Schriftelijke inbreng Digitale Weerbaarheid - Havenbedrijf Rotterdam N.V.

Geachte leden van de vaste commissie voor Digitale Zaken,

Met deze position paper deelt het Havenbedrijf Rotterdam (HbR) haar standpunten ter voorbereiding van de rondetafel sessie Digitale weerbaarheid van 6 september 2022. Daarbij schetsen wij de context waarin HbR en de bedrijven in de Rotterdamse haven opereren, ons perspectief op de digitale weerbaarheid in de haven en dragen wij onze standpunten aan op de vooraf aangeleverde vragen.

Het doel van HbR is de versterking van de concurrentiepositie van de Rotterdamse haven als logistiek knooppunt én industriecomplex van wereldniveau. Niet alleen in omvang, maar ook in kwaliteit. De kerntaken van het HbR zijn de duurzame ontwikkeling, beheer en exploitatie van de haven, het handhaven van de vlotte en veilige afhandeling van de scheepvaart en het ondersteunen van de toekomst-bestendigheid van de Rotterdamse haven. De Rotterdamse haven huisvest ca. 3000 bedrijven en biedt aan werkgelegenheid (direct en indirect) 565.000 arbeidsplaatsen in Nederland.
De bedrijven zijn sterk met elkaar verbonden in de logistieke ketens. Tegenwoordig zijn ze niet alleen in het fysieke proces nauw met elkaar verbonden maar ook steeds meer digitaal. Denk daarbij aan data-uitwisseling met betrekking tot actuele weersomstandigheden, infrastructuurdata uit de haven zoals de bezettingsgraad, transportdata zoals aankomsttijden van schepen bij terminals of andere modaliteiten of logistieke data zoals bijvoorbeeld transportdocumenten van logistieke partijen. In de logistieke ketens wordt deze informatie-uitwisseling tussen partijen steeds belangrijker en processen en systemen worden efficiënter, maar tegelijkertijd ook afhankelijker van goede informatie.

Helaas zien we dat ook de dreiging op een cyberaanval toeneemt, de strategische rol van de Rotterdamse haven voor Nederland en Europa maakt haar tot een strategisch doelwit voor statelijke actoren of andere kwaadwillenden. Een cyberaanval kan ervoor zorgen dat (kritieke) systemen van bedrijven in de haven, waaronder die van HbR, uitvallen en informatie niet beschikbaar en/of betrouwbaar is voor het bedrijf zelf en anderen. Dit verstoort de logistieke ketens en scheepvaartafwikkeling en zorgt mogelijk voor risico's op het gebied van veiligheid (incidenten en integriteit), bereikbaarheid (congesties) en het imago van de betrouwbaarheid van de haven als geheel. De mate van digitale weerbaarheid van de bedrijven verschilt sterk en dat maakt de ketens als geheel kwetsbaar. Gezien de toenemende digitale onderlinge verbondenheid van en tussen bedrijven en de toenemende dreiging van een cyber aanval, vormt cyber dus een reëel risico voor de continuïteit van de Rotterdamse haven.

Van de 3000 bedrijven in de Rotterdamse haven zijn er slechts een aantal aangemerkt als vitaal. Dat betekent dat bijna alle andere partijen die een essentieel onderdeel vormen van de haven, op dit moment niet vallen binnen de scope van de huidige WBNI. Zij staan dus niet onder een vorm van toezicht op het gebied van cyber en hebben dan ook geen toegang tot de dreigingsinformatie die in het Nationaal Detectie Netwerk (NDN) vanuit de overheid wordt uitgewisseld. Dit zorgt ervoor dat partijen niet weten waar zij aan moeten voldoen om hun digitale weerbaarheid op orde te hebben, de digitale weerbaarheid vaak te laag op de agenda staat en zij niet of lastig kunnen acteren op actuele dreigingsinformatie.

<u>Standpunten op de vragen:</u>

1. Is het voor een specifieke organisatie die getroffen wordt door bijvoorbeeld een cyberaanval ook duidelijk welke crisisstructuur er is en wat verwacht wordt?
   Er is een Nationaal Crisisplan Digitaal met daarin een beschrijving van de crisisstructuur en wat er wordt verwacht. HbR vertegenwoordigt het vitale proces afwikkelen scheepvaartverkeer in de ICT response board. Hier vindt de afstemming plaats tussen enerzijds de impact van de crisis op een sector en anderzijds de toetsing van impact van een voorgestelde maatregel met een sector. In aanvulling op het Nationaal Crisisplan Digitaal is er voor de haven van Rotterdam een decentrale crisisaanpak ontwikkeld die past binnen de landelijke aanpak. Deze begint regionaal op het niveau van een getroffen bedrijf en loopt op tot de landelijke crisisstructuur (na gelang de aard en omvang van het incident).

2. Hoe wordt er gehandeld bij een cyberincident?
   Wanneer een cyberincident zich voortdoet bij een bedrijf, kan het bedrijf dat melden bij het Haven cybermeldpunt. Deze is bestemd voor alle bedrijven in het Rotterdams haven- en industriegebied. Er

geldt een meldplicht voor bedrijven die vallen onder de havenbeveiligingswet of een havenbeveiligingscertificaat bezitten. Voor HbR geldt dat bij een cyberincident we het hierboven beschreven crisisplan volgen. Afhankelijk van de aard en omvang van het incident of dat deze mogelijk het vitale proces raakt, meldt HbR in overeenstemming met het bedrijf het cyberincident bij het NCSC. Het NCSC fungeert als het expertisecentrum en informatieknooppunt voor cybersecurity binnen de Nederlandse overheid en bemannen onder andere een 24/7 meldpunt voor cyberincidenten (NCSOC). Bij een eventuele dreiging of aanval kan het NCSC hulp bieden in de vorm van: expertise en advies, analyse van het probleem en de inzet van gespecialiseerde responsmedewerkers. Bij cybercrises kan vanuit het NCSC een adviesorgaan ten behoeve van de nationale crisisstructuur worden geactiveerd: de ICT response board (IRB). In de IRB komen vitale partijen uit het cyberdomein bijeen om advies te geven over te nemen maatregelen. De IRB fungeert enerzijds als schakelpunt tussen technisch en bestuurlijk niveau, en anderzijds als schakelpunt tussen het bedrijfsleven en de overheid. De IRB wordt gefaciliteerd door het NCSC en voorgezeten door het ministerie van Economische Zaken.

Wanneer een (cyber)incident in de haven gevolgen heeft voor de openbare orde en veiligheid, zal de veiligheidsregio naar aard en omvang van het incident ook opschalen en de crisisaanpak coördineren voor wat betreft OOV-taken. Het bevoegd gezag van de veiligheidsregio is de (regio)burgemeester. Als de veiligheidsregio is opgeschaald zal het HCT informatie uitwisselen en de maatregelen afstemmen.

3. Welke lessen hebben cyberoefeningen (bijvoorbeeld ISIDOOR) opgeleverd en hoe wordt daardoor mee omgegaan?
   Wij zien dat cyberoefeningen voordelen opleveren op een aantal aspecten:
   - Het helpt in het leggen van sociale relaties (in de koude fase) en het creëren van vertrouwen die nodig is in de warme fase.
   - Het geeft inzicht in de complexiteit van de bedrijfsprocessen en het bijhorende IT-landschap.
   - Tegelijkertijd legt het ook de kwetsbaarheid in Nederland bloot, hoe gaan we om met het beperkte cyber specialisme bij een grootschalige calamiteit.

4. Wat zijn nog belangrijke zorgpunten?

   - <u>Huidige- en toekomstig organisatie van het cybertoezicht</u>

De beperkte scope van de huidige WBNI levert de al eerdergenoemde zorgpunten op voor de digitale weerbaarheid van de bedrijven in de Rotterdamse haven. Door de komst van het Europese NIS2 Directive wordt deze scope wel verbreed, maar loopt deze (logischerwijs) achter op de actualiteit. Voor de bedrijven in de haven geldt dat zij nu al te maken hebben met verschillende toezichthouders die ieder voor zich met beperkte kennis van zaken (onderdelen) van cyber onderzoeken. Ook komt er een voor de toezichthouders een grote hoeveelheid bedrijven bij naast hun huidige werkzaamheden. HbR is voorstander van het organiseren van een samenhangende vorm van cybertoezicht. Hierdoor kan de kwaliteit van het cybertoezicht worden verhoogd en de (administratieve) lasten voor bedrijven worden verlaagd. Een onderdeel hiervan is het opstellen van een gemeenschappelijk normenkader door toezichthouders, waarmee de gezamenlijke hoogte van de ‘lat’ van de digitale weerbaarheid wordt bepaald.

   - <u>Nationale regie bij een grootschalige calamiteit</u>

Zorgen zitten ook bij hoe we in Nederland omgaan met het beperkte cyber specialisme bij een grootschalige calamiteit. Veel van de expertise en kennis is aanwezig bij commerciële bedrijven. Hoe zou de overheid daar over kunnen beschikken wanneer nodig en wie coördineert de inzet hiervan tijdens een crisis? Is er een crisisplan of model die verschillende niveaus van vitaal onderscheidt en een organisatie die de regie neemt waar de middelen en cyberexperts op worden ingezet: wat wordt als eerste hersteld en wat als laatste. Dit is bijvoorbeeld wel aanwezig bij de huidige watercrisis waar het managementteam watertekorten (MTW) de verdeling van water onder sectoren/gebruikers landelijk coördineert.

   - <u>Vitale infrastructuur en (buitenlandse) afhankelijkheden</u>

Meer dan in andere landen is er in Nederland een sterke afhankelijkheid van technologie en buitenlandse leveranciers, wat voor risico’s zorgt met betrekking tot leveringszekerheid en continuïteit. Hierop zou specifiek beleid opgemaakt moeten worden vanuit de overheid. Zo moet er rekening gehouden worden met de lange termijn capaciteit en kwaliteitsgaranties van digitale infrastructuur die de bedrijven in de haven gebruiken om missie kritische toepassingen op te bouwen. Daarnaast zijn veel vitale processen in hoge mate afhankelijk van Amerikaanse Cloud aanbieders.