechtverdrag wie in welke maritieme zones kabels en pijpleidingen mag leggen[6] en wie in welke gebieden rechtsmacht -regels maken, handhaven en rechtspreken- heeft over de infrastructuur. Het verplicht staten ook nationale wetgeving te maken om opzettelijke beschadiging strafbaar te stellen.[7]

In de 19e eeuw werd geopperd om moedwillige daden tegen onderzeese kabels en pijpleidingen onder universele rechtsmacht te laten vallen, zodat elke staat - net als piraterij - ertegen kon optreden.[8] Dat idee heeft het niet gered. Op zee kleeft daarom een aantal beperkingen aan de rechtsmacht van een kuststaat om regels vast te stellen en te handhaven. Ten eerste een geografische beperking. Rechtsmacht reikt in beginsel niet verder dan de territoriale zee, waarbinnen de kuststaat regels kan opstellen en handhaven ter bescherming van kabels en pijpleidingen.[9] In de tweede plaats kan daarbuiten wel opgetreden worden, maar in beperkte mate. Over kabels en pijpleidingen op het continentaal plat kent het VN-Zeerechtverdrag een ingewikkelde bepaling, op grond waarvan een kuststaat rechtsmacht kan uitoefenen over onderzeese infrastructuur die is aangelegd of gebruikt wordt in verband met de exploratie van het continentaal plat van die staat, of verband houdt met de werkzaamheden op onder meer kunstmatige eilanden en installaties die zich onder zijn rechtsmacht bevinden.[10] En als derde kunnen buiten de territoriale zee over personen of schepen slechts in beperkte mate andere vormen van rechtsmacht bestaan, zoals over de eigen onderdanen van een staat of wanneer het schip de vlag van de staat voert.[11] Nationale wetgeving moet daarbij dan wel mogelijkheden bieden om te sanctioneren. Het is echter voorstelbaar dat wanneer er geen specifieke wetten bestaan, algemene strafbaarstellingen zoals die van diefstal of vernieling van toepassing kunnen zijn.

Rechtsmacht op zee is dus een soort lappendeken. En als we deze in de context van de huidige hybride dreigingen plaatsen, verliest ze mogelijk verdere effectiviteit. Bij 'gewone' criminaliteit zullen staten geneigd zijn op te treden. Maar zal bij indirecte staatsgeleide acties een opdrachtgevende staat genegen zijn daders onder zijn rechtsmacht aan te pakken? Anders dan piraterij, waarover wereldwijd consensus bestaat dat hiertegen opgetreden moet worden, is de inzet op kabels en pijpleidingen als onderdeel van interstatelijke spanningen van een andere veiligheidsorde.

Naast strafrechtelijk optreden tegen moedwillige breuken, zijn over bevoegdheden van een staat op basis van het zeerecht nog twee punten van belang. In de eerste plaats is relevant dat in de territoriale zee handelwijzen van schepen die een gevaar voor de vrede, veiligheid of orde van de kuststaat vormen, en in het bijzonder gericht zijn op de verstoring van communicatiesystemen of andere voorzieningen of installaties van de kuststaat, niet stroken met onschuldige doorvaart.[12] De kuststaat mag daartegen maatregelen nemen die nodig zijn om doorvaart die niet onschuldig is te voorkomen.[13] Daarnaast is interessant dat de Conventie van 1884 toestaat dat staatsschepen - dus inclusief oorlogsschepen - een visitatierecht hebben ten aanzien van schepen die ervan verdacht worden een kabel te hebben gebroken. Het doel is de identiteit van vaartuig en personen te achterhalen met het oog op vervolging door het land wiens onderdanen het zijn of onder wiens vlag het vaart.[14] Maar omdat deze regel niet is opgenomen in het VN-Zeerechtverdrag, is het onduidelijk in hoeverre deze bevoegdheid rijmt met de regels over visitatie en onderzoek in dat verdrag, of deze regel een regel van gewoonterecht is, of dat de regel alleen tussen de verdragspartijen bij de Conventie van 1884 geldt.[15] En dat zijn er maar een veertigtal.

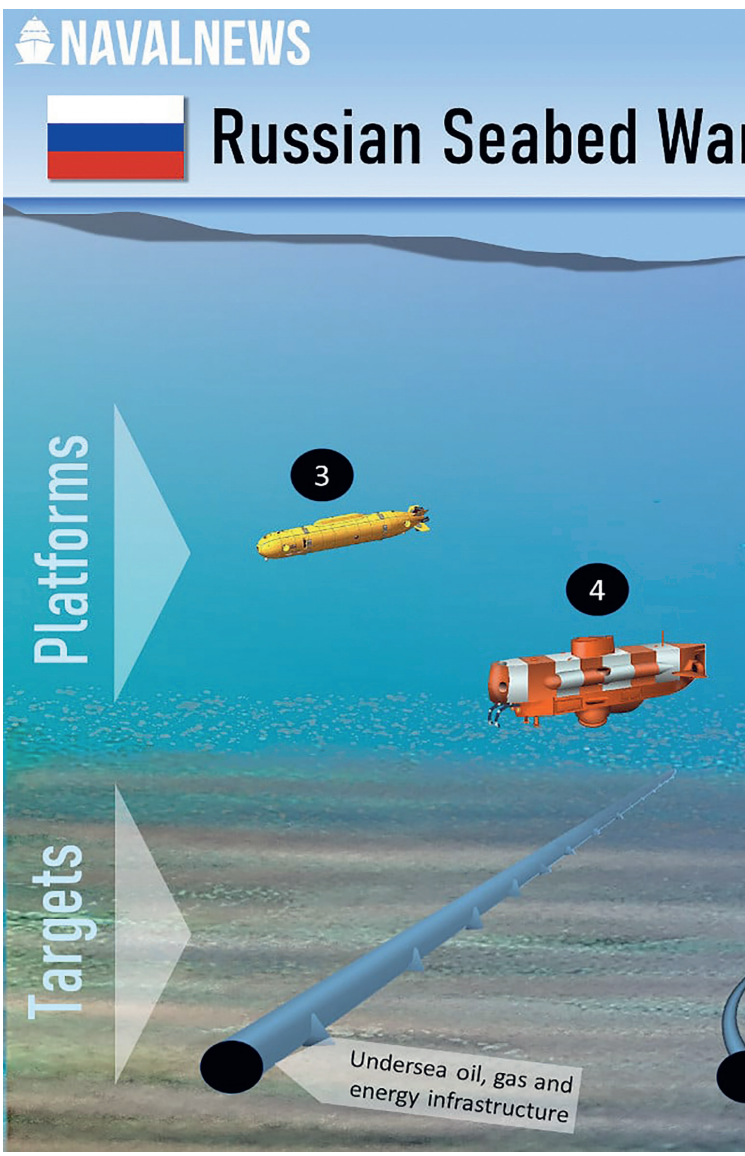
Een gewapende aanval?

De minister van Defensie gaf in najaar 2021 antwoord op de vraag of de Koninklijke Marine middelen beschikbaar heeft om datakabels te beschermen:[16]

Vraag 14: Welke capaciteiten heeft de Nederlandse marine om Nederlandse datakabels te monitoren en te beschermen, en in hoeverre worden deze capaciteiten daarvoor ingezet?
Antwoord 14: De Koninklijke Marine heeft op dit moment geen capaciteiten om Nederlands datakabels te monitoren en te beschermen. De Koninklijke Marine beschikt wel over capaciteiten (als fregatten, onderzeeboten en NH90 helikopters) voor indirecte datakabel bescherming en kan daarmee oppervlakte-eenheden en onderzeeboten detecteren, volgen en eventueel neutraliseren.
Interessant is de laatste zin over het vinden van oppervlakte-eenheden en onderzeeboten, en het 'eventueel neutraliseren' daarvan. De juridische context die hierin gelezen kan worden is geweld in het kader van (het verbod op) interstatelijk geweldgebruik. Met andere woorden, is met de actie sprake van een gewapende aanval en komt een staat het recht van zelfverdediging toe. En (/of) leidt de actie tot een conflict waarop het oorlogsrecht van toepassing wordt. Nog voor het *Nord Stream*-incident, meende de Britse *Chief of the Defence Staff* Admiral Sir Tony Radakin volgens een Britse krant dat het doorsnijden van onderzeese kabels een *act of war* zou kunnen zijn.[17] Hoewel de aandacht op het belang van bescherming van onderzeese kabels daarmee gevestigd wordt, is het lastig om te voldoen aan de criteria voor een gewapende aanval in geval van een kabelbreuk. Welke staat, of mogelijk *non-state actor,* heeft het gedaan en tegen welke staat is de aanval - op een doorgaans private commerciële kabel of pijpleiding, die mogelijk wel door de wateren van de kuststaat, maar niet naar de kuststaat loopt - gericht? Hoe wegen we de intensiteit van de aanval op de staat en hoe ernstig zijn de effecten van de schade? En als een staat zich eenmaal aangevallen voelt, volgt de vraag of een *militaire* reactie wel noodzakelijk en proportioneel is. Het *Nord Stream*-scenario leidde niet tot die constatering. Eventueel optreden blijft dan in de eerdergenoemde mogelijkheden van het zeerecht en strafrecht vallen.

Gewapend conflict

Bij het uitbreken van de Eerste Wereldoorlog liet Groot-Brittannië het kabelschip *Alert* de kabels tussen Duitsland en de VS en de Azoren doorsnijden.[18] De crew van het Duitse *SMS Emden* vernietigde de kabel op *Direction Island* in de Indische Oceaan, waarna het zich in een gevecht met *HMAS Sydney* moest overgeven.[19] Maar mogen oorlogvoerende partijen onderzeese kabels en pijpleidingen aanvallen of op een andere wijze onderbreken als methode van oorlogvoering? Of anders gesteld: zijn onderzeese kabels en pijpleidingen beschermde objecten tijdens een gewapend conflict? De Conventie van 1884 zegt dat 'de bepalingen dezer overeenkomst [strafbaarheid van kabelbreuk, *MDF*] geen inbreuk maken op de vrijheid van handelen van oorlogvoerenden.'[20] Het Haags Landoorlogsreglement (1907) stelt dat kabels tussen neutralen en bezet gebied in uiterste noodzaak mogen worden vernietigd en moeten worden hersteld wanneer de oorlog voorbij is.[21] Deze twee aanknopingspunten impliceren dat er geen absolute bescherming



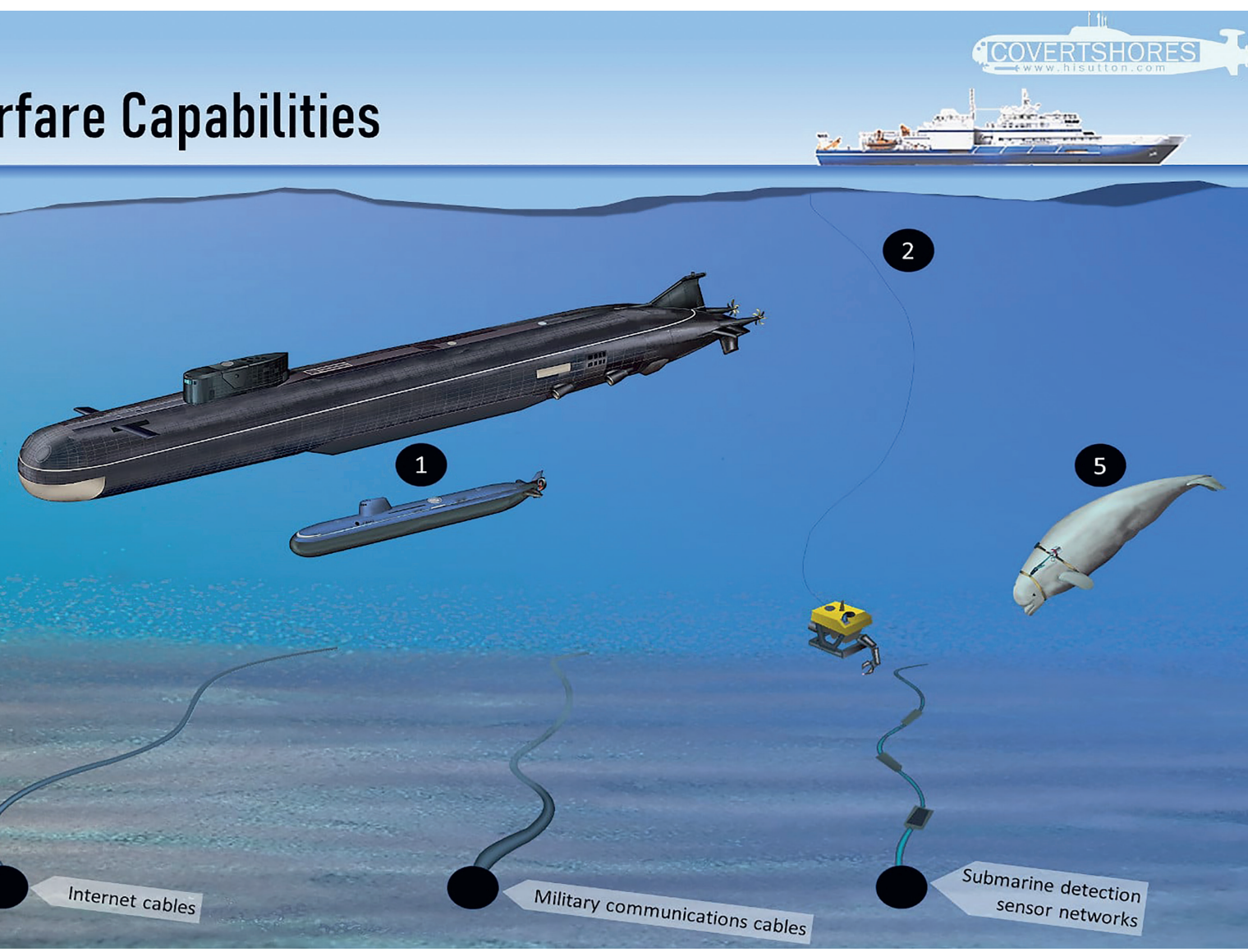
is voor kabels in oorlogstijd - waaronder kabels die naar neutrale staten gaan - en onder bepaalde omstandigheden doelwit mogen zijn.[22] Omdat het aantasten van onderzeese kabels tegenwoordig in het digitale tijdperk een enorme impact kan hebben, en ook op meerdere staten, is het de vraag of dit uitgangspunt nog houdbaar is. Maar over het algemeen vinden we het uitgangspunt dat een kabel doelwit mag zijn met meer of mindere mate van stelligheid in huidige juridische posities zowel in de fysieke als de cyberdimensie terug.[23]
Wanneer een onderzeese kabel inderdaad doelwit mag zijn, kan vernietiging ervan nog niet zomaar. Een aanval moet voldoen aan de *targeting*-regels: is de kabel een militair doel en is de verwachte nevenschade niet buitenproportioneel ten opzichte van het verwachte militaire voordeel van de aanval. In de tweede vraag zal met name het wegvallen van de data en de gevolgen ervan aan de orde zijn. Over pijpleidingen staat niets specifieks in het oorlogsrecht. Maar indien op dit vlak dezelfde positie kan worden ingenomen als kabels, valt een pijpleiding ook onder de *targeting*-regels in geval van een aanval.

Ten slotte

Tot meer dan flink opborrelen van het debat over de bescherming van onderzee kabels en pijpleidingen, interstatelijk vingerwijzen en groeiende zorg van activiteiten in de hybride omgeving, heeft het *Nord Stream*-incident voorlopig nog niet geleid. Deze bijdrage, die vooral aantoont hoe lastig de bescherming van onderzeese infrastructuur in de context van interstatelijke spanningen kan zijn, heeft slechts de oppervlakte aangestipt van enkele onderwerpen die met de bescherming van kabels en pijpleidingen gepaard gaan. Dit artikel beoogt de discussie over de bescherming van onderzeese kabels en pijpleidingen vanuit een juridisch perspectief wat structuur te bieden. Hierbij de eerste aanzet.[25]

KTZ (LD) mr. dr. Martin Fink is Universitair Hoofddocent Militair Recht aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie (NLDA).

Weergave van Russische onderwatercapaciteit met betrekking tot het benaderen, aftappen en/of vernietigen van onderzeese infrastructuur (H.I. Sutton, Covert Shores[24]).
1. Een 'host'-onderzeeër die een kleinere nucleaire onderzeeër kan lanceren voor bodemoperaties;
2. Het oceanografisch onderzoeksschip Yantar die diverse ROV's en AUV's (3) kan inzetten;
4. Reddingsboten die ook uitgerust kunnen worden voor bodemoperaties;
5. Getrainde zeezoogdieren waar Rusland mogelijk mee experimenteert.



Noten

1 https://www.navalnews.com/naval-news/2021/08/russian-spy-ship-yantar-loitering-near-trans-atlantic-internet-cables/
2 https://www.nytimes.com/2005/02/20/politics/new-nuclear-sub-is-said-to-have-special-eavesdropping-ability.html?_r=1
3 N. Morris, 'Operation Tempora: GCHQ in fresh snooping row as it eavesdrops on phones and the internet', *The Independent*, 22 juni 2013. https:// https://www.independent.co.uk/news/uk/politics/operation-tempora-gchq-in-fresh-snooping-row-as-it-eavesdrops-on-phones-and-the-internet-8669137.htmlbusinessam.be/knippen-russische-vissersschepen-onderzeese-kabels-door/
4 A. Bilal, 'Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote', in NATO Review, 30 november 2021. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html
5 D. R. Burnett, 'Submarine Cable Security and International Law', in *International Law Studies*, vol. 97 (2021), 1659-1682, 1668.
6 Zie artikel 58, 79(1) en 87 VN-Zeerechtverdrag.
7 Het gaat hier om opzet of grove onachtzaamheid. Zie artikelen 113-115 VN-Zeerechtverdrag.
8 J.P.A. Francois, *Grondlijnen van het Volkenrecht* (Tjeenk Willink, Zwolle, 1954), 540.
9 Art. 3 en 21 lid 1 onder c VN-Zeerechtverdrag.
10 Zie artikel 79 sub 4 VN-Zeerechtverdrag.
11 Art. 3 Wetboek van strafrecht.
12 Artikel 19 lid 1 en tweede lid, onder k VN-Zeerechtverdrag.
13 Artikel 25 VN-Zeerechtverdrag.
14 Zie artikel X 1884 Conventie.
15 Zie artikel 92 en 110 VN-Zeerechtverdrag.
16 Tweede Kamer, vergaderjaar 2021–2022, Aanhangsel, 4. Vragen van de leden Van Wijngaarden en Rajkowski (beiden VVD) aan de Minister van Defensie over het bericht «Minister Bijleveld en Admiraals Kramer en Tas uiten zorgen tijdens commando-overdracht (ingezonden 13 september 2021). Antwoord van Minister Kamp (Defensie) (ontvangen 4 oktober 2021).
17 H. Bone, 'Russian submarines cutting underwater cables is 'act of war', UK defence chief warns', in *The Mirror* januari 2022. https://www.mirror.co.uk/news/uk-news/russian-subs-cutting-underwater-cables-25889266
18 G. Corera, The UK's most senior military officer has warned of a new threat posed by Russia to communications and internet cables that run under the sea', in *BBC*, 15 December 2017. https://www.bbc.com/news/world-europe-42367551
19 E. Bruton, *From Australia to Zimmermann: A Brief History of Cable Telegraphy during World War One (2013).*
20 Artikel 15 Conventie van 1884.
21 Artikel 54 Landoorlogreglement 1907 stelt:
De onderzeese kabels die een bezet gebied met een neutraal gebied verbinden, mogen alleen in uiterste noodzaak worden ingenomen of vernietigd. Wanneer de vrede is gesloten, moeten ze ook worden teruggegeven en moet de compensatie worden geregeld.
22 James Kraska, The Law of Maritime Neutrality and Submarine Cables, EJIL:TALK! (July 29, 2020), https://www.ejiltalk.org/the-law-of-maritime-neutrality-and-submarine-cables/
23 Rule 91 (uitleg paragraaf 5) Tallin Manual. Maar zie ook het San Remo Manual over zeeoorlogsrecht (sectie 37) en het Oslo Manual over bijzondere oorlogsrechtelijke onderwerpen (67 t/m 69).
24 Zie: www.hisutton.com
25 Van interesse in deze context is een Working Paper (no. 5, Handbook on Maritime Hybrid Threats - 10 Scenarios and legal scans) uitgebracht door het Hybrid Centre of Excellence (COE) in november 2019.

CARTOON