Mr. A.J. Nagtegaal, dr. J.A. Kruit en dr. F.L. Stevens***

IMO Cyber Risk Management Resolution – óók relevant voor ladingbelanghebbenden

Scheepseigenaren en scheepsmanagers zijn sinds 1 januari 2021 verplicht om de cyberrisico's van hun schepen en organisaties in kaart te brengen, te beoordelen en zo nodig maatregelen te nemen in hun veiligheidsmanagementsystemen. Maar over welke risico's hebben we het dan? Welke verplichtingen worden nu opgelegd? Als niet voldaan wordt aan deze verplichtingen kan dat naast publiekrechtelijke sancties bovendien aansprakelijkheid naar ladingbelanghebbenden met zich meebrengen. De auteurs gaan in op rechtspraak waarin een gebrekkige naleving van de ISM Code een rol speelde bij de aansprakelijkheidsvraag.

1. Inleiding

De omvang en ernst van cyberrisico's zijn het afgelopen jaar sterk toegenomen. Onderzoeksrapporten laten een stijging zien van het aantal hacks en (maritieme) cyberinbreuken.[1] Het feit dat bedrijven mede als gevolg van COVID-19 steeds meer gebruikmaken van onlinesystemen en vaker op afstand werken is hier medeverantwoordelijk voor.[2] Maar ook voordat we het begrip 'anderhalve-meter-samenleving' ooit hadden gebruikt, stond cyber security al hoog op de agenda van de International Maritime Organisation (IMO). Al in juni 2017 heeft de IMO de *Cyber Risk Management Resolution* (hierna: de Cyber Resolution) aangenomen.[3] Op grond van deze resolutie zijn scheepseigenaren en scheepsmanagers onder de ISM Code verplicht om de cyberrisico's van hun schepen en organisaties in kaart te brengen, te beoordelen en zo nodig maatregelen te nemen in hun veiligheidsmanagementsystemen (*Safety Management Systems*, SMS).

Dat een adequaat veiligheidsbeleid met aandacht voor het managen van cyberrisico's niet alleen relevant is voor scheepseigenaren en scheepsmanagers, is evident. Een deugdelijk beleid voorkomt cyberaanvallen enerzijds en beperkt de gevolgen van eventuele aanvallen anderzijds. Daardoor neemt de kans op (aanzienlijke) schade, waaronder die aan of met betrekking tot de lading, af. Een cyberaanval kan immers leiden tot vertraagde aflevering van lading, al dan niet in beschadigde toestand. Ook kan de aanval directe schade aan de lading veroorzaken.

Uit de rechtspraak volgt dat gebrekkige naleving van de ISM Code tot aansprakelijkheid van de vervoerder kan leiden. Dat wordt in deze bijdrage toegelicht, aan de hand van uitspraken van respectievelijk het hof Amsterdam en het hof Arnhem-Leeuwarden. Ook de recente uitspraak van de Engelse Court of Appeal in de '*CMA CGM Libra*' komt daarbij aan de orde. Allereerst gaan we uitgebreid in op de verschillende concrete cyberrisico's en de inhoud van de Cyber Resolution. Daarna zal het juridisch kader van de ISM Code uiteengezet worden.

2. Cyberrisico's

Het begrip 'cyberrisico's' is nogal abstract. Welke risico's loopt een schip, althans haar scheepseigenaar of manager concreet op het gebied van cyber security?

In dit verband wordt doorgaans een onderscheid gemaakt tussen 'IT' (Information Technology) en 'OT' (Operational Technology). IT verwijst naar systemen die informatie (data) opslaan en verwerken om bedrijfsprocessen te ondersteunen of mogelijk te maken. Denk bijvoorbeeld aan het klantenbestand van de zeevervoerder, aan de software die bijhoudt waar containers zich bevinden, enz. OT verwijst naar (fysieke) systemen die een schip, een fabriek enz. tot een werkend geheel maken. Denk bijvoorbeeld aan het voortstuwingssysteem of het ballastsysteem van een schip. Heel veel van deze systemen worden aangestuurd door ingebouwde computers (*Programmable Logic Controllers*, PLC's). Aanvankelijk waren deze PLC's aparte, niet-verbonden eenheden, en was de OT- en PLC-markt quasi volledig gescheiden van de IT-markt. Deze scheiding is echter aan het verdwijnen, omdat steeds meer PLC's verbonden worden met het internet en met IT-systemen (*the Internet of Things*, IoT).

Verder kan een onderscheid gemaakt worden tussen de bedrijfsactiviteiten van de zeevervoerder aan land enerzijds, en het schip en de activiteiten aan boord van het schip anderzijds.

Het hoeft geen betoog dat ook aan land, in het (hoofd)kantoor van de scheepseigenaar of zeevervoerder, allerlei IT-systemen worden gebruikt die een impact kunnen hebben op de veiligheid van schip en lading. Dat gaat over systemen met informatie over de identiteit van afzender en ontvanger, de aard en het gewicht van de lading, werknemersgegevens, toegangscontrole, enz. Ook kan het beheerssystemen betreffen (bijvoorbeeld software om het onderhoud van de schepen te managen) en systemen die rechtstreeks invloed hebben

* **Aaron Nagtegaal en Jolien Kruit zijn beiden werkzaam als advocaat bij Van Traa Advocaten N.V. te Rotterdam.**
** **Frank Stevens is hoofddocent aan de Erasmus Universiteit Rotterdam en redacteur van dit tijdschrift.**

1. hellenicshippingnews.com/maritime-cyber-attacks-increase-by-900-in-three-years/; blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/; hongkongmaritimehub.com/shipping-subjected-to-400-increase-in-attempted-hacks/.
2. mmc.com/insights/publications/2020/march/cyber-risk-grows-as-covid-19-spreads.html;home.kpmg/ch/en/home/insights/2020/04/coronavirus-increased-forensic-and-cyber-risks.html.
3. IMO Resolution MSC.428(98), te downloaden op: imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

op de veiligheid (bijvoorbeeld beladingssoftware)[4]. Al deze systemen kunnen aangevallen worden, zowel door aanvallers die het specifiek op de scheepseigenaar of de zeevervoerder gemunt hebben als door 'algemene' malware die gericht is op elk kwetsbaar systeem, ongeacht van welk bedrijf. Het NotPetya-virus dat in 2017 grote problemen veroorzaakt heeft voor Maersk was bijvoorbeeld niet specifiek tegen Maersk gericht. Zijn de diverse componenten van de IT-infrastructuur (servers, netwerk, routers, enz.) voldoende beschermd tegen ongeoorloofde toegang?

Cyberrisico's blijven echter geenszins beperkt tot enkel gerichte of algemene aanvallen (cybercriminaliteit). Software is nooit perfect, en de manier waarop mensen met software omgaan is dat al evenmin. Vroeger hadden veel bedrijven hun eigen servers. Tegenwoordig wordt dit regelmatig uitbesteed en in 'the cloud' ondergebracht. Het cloudbedrijf moet dan zorgen voor de bescherming en de back-up van de gegevens. Hoe dikwijls controleert de scheepseigenaar of zeevervoerder of het cloudbedrijf inderdaad de beloofde back-ups maakt? Hoe vaak wordt gecheckt of de back-ups in geval van nood inderdaad teruggezet kunnen worden? In (sommige) software worden wel eens beveiligingsproblemen of -lekken ontdekt. Fabrikanten brengen dan een patch of een update uit, maar wat is het beleid van de scheepseigenaar of zeevervoerder met betrekking tot updates? Er wordt regelmatig vastgesteld dat IT-systemen nog steeds kwetsbaar zijn voor reeds lang gekende problemen, omdat de betrokken bedrijven de updates niet (tijdig) installeren. Anderzijds kan ook een update malware bevatten.[5] Verder draait software noodzakelijkerwijze op een Operating System. Er is een geval bekend waarin de ECDIS van een schip vastgelopen is doordat een software-update van de ECDIS niet compatibel bleek met het (verouderde) operating system.[6] Gevolg was dat de bemanning zich twee dagen lang moest behelpen met een papieren zeekaart. Cyber security is tegenwoordig een bekend begrip, maar beveiliging is een zeer gespecialiseerde en complexe materie, en vele softwareontwikkelaars kopen beveiligingsoplossingen of -componenten in van derden (bijvoorbeeld het hashing algoritme SHA256). In welke mate weten scheepseigenaren en zeevervoerders welke beveiligingscomponenten geïncorporeerd zijn in bijvoorbeeld de boekings- of beladingssoftware die zij gebruiken? Dit is niet zonder relevantie, omdat de ontwikkelingen op dit terrein zeer snel kunnen gaan en bepaalde toepassingen van vandaag al morgen achterhaald kunnen zijn. Asymmetrische cryptografie bijvoorbeeld, die onder meer gebruikt wordt bij digitale handtekeningen en om de integriteit van bestanden te garanderen, berust op zogenaamde 'eenrichtingsfuncties': een bewerking die in de ene richting heel gemakkelijk uit te voeren is, maar in de andere richting heel moeilijk. Een voorbeeld: het is voor een computer eenvoudig om twee (zeer grote) priemgetallen met elkaar te vermenigvuldigen, maar er bestaat momenteel geen snelle methode om het resultaat te ontbinden in factoren en zo de oorspronkelijke priemgetallen terug te vinden. Wordt een dergelijke methode morgen wel gevonden, dan verdwijnt op slag de zekerheid en de veiligheid die nu geboden wordt door deze vorm van cryptografie. Via welk kanaal en op welke termijn zou de scheepseigenaar of de zeevervoerder van dergelijke ontwikkelingen op de hoogte gebracht worden? En hoe zouden deze bedrijven daarmee omgaan? Hoeveel tijd en hoeveel moeite zou het hun kosten om over te schakelen op een ander softwarepakket? De manier waarop software wordt gebruikt is uiteraard ook niet zonder belang. Wachtwoorden zijn algemeen ingeburgerd als middel voor toegangscontrole, maar heeft het bedrijf een (deugdelijk) wachtwoordbeleid? Hoe complex moet een wachtwoord zijn? Om de hoeveel tijd moet het veranderd worden? Ten slotte, maar zeker niet in het minst, zijn er ook de werknemers die de IT-systemen gebruiken. Heeft bijvoorbeeld iedere werknemer van de scheepseigenaar of zeevervoerder toegang tot (potentieel) gevoelige informatie, zoals ladinglijsten of vaarschema's? Zou het systeem het merken als een onderhoudstechnicus plots ladinglijsten gaat consulteren en downloaden naar een externe locatie zoals een usb-stick? Hoe zou daarop dan gereageerd worden? Het voorgaande mag duidelijk maken dat cyberrisico's en cyberbeveiliging veel ruimer zijn en veel verder gaan dan 'alleen maar' de systemen beschermen tegen ongeoorloofde toegang.

Cyberrisico's spelen niet enkel aan land, maar ook aan boord van het schip. Vele schepen hebben tegenwoordig zelf ook IT-systemen aan boord (bijvoorbeeld software voor stabiliteitsberekeningen). Voor deze systemen geldt in essentie hetzelfde als voor de IT-systemen in de kantoren van de scheepseigenaar of zeevervoerder. Daarnaast hebben moderne schepen ook tal van OT-systemen aan boord. Scheepsmotoren, ballastsystemen, ladingpompen, branddetectie- en -bestrijdingssystemen, navigatieapparatuur, noem maar op. Al deze systemen worden in meerdere of mindere mate aangestuurd en gecontroleerd door (ingebouwde) computers en software. Vroeger stonden deze systemen op zichzelf; zij konden niet met de buitenwereld communiceren. Dit is echter tegelijk een voor- en een nadeel. Het voordeel is dat malware enkel in deze systemen geïntroduceerd kon worden door iemand met fysieke toegang tot deze systemen. Het nadeel is dat, als er een probleem wordt vastgesteld, het ook veel moeilijker is om updates of patches te installeren – voor zover de OT-fabrikanten überhaupt al patches uitbrengen. Tegenwoordig staan dergelijke OT-systemen veel vaker in connectie met andere systemen, met het internet, met de servers van de leverancier, enz. Dit creëert uiteraard nieuwe risico's en nieuwe uitdagingen voor de fabrikanten, vaak ook op niet voor de hand liggende manieren. Het schip kan bijvoorbeeld uitgerust zijn met een entertainmentsysteem voor de bemanning dat toegang heeft tot het internet om films, muziek e.d. te downloaden. Wanneer in dit systeem een beveiligingslek zit waardoor een aanvaller toegang kan krijgen, en het entertainmentsysteem vervolgens niet correct is afgescheiden van bijvoorbeeld het motormanagementsysteem, zou een aanvaller zich via het entertainmentsysteem toegang kunnen verschaffen tot het motormanagementsysteem. Mogelijk kan de aanvaller dan enkel informatie over de mo-

4. In 2018 bijvoorbeeld maakte het binnenschip 'Comienzo' tijdens het laden slagzij en verloor uiteindelijk veertig containers. Na analyse bleek dat de stuw- en stabiliteitssoftware die de schipper gebruikte fouten bevatte (zie het Jaarverslag Inspectie Leefomgeving Transport 2018, p. 43).
5. Een scenario waar de *BIMCO Guidelines on Cyber Security Onboard Ships* (onder 2.3) voor waarschuwen, te downloaden op: bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.
6. ECDIS staat voor Electronic Chart Display Information System. Via dit systeem kunnen elektronische zeekaarten geraadpleegd worden.

torprestaties zien (wat op zich in sommige omstandigheden al nuttige informatie kan zijn), maar het is ook mogelijk dat de aanvaller de controle over het systeem kan overnemen en bijvoorbeeld de bemanning kan beletten om vaart te minderen of de motor af te zetten. Ook hier zijn opzettelijke aanvallen echter niet het enige probleem. Een technicus die onderhoud moet verrichten op een systeem en daarvoor zijn laptop aansluit zou via die weg bijvoorbeeld onbewust en onbedoeld een virus in het systeem kunnen introduceren. Verder zijn OT-systemen, net als IT-systemen, vatbaar voor 'bugs' en softwarefouten. Dit probleem wordt verergerd door het feit dat schepen een (relatief) lange levensduur hebben en oudere schepen soms ook nog oudere (of zelfs ronduit verouderde) OT-systemen aan boord hebben.

Ten slotte zijn de IT- en OT-systemen aan boord van schepen soms ook afhankelijk van externe signalen. De navigatieapparatuur aan boord bijvoorbeeld verwerkt GPS-signalen, de AIS-signalen van schepen in de buurt, enz. Deze systemen zijn (momenteel) echter niet beveiligd, en een sterke lokale zender kan bijvoorbeeld de echte GPS-satellietsignalen verstoren of zelfs 'vervangen' door valse signalen en zo de navigatieapparatuur volledig misleiden (GPS spoofing). In de Golf van Aden en delen van de oostelijke en centrale Middellandse Zee zijn de meldingen daarover de afgelopen periode aanzienlijk gestegen.[7] In principe hoeft dit niet tot incidenten te leiden, omdat de bemanning kan terugvallen op alternatieve vormen van navigatie, maar daarvoor is wel vereist dat de bemanning zich (tijdig) realiseert dat er iets mis is en daar correct op reageert.

Verder beperken cyberrisico's zich niet tot enkel de scheepseigenaren en zeevervoerders en de schepen zelf. Schepen kunnen nu eenmaal niet permanent op zee blijven. Zij moeten regelmatig havens aandoen, naar een scheepswerf voor onderhoud, bunkers en voorraden innemen, enz. Al deze externe partijen gebruiken eveneens IT- en OT-systemen, die zelf ook op allerlei manieren kwetsbaar kunnen zijn. Het is niet moeilijk voor te stellen dat een gecompromitteerd systeem in een haven of een scheepswerf ook schade aan schip of lading kan veroorzaken.

Volledigheidshalve dient nog opgemerkt dat schepen tegenwoordig bemand zijn. Wanneer een IT- of OT-systeem vastloopt of slecht functioneert, dan zijn er mensen aan boord die minstens kunnen proberen om het probleem op te lossen. Wanneer in de toekomst autonome schepen in de vaart zullen komen wordt nog meer vertrouwd op technologie, en zullen de eisen – inbegrepen de beveiligingseisen – die aan deze technologie worden gesteld nog toenemen.[8]

Cyberbeveiliging is een zeer complexe, gespecialiseerde materie. Bovendien willen beveiligingsbedrijven hun kennis en ervaring vaak geheim houden, waardoor het voor de 'gewone' bedrijven (de gebruikers van beveiligingssoftware of -componenten) dikwijls moeilijk is om het kaf van het koren te scheiden. Ook is cyberbeveiliging (net als verzekering) een loutere kostenpost, waarvoor men niets tastbaars terugkrijgt: voor bedrijven die nog geen incident hebben meegemaakt lijkt elke euro uitgegeven aan verzekering of beveiliging weggegooid geld.

3. ISM Code en Cyber Resolution

De verwezenlijking van cyberrisico's kan onder meer leiden tot vertragingen, het beschadigen of verloren gaan van de lading en/of het missen van een tijdslot in de loshaven. Schade kan bestaan uit herstelschade voor de scheepseigenaar indien het schip en zijn systemen geïnfecteerd zijn met een virus. Anderzijds kan dit zich ook uitstrekken over de lading. Een voorbeeld is als reefer- (koel)containers door een virus of softwarefout niet meer correct functioneren en bovendien het probleem ook niet direct verholpen kan worden. Ook kunnen cyberaanvallen maatregelen ter beperking van schade en kosten noodzakelijk maken, die vervolgens worden gevorderd van ladingbelanghebbenden. Zo is denkbaar dat deze kosten worden omgeslagen in averij-grosse. Ook is mogelijk dat de hulpverlener een directe vordering op de belanghebbenden bij de geredde lading heeft voor hun bijdrage in het hulploon, zoals onder het Lloyds Standard Form of Salvage Agreement (LOF)[9] en onder Engels recht.[10]

Het hoeft dan ook niet te verwonderen dat de maritieme sector cyberincidenten en de gevolgen daarvan zoveel mogelijk wil voorkomen. Sinds 1998 moesten scheepseigenaren onder de ISM Code reeds een veiligheidsmanagementsysteem hebben. Sinds 1 januari 2021 moet dit veiligheidsmanagementsysteem conform IMO Resolution MSC.428(98) ook betrekking hebben op cyberrisico's.

De ISM Code is onderdeel van het SOLAS-verdrag, oftewel de *International Convention for the Safety of Life at Sea*.[11] Het SOLAS-verdrag wordt steeds aangepast om up-to-date te blijven en ook nieuwe risico's te adresseren. Zo ondergaat ook de ISM Code jaarlijks meerdere aanpassingen.

Het doel van de ISM Code is het creëren van een internationale standaard voor het veilige management en veilig opereren van schepen, alsmede voor het voorkomen van vervuiling van het mariene milieu. In dat kader schrijft de ISM Code werkwijzen voor en geeft het waarborgen die geïmplementeerd moeten worden tegen verschillende risico's. De ISM Code is van toepassing op verschillende categorieën passagiers- en vrachtschepen.[12] Binnen de Europese Unie wordt

7. skuld.com/topics/port/piracy/us-maritime-us-marad-updates-its-gulf-of-guinea-red-seagulf-of-aden-and-persian-gulf-security-advisories/; channel16.dryadglobal.com/gps-interference-and-jamming-on-the-increase.
8. Zie voor de mogelijke risico's voor (semi-)autonome schepen: vantraa.nl/nl/kennis/de-hackende-hulpverlener/.
9. Het LOF voorziet in een contractueel regime voor het hulploon van de hulpverlener. Zie ook: lloyds.com/resources-and-services/lloyds-agency/salvage-arbitration-branch/lloyds-open-form-lof.
10. Naar Nederlands recht heeft de hulpverlener slechts een vordering op de scheepseigenaar (art. 8:563 lid 3 BW).
11. Hoofdstuk IX van het SOLAS-verdrag.
12. Hoofdstuk IX, Voorschrift 2, van het SOLAS-verdrag: (hogesnelheids)passagiersschepen en olietankschepen, chemicaliëntankschepen, gastankschepen, bulkcarriers, hogesnelheidsvrachtschepen, overige vrachtschepen en booreenheden met een bruto tonnage van 500 of meer.

een aparte ruimere toepassingsmaatstaf gehanteerd.[13] Ook kan een scheepseigenaar zich vrijwillig onderwerpen aan de vereisten van de ISM Code.

De IMO Resolution on Maritime Cyber Risk Management (MSC.428(98)) is op zichzelf een zeer kort document. Er wordt eigenlijk enkel in gesteld dat het veiligheidsmanagementsysteem ook aandacht moet hebben voor cyberrisico's, en dat de bevoegde overheden er bij de jaarlijkse controles over moeten waken dat dit effectief het geval is. Op welke wijze cyberrisico's dan geadresseerd moeten worden staat op hoofdlijnen beschreven in de IMO 'Guidelines on Maritime Cyber Risk Management',[14] en in meer detail in 'The Guidelines on Cyber Security onboard Ships',[15] opgesteld door BIMCO en tien andere maritieme organisaties.[16]

Cyber risk management is een proces dat uit verschillende stappen bestaat. Een eerste stap is identificatie: de scheepseigenaar moet nagaan aan welke bedreigingen hij bloot staat, zowel van externe partijen (criminele hackers, activisten, enz.) als van interne partijen (bijvoorbeeld ontevreden werknemers), en moet nagaan wat de zwakke punten zijn van zijn IT- en OT-infrastructuur. De tweede stap bestaat erin te beoordelen, in het licht van wat uit het identificatieproces is gekomen, hoe groot het risico werkelijk is. Het is bijvoorbeeld mogelijk dat er een (theoretische) kwetsbaarheid in een bepaald systeem zit, maar dat het zo veel middelen zou kosten om daarvan gebruik te maken dat dit niet echt een realistische bedreiging is. De derde stap bestaat erin om detectie- en beschermingsmaatregelen op te zetten. De scheepseigenaar kan uiteraard pas iets doen als hij weet dat er zich een incident heeft voorgedaan of dat er pogingen daartoe werden gedaan, dus het monitoren van de systemen en het detecteren van vreemde of ongewenste activiteiten is van primair belang. Daarnaast moeten maatregelen genomen worden om de gevolgen van een eventueel incident zo beperkt mogelijk te houden. Stel dat een aanvaller binnendringt in de server van de scheepseigenaar, heeft hij dan alleen maar toegang tot de onderhoudsgegevens, of heeft hij dan meteen toegang tot alle mogelijke informatie op de server? De vierde stap is het bepalen hoe het bedrijf zal reageren ingeval zich een incident voordoet. Moet er bijvoorbeeld een back-upsysteem voor kritieke processen geïnstalleerd worden? Aan welke voorwaarden moet dit back-upsysteem voldoen?

De vijfde stap ten slotte is de stap die scheepseigenaren hopen nooit te moeten zetten: dit is het effectief omgaan met en reageren op een daadwerkelijk cyberincident. De systemen liggen plat: klanten kunnen geen boekingen meer plaatsen, de planning weet niet meer waar de containers zijn, de kapiteins kunnen geen bunkers meer bestellen en geen havengelden meer betalen, enz. Aan de hand van het Cyber Risk Management Plan zal de scheepseigenaar hier zo goed mogelijk mee moeten omgaan.

Na deze vijfde stap draait het proces weer door naar de eerste stap. Door een werkelijk cyberincident te beleven heeft de scheepseigenaar wellicht nieuwe informatie verkregen en nieuwe inzichten opgedaan over de weerbaarheid van zijn IT- en OT-systemen, die hij dan weer moet gebruiken om zijn Cyber Risk Management Plan aan te passen.

Het SOLAS-verdrag, en daarmee de ISM Code, betreft publiekrechtelijke regelgeving. Controle op de naleving vindt plaats door de vlaggenstaat en tijdens havenstaatcontroles.[17] Gebreken kunnen leiden tot detentie of boetes. Uit de rechtspraak volgt dat het niet voldoen aan de publiekrechtelijke vereisten ook privaatrechtelijke gevolgen kan hebben in de verhouding tussen de vervoerder en ladingbelanghebbenden.

4. Aansprakelijkheid vervoerder

Het in de praktijk doorgaans toepasselijke aansprakelijkheidsregime voor goederenvervoer over zee is het regime zoals neergelegd in de *Hague (Visby) Rules*. Dat regime kan verdragsrechtelijk gelden, maar ook op basis van implementatie in nationale wetgeving of door een contractuele incorporatie.

Onder de *Hague (Visby) Rules* is de zeevervoerder verplicht om voor en bij aanvang van de reis redelijke zorg te betrachten voor de zeewaardigheid van het schip. Ook moet hij tijdens de reis goed voor de lading zorgen.[18] Als een scheepseigenaar niet voldoet aan de cybersecurity-vereisten van de ISM Code, kan dat ertoe leiden dat hij niet aan zijn zorgverplichtingen voldoet en dus aansprakelijk is. Weliswaar is er voor zover ons bekend nog geen jurisprudentie over de Cyber Resolution. Desalniettemin laten de uitspraken over andere onderdelen van de ISM Code zien dat de naleving hiervan relevant is voor de beantwoording van de vraag of de vervoerder al dan niet aan zijn zorgverplichtingen naar ladingbelanghebbenden heeft voldaan. Rechtscolleges toetsen onder meer of het veiligheidsmanagementsysteem van het betreffende schip op orde is en is nageleefd en verbinden daar gevolgen aan. De publiekrechtelijke regeling werkt dus door in het civiele recht. Als publiekrechtelijke veiligheidsnormen niet zijn nageleefd, kan dat betekenen dat het schip daardoor niet zeewaardig was en de vervoerder dus aansprakelijk is tegenover ladingbelanghebbenden.

De aansprakelijkheid van de zeevervoerder ten gevolge van een gebrekkige naleving van de ISM Code zal hierna behandeld worden aan de hand van jurisprudentie van het hof Amsterdam en van het hof Arnhem-Leeuwarden. De uitspraak van het hof Arnhem-Leeuwarden zal samen behandeld worden met de recente uitspraak van de Engelse Court

13. Verordening (EG) 336/2006 inzake de implementatie van de Internationale Veiligheidsmanagementcode in de EU.
14. MSC-FAL. 1/Circ.3 van 5 juli 2017, te downloaden op: imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.
15. Te downloaden op: bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.
16. Ook wordt een handzaam overzicht van de door scheepseigenaren en scheepsmanagers te nemen maatregelen en de risico's waartegen zij dienen gegeven in een rapport van Inmarsat over Cyber Security en IMO 2021. Te downloaden op: inmarsat.com/en/insights/maritime/2020/imo-2021-cyber-requirements.html.
17. Vgl. Wet Havenstaatcontrole en de Regeling Havenstaatcontrole.
18. Art. III HVR.

of Appeal in '*CMA CGM Libra*'.[19] Ook zal gekeken worden naar wat beide uitspraken voor ladingbelanghebbenden betekenen in geval van ladingschade door een cyberincident.

i. *S&S* 2009/102 (*Egelantiersgracht*)[20]
Tijdens het vervoer onder cognossement van België naar Venezuela ontstaat schade aan de lading ten gevolge van een brand aan boord van het schip. Uit het rapport van de gerechtsexpert bleek dat ten tijde van het uitbreken van de brand enkele veiligheidsvoorschriften niet zijn nageleefd door de bemanning tijdens laswerkzaamheden. Dergelijke voorschriften zijn vereist onder het veiligheidsmanagementsysteem van de ISM Code.

Ladingbelanghebbenden betogen dat de vervoerder vóór aanvang van de reis onvoldoende zorg heeft betracht voor de zeewaardigheid van het schip en dat de vervoerder bovendien persoonlijke (eigen) schuld zou hebben aan de brand. Hierover oordeelde het hof: 'Het enkele feit dat ten tijde van de brand toepasselijke (veiligheids)voorschriften niet zijn nageleefd, wettigt een zo vérstrekkende gevolgtrekking niet.' Het feit dat het schip ISM-gecertificeerd was speelde hierbij een rol. De naleving van de ISM Code was jaarlijks gecontroleerd en bevestigd. Uit de gerechtsexpertise volgde bovendien dat er voldoende aandacht was besteed aan de te nemen veiligheidsmaatregelen. Daarom kon niet worden vastgesteld dat onvoldoende zorg voor de zeewaardigheid van het schip vóór aanvang van de reis was betracht. Hierdoor stond een beroep op de excepties uit artikel 8:383 lid 2 BW, althans artikel IV lid 2 HVR, open voor de vervoerder.

In deze zaak werd gesteld dat de vervoerder onvoldoende zorg had aangewend voor het zeewaardig maken van het schip. Dit kan leiden tot de aansprakelijkheid van de scheepseigenaar of scheepsmanager. Ook een incompetente bemanning kan ertoe leiden dat de vervoerder niet voldaan heeft aan zijn verplichting tot het betrachten van redelijke zeewaardigheidszorg. Bij een cyberincident zou dat kunnen betekenen dat de bemanning niet juist heeft gehandeld ter voorkoming of beperking van de schade. Dat leidt echter niet steeds zonder meer tot aansprakelijkheid. Het gaat erom of de zeewaardigheid van het schip in het geding was en dit tot schade heeft geleid. In dat kader is van belang of de bemanning de juiste training heeft gekregen en zij bekend is met de veiligheidsprotocollen in geval van een cyberincident.[21] Een expertiseonderzoek zou uit kunnen wijzen dat hier vóór aanvang van de reis al geen sprake van was. Dan kan dat betekenen dat de vervoerder niet aan zijn verplichtingen heeft voldaan en hem geen beroep toekomt op enige exceptie uit artikel 8:383 lid 2 BW, althans artikel IV lid 2 HVR.[22]

ii. *S&S* 2017/27 ('*Harns*')[23] en '*CMA CGM Libra*'[24]
In zowel de '*Harns*' als de '*CMA CGM Libra*' was sprake van een stranding ten gevolge van gebrekkige nautische documentatie aan boord. Onderdeel van het veiligheidsmanagementsysteem is dat erop wordt toegezien dat alle geldende regelgeving wordt nageleefd. Op grond van het SOLAS-verdrag geldt de verplichting om relevante en bijgewerkte nautische kaarten aan boord te hebben.[25] Deze ontbraken in de *Harns*-zaak, zo stelde het hof Arnhem-Leeuwarden in navolging van de rechtbank vast.

In de zaak *CMA CGM Libra* werd in diverse 'Notices to Mariners' gewaarschuwd voor niet in kaart gebrachte ondieptes. Deze waren echter niet opgenomen in het vereiste 'passage plan' van het schip en waren evenmin vermeld op de gebruikte nautische kaarten. De noodzaak van een dergelijk 'passage plan' volgt uit de IMO 'Guidelines for voyage planning'.[26]

Deze gebreken leidden in beide gevallen tot het oordeel dat de vervoerder met deze schending van zijn zorgplicht de schade had veroorzaakt.

Indien de navigatiesystemen door een cyberincident buiten werking zijn gesteld, kan dat een schending van de zeewaardigheidszorgverplichting opleveren. Enerzijds bijvoorbeeld als er geen back-up- (papieren) zeekaarten aan boord zijn. Anderzijds als het virus al vóór aanvang van de reis de systemen van het schip was binnengedrongen of blijkt dat de beveiliging van de systemen dermate gebrekkig was dat het in feite wachten was op een incident tijdens de reis. Het schip was dan in beginsel niet in staat om de goederen in dezelfde deugdelijke staat veilig te vervoeren.

Concluderend toont het voorgaande aan dat het niet voldoen aan de publiekrechtelijke vereisten van de ISM Code en het hebben van een ongetrainde bemanning onder bepaalde omstandigheden kan betekenen dat onvoldoende zorg voor de zeewaardigheid van het schip vóór aanvang van de reis in de privaatrechtelijke verhouding tussen vervoerder en ladingbelanghebbende was betracht. Als daar inderdaad sprake van is, is de scheepseigenaar in beginsel aansprakelijk. Ons inziens zal dit, zoals de gegeven voorbeelden al kort aanstipten waarschijnlijk niet anders zijn in het kader van ISM-verplichtingen die voortvloeien uit de nieuwe IMO Cyber Resolution. Steeds zal concreet getoetst moeten worden.

5. Conclusie

In deze bijdrage is slechts een klein deel van de cyberrisico's waaraan een schip zoal kan worden blootgesteld benoemd. De verschillende internationale 'Guidelines on Cyber Security Onboard Ships' bevatten een meer uitgebreide uiteenzetting van deze risico's. Onder de ISM Code moeten scheeps-

19. Alize 1954 & Anor v Allianz Elementar Versicherungs AG & Ors [2020] EWCA Civ 293 (4 maart 2020). De Supreme Court heeft inmiddels leave for appeal aan Owners verleend.
20. Hof Amsterdam 11 oktober 2007, *S&S* 2009/102 (*Egelantiersgracht*).
21. K. Tam, K. Moara-Nkwe & K. Jones, 'The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training', *Maritime Technology and Research* (3) 2020, afl. 1.
22. Artikel 8:383 lid 2 BW, althans artikel IV lid 2 HVR.
23. Hof Arnhem-Leeuwarden 27 september 2016, *S&S* 2017/27 (*Harns*).
24. Alize 1954 & Anor v Allianz Elementar Versicherungs AG & Ors [2020] EWCA Civ 293 (4 maart 2020).
25. Voorschrift 27 van hoofdstuk 5 van het SOLAS-verdrag.
26. In te zien op: puc.overheid.nl/nsi/doc/PUC_1462_14/1/.

eigenaren en operators daar sinds 1 januari 2021 verschillende waarborgen tegen implementeren. Mocht onverhoopt toch ladingschade ontstaan als gevolg van een cyberincident, dan kan dat betekenen dat zij hun verplichtingen niet juist hebben nageleefd. In dat geval kunnen scheepseigenaren ook privaatrechtelijk aansprakelijk zijn. Informatievergaring in een vroeg stadium is dan van groot belang.