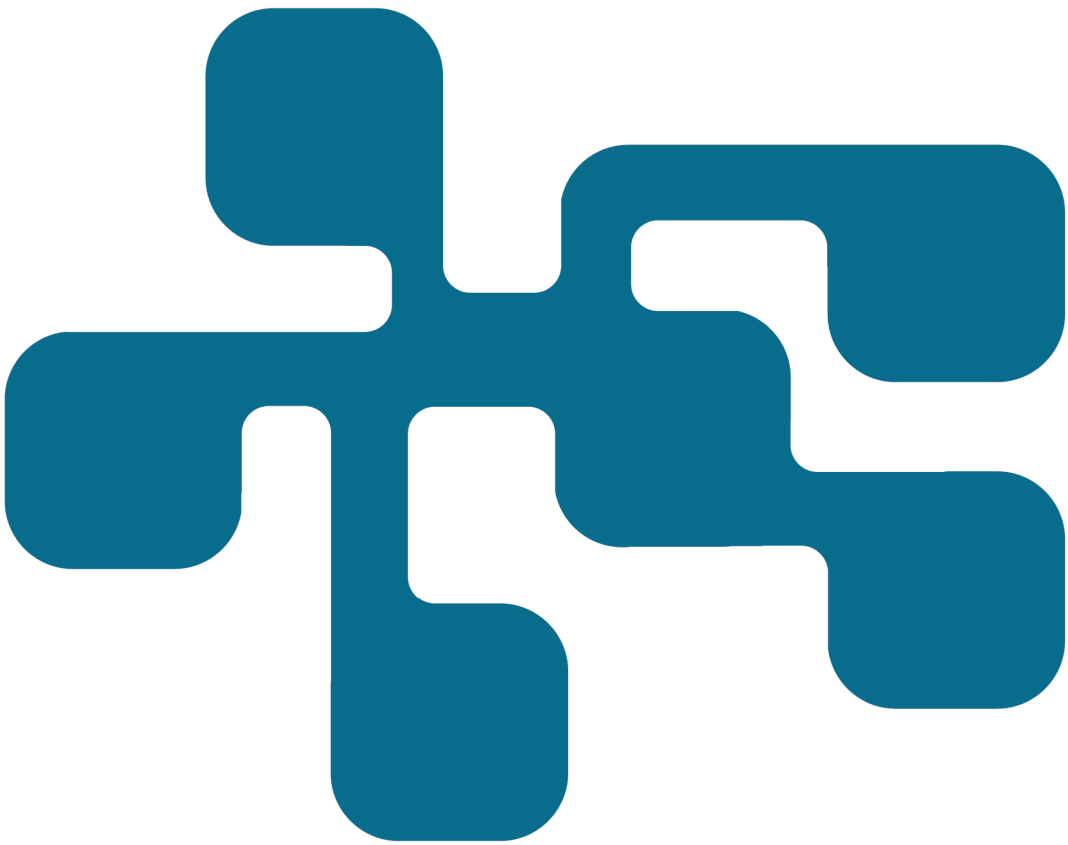
NCS3 – Ett skepp kommer lastat

En kartläggning av informationsflöden, cyberfysiska system och aktörer inom svenska hamnar

Mari Olsén, Christian Valassi,
Ann-Sofie Stenérus Dover

FOI
MSB



FOI-R--5405--SE
MSB 2022-06361
ISSN 1650-1942

Januari 2023

Mari Olsén, Christian Valassi,
Ann-Sofie Stenérus Dover

NCS3 – Ett skepp kommer lastat

En kartläggning av informationsflöden, cyberfysiska system och aktörer inom svenska hamnar

Titel	NCS3 – Ett skepp kommer lastat
Title	NCS3 – A ship comes loaded
Rapportnr	FOI-R--5405--SE
Månad	Januari
Utgivningsår	2023
Antal sidor	58
ISSN	1650-1942
Uppdragsgivare	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr	E13838
Godkänd av	Malek Finn Khan
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Hamnar är en kritisk nod i transportsystemet där många olika aktörer och godsflöden möts. Syftet med denna studie är stödja Myndigheten för samhällsskydd och beredskap med underlag för att stärka skyddet av samhällsviktig verksamhet. Detta görs genom en översiktlig kartläggning av aktörer, informationsflöden och cyberfysiska system av vikt för godsflödet i svenska hamnar. Vidare beskrivs läget avseende digitalisering samt en översiktlig bedömning av mognadsnivån avseende cybersäkerhetsarbetet. Datainsamlingen har primärt genomförts via intervjuer med olika hamnaktörer och myndigheter.

Studien visar att mängden cyberfysiska system inom hamnar är begränsade och att informationsflödet är fragmenterat. En viss typ av information samlas i gemensamma system medan annan information skickas via mail mellan olika aktörer. Detta gör att hamnaktörerna själva bedömer att det finns få system som är så pass kritiska att en attack mot dessa skulle stoppa godsflöden helt även om hanteringen skulle gå långsammare. Samtidigt har digitaliseringen fått ökat utrymme vilket på sikt kommer att kunna effektivisera såväl godshantering som utbyte av information men också riskera att öka sårbarheten. De hamnaktörer som deltagit i studien har de senaste åren ökat sitt arbete kring cybersäkerhet och det finns en vilja hos respektive hamns ledning att arbeta med frågorna. Dock ligger deras främsta fokus avseende säkerhet i hamnar framförallt på det fysiska skyddet.

Nyckelord: Hamnar, cybersäkerhet, informationsflöden, cyberfysiska system, digitalisering

Summary

Sea ports are a critical node in the transport system, where many different types of actors and freight goods meet. The objective of this study is to provide additional grounds to the Civil Contingency Agency in their work with cyber security for critical infrastructure. This is carried out through an overview of actors, informations flows and cyber-physical systems of importance for the flow of freight goods. Further, a brief overview of digitalisation and an assessment of cyber security maturity is presented. Data collection for this study has primarily been carried out via interviews with various port actors and authorities.

The results of the study shows that the amount of cyber-physical systems within ports is still limited and that the flow of information is fragmented. Certain types of information are collected in joint systems, while other types are sent via email between different actors.

Rudimentary solutions that are not reliant on complex and automated flows of information is perhaps why Port operators assess that there are few systems that are so critical that an attack on them would stop the flow of goods. At the same time, digitization is on the rise, which in the long term will allow for streamlining both handlig of goods and exchange of information. The port operators who participated in the study have expanded their work related to cyber security during the resent years. There also seems to be a willingness to work on cyber security-related issues on part of management. At the same time, focus on security in ports is still focused on physical security.

Keywords: Sea ports, cyber security, information flows, cyber-physical systems, digitization.

Innehållsförteckning

1 Inledning

Sjöfartstransport utgör det i särklass viktigaste transportslaget för den internationella handeln. World Economic Forum uppskattar att så mycket som 90 procent av all världens gods transporteras via sjöfart (Nagurney, 2021). Samma siffra gäller även för import och export av gods till och från Sverige (Sjöfartsverket, 2015). I svenska hamnar hanterades 186 miljoner ton gods under år 2021, 86 % av detta rörde utrikes gods (Trafikanalys, 2021).

Den centrala byggstenen för sjötransport är, förutom fartygen, de hamnar som hanterar gods och transport av människor. Hamnar och hamnverksamhet är därmed att betrakta som samhällsviktig verksamhet då de utgör en viktig funktion för att tillgodose samhällets behov av flera viktiga varor.

Mycket i dagens samhälle har digitaliserats eller är i färd med att digitaliseras och hamnar är inget undantag. Hamnar är idag beroende av IT- och OT[1]-relaterade system för att upprätthålla sin funktion och för att vara konkurrenskraftiga (ENISA, 2019). IT- och OT-system kan dock vara sårbara för cyberangrepp och behöver därför tillges adekvat skydd i syfte att minska risken för framgångsrika angrepp. Det finns flera kända exempel på framgångsrika cyberangrepp mot hamnar och hamnverksamhet. Dessa angrepp har bland annat underlättat smuggling av narkotika och stöld av gods men har i andra fall resulterat i att hamnverksamheten helt stannat av. Sådana angrepp leder till stora förseningar och en bred ekonomisk påverkan inte bara på de företag som angripits utan även i flera led i försörjningskedjan. Framgångsrika angrepp har potential att ge ännu värre konsekvenser som kan påverka hela länders import och export. Förutom direkta ekonomiska konsekvenser kan tillförseln av råvaror i olika sektorer påverkas, vilket i sin tur kan få konsekvenser för produktion och distribution av livsnödvändiga produkter.

Med ovanstående som grund är det av vikt att undersöka svenska hamnar i syfte att skapa en lägesbild för hur hamnarna arbetar med och hanterar cybersäkerhetsfrågor.

1.1 Syfte och mål

Totalförsvarets forskningsinstitut (FOI) har inom ramen för Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) fått i uppdrag av Myndigheten för samhällsskydd och beredskap (MSB) att kartlägga de system och

[1] OT eller operativ teknik (eng. Operational Technology) avser datorsystem och enheter som styr och övervakar industriella eller fysiska processer eller funktioner.

aktörer som finns i svenska hamnar samt hur den generella cybersäkerhetsmognaden ser ut. Syftet med uppdraget är att stödja MSB i deras arbete att stärka skyddet för samhällsviktigt verksamhet.

Studien avser besvara följande frågeställningar:

1. Vilka informationsflöden är viktiga för att godsflödet ska fungera genom hela hamnområdet från väg/järnväg, via förvar/lastning/omlastning till sjöfart?
2. Vilken typ av cyberfysiska system är nödvändiga för att godsflödet ska fungera?
3. Vilka hamnaktörer, myndigheter och regelverk är centrala i fråga om informations- och cybersäkerhet?
4. Vilket genomslag har digitaliseringen fått hos de hamnaktörer/system som identifierats i svenska hamnar och hur ser en sannolik utveckling ut framöver?
5. Hur ser digitaliseringen ut i internationella hamnar?
6. Vilken cybersäkerhetsmognad finns hos de hamnaktörer/system som identifierats i svenska hamnar?
7. Hur utbildar och övar andra länder cybersäkerhet för aktörer inom hamnsektorn?

Tyngdpunkten för studien ligger på de första tre frågeställningarna.

1.2 Avgränsningar

Studien avgränsar sig till att undersöka och inventera de typer av system och de aktörer som direkt relaterar till hamnar och hamnverksamhet snarare än till de fartyg som nyttjar hamnarna. Det finns antagligen visst överlapp mellan dessa, men fokus ligger på hamnarna.

Vidare avgränsas studien till att studera godshamnar och större passagerarhamnar av samhällsviktig natur, snarare än småbåtshamnar eller marinor.

För denna studie har fyra svenska hamnar valts ut och studerats djupare, vilket bland annat inkluderat intervjuer och studiebesök till dessa hamnar. På grund av tidsmässiga begränsningar för studien har det inte varit möjligt att besöka eller i mer detalj studera fler svenska hamnar.

1.3 Läsanvisning

Kapitel 2 är ett metodkapitel som beskriver studiens datainsamlingsmetoder samt en reflektion kring de valda metoderna.

Kapitel 3 är ett bakgrundskapitel som övergripande beskriver vad en hamn är och vilka delar som de består av.

I *kapitel 4* besvaras frågeställning tre genom en presentation av de olika regelverk som har en inverkan på hamnverksamhet, både allmänt och relaterat specifikt till cyber.

Detta följs av *kapitel 5* där olika informationsflöden och cyberfysiska system beskrivs. Detta kapitel besvarar främst frågeställning ett och två men även till viss del frågeställning tre avseende på viktiga aktörer.

Kapitel 6 beskriver den digitalisering som sker i svenska hamnar och vilka utmaningar detta ger. Vidare görs en kort internationell utblick till ett antal större internationella hamnar som kommit långt i sitt arbete med digitalisering. Detta kapitel besvarar därmed frågeställning fyra och fem.

Kapitel 7 lyfter fram olika hot som kan föreligga mot hamnar och de system som används, samt beskriver tidigare angrepp mot hamnar.

Kapitel 8 behandlar frågeställning sex och presenterar den logiska grund som nyttjas för att bedöma cybersäkerhetsmognad hos hamnar. I kapitlet görs även en övergripande bedömning av mognaden hos intervjuade hamnar baserat på intervjusvar.

I *kapitel 9* beskrivs övning och träning inom hamnsektorn med fokus på cyberområdet vilket besvarar frågeställning sju.

Slutligen diskuteras resultaten och några slutsatser dras i *kapitel 10*.

2 Metod

Detta avsnitt innehåller en beskrivning av tillvägagångssättet för studiens datainsamling samt en metodreflektion. Den primära datainsamlingen har genomförts via intervjuer och studiebesök (avsnitt 2.1). Vidare har tilläggsinformation samlats in som stöd för framtagande av intervjufrågor, som bakgrundsinformation och som fördjupningar till studiens frågeställningar. Inga specifika söksträngar nyttjades utöver sökord som relaterar till begreppen *hamnar* och *cybersäkerhet* i olika kombinationer, både på svenska och på engelska. De skriftliga källor som primärt har använts är (1) rapporter publicerade av svenska och internationella myndigheter, (2) nyhetsartiklar, (3) relevant lagstiftning, samt (4) information från hamnarnas webbsidor.

2.1 Intervjuer och studiebesök

Datainsamling har skett genom semistrukturerade intervjuer med hamnaktörer och myndigheter. Två intervjuguider har tagits fram, en riktad mot hamnarna och en riktad mot myndigheter. Frågorna i intervjuguiderna skiljer sig något mellan varandra i syfte att skräddarsy innehållet till de olika aktörstyperna. Framtagandet av intervjufrågorna gjordes baserat på bakgrundsmaterial i form av rapporter från svenska och utländska myndigheter.

Totalt genomfördes tio intervjuer varav fyra på plats vid hamnarna och sex via Skype. Varje intervju tog cirka en timme och inför intervjuerna hade deltagarna fått information om studien.

Personal från fyra olika hamnar intervjuades och studiebesök genomfördes på två av dessa. Urvalet baserades på att samtliga är större hamnar som alla är centrala för import av olika typer av gods. De personer som intervjuades vid hamnarna har någon roll kopplad till hamnaktörernas säkerhetsorganisation. Antalet intervjuer som genomförts vid respektive hamn har varierat beroende på vilka aktörer som har funnits tillgängliga för intervjuer. Framförallt är det representanter från hamnbolagen som har intervjuats men en intervju har genomförts med representanter från en terminaloperatör och en med representanter från en energihamn. På respektive intervju har 1-3 personer deltagit vilket resulterar i ett deltagarantal om totalt 15 personer från hamnaktörerna.

Nedan ges en övergripande beskrivning av de hamnar som har varit föremål för studiens datainsamling.

Gävle hamn beskriver sig som Mellansveriges största logistiknav från vilken gods transporteras med såväl fartyg som tåg och lastbil. Hamnen består av containerterminal, bulkterminal, kombiterminal och energihamn. Verksamheten bedrivs av ett kommunalägt bolag, en privat terminaloperatör samt ett flertal bolag inom

energihamnen. Godshanteringen uppgår till cirka 6 miljoner ton och cirka 900 fartygsanlöp årligen (Gävle hamn, 2022).

Göteborgs hamn är Nordens största hamn och verksamheten bedrivs av Göteborgs hamn AB vilket är ett kommunalägt bolag som ansvarar för infrastrukturen, samt ett flertal privata terminaloperatörer. Hamnen har terminaler för container, Ro/Ro[2], olja och andra energiprodukter samt passagerare. Enligt årsredovisningen var hamnens totala godshantering 2020 37,9 miljoner ton och ett totalt antal anlöp om 5 300 (Göteborgs hamn AB, 2022).

Norrköpings hamn drivs av ett kommunalägt bolag vilket ansvarar för såväl infrastruktur som stuveri- och terminalverksamhet. Inom hamnen hanteras en rad olika varor som skogs-, stål-, spannmåls-, energi- och petroleumprodukter samt containrar. Godshanteringen uppgick 2021 till 4,5 miljoner ton och cirka 1 100 fartyg anlöpte till hamnen (Norrköpings hamn, 2022).

Stockholms hamnar består av flera olika hamnar inom Stockholms län; Norviks- och Nynäshamns hamn i Nynäshamns kommun, Värtahamnen, Frihamnen och Stadsgården i Stockholms stad samt Kapellskärs hamn i Norrtälje kommun. Ägarskapet är delat men drivs i huvudsak av Stockholms hamnar AB vilket i sin tur ägs av Stockholms stad. Stockholmshamnar hanterar både gods och passagerartrafik. Godshanteringen ligger på cirka 9 miljoner ton gods och hamnarna har cirka 9 000 fartygsanlöp årligen (Stockholms hamnar, 2022).

Utöver intervjuer med hamnaktörer har intervjuer även genomförts med relevanta myndigheter. Intervjuförfrågan skickades till Transportstyrelsen, Sjöfartsverket, Kustbevakningen, Polisen och Tullverket varav Kustbevakningen och Polisen avböjde medverkan. Vid varje intervju deltog en person vilket resulterar i ett deltagarantal om totalt tre personer. Vidare har frågor relaterade till energihamnar ställts och besvarats via mail till Länsstyrelsen Gävleborg samt Energimyndigheten.

2.2 Metodreflektion

Intervjuer har endast genomförts med ett mindre antal hamnar och andra relaterade aktörer, vilket begränsar resultatets generaliserbarhet. Detta gäller särskilt för bedömningen av cybersäkerhetsmognad, se kapitel 8. Vidare är det svårt att skapa en helhetsbild för svenska hamnar baserat på det begränsade urvalet även om denna studie kan ge viktiga indikationer på områden för en djupare bedömning.

De genomförda intervjuerna var av semistrukturerad karaktär, vilket lämpade sig väl för denna studie eftersom detta gav möjligheter till att ställa följdfrågor eller

[2] Roll on/Roll off (Ro/Ro eller RORO) avser fartyg som är designade för att transportera olika typer av fordon. Där fordonen körs på fartyget för egen maskin, snarare än att det lastas med hjälp av exempelvis en kran.

andra frågor som uppdagades under själva intervjuerna. Vidare ger semistrukturerade interjuver respondenter möjlighet att utveckla och resonera kring sina svar. Samtidigt innebar detta att alla respondenter inte nödvändigtvis ställdes exakt samma frågor, eftersom specifika följdfrågor kunde vara beroende av vilka svar respondenter gav. Det går därför inte att se detta som en jämförande studie mellan olika hamnar.

De kvalitativa data som samlas in via intervjuer lämpade sig väl som datainsamlingsmetod för denna studie, då de möjliggör skapandet av en djupare förståelse för området som helhet. Däremot kunde en kvantitativ datainsamlingsmetod som exempelvis enkäter eller frågeformulär varit bättre lämpat i syfte att få en bredare spridning och kartläggning av svenska hamnar relaterat till studiens frågeställningar. Detta hade möjligtvis kunnat påverka generaliserbarheten i positiv mening. Enkäter och andra typer av kvantitativ datainsamling lämpar sig dock bäst när det finns tydligt formulerade frågor som behöver besvaras, där frågorna kan besvaras av majoriteten av eller rent av alla respondenter. Då denna studie i hög grad kan anses som explorativ och dessutom innefattar olika typer av aktörer i relation till hamnar, anses kvalitativ datainsamling genom intervjuer vara den mer lämpade datainsamlingsmetoden. Det är däremot möjligt och kanske även önskvärt att en framtida relaterad studie nyttjar enkäter i syfte att komplettera resultaten från denna studie. En sådan insamling blir även mer görbar med denna studie som grund då det troligen underlättar formulerandet av konkreta och relevanta frågor som lämpar sig för enkätformatet.

Rapporten innehåller endast öppen information och intervjuerna har inte genomförts på ett sådant sätt att de har möjliggjort frågor som berör känslig information. Detta har varit möjligt då studiens frågor är av övergripande karaktär och främst syftar till en generell kartläggning. För att gå djupare och mer detaljerat i frågeställningarna behöver det övervägas huruvida insamlad data är känslig, både frågan i sig och det sammanställda materialet, och hur detta ska hanteras.

3 Hamnar

En hamn definieras av Svensk ordbok utgiven av Svenska Akademien (SO 2022) som:

[En] större anläggning för (skyddad) förtöjning, lossning och lastning av fartyg bestående av kajer, pirar, dockor etc. med kranutrustning m.m. med naturligt el. konstgjort skydd mot sjögång.

Det finns idag cirka hundra hamnar i Sverige, varav 54 är utpekade som allmänna hamnar[3] och övriga betecknas som enskilda hamnar. De allmänna hamnarna står för cirka 80 procent av all trafik sett till transporterat gods och passagerare. I tillägg uppskattas så mycket som 90 procent av alla importer och exporter av gods till och från Sverige hanteras via sjöfart (Sjöfartsverket, 2015). Hamnar är därför en kritisk del i hela landets import- och exportkedja.

Göteborgs hamn är Nordens största godshamn och hanterade totalt 36,8 miljoner ton gods år 2021. Detta motsvarar drygt 22 procent av den totala godsmängden som hanterades inom svenska hamnar. I jämförelse hanterade Sveriges näst största godshamn, Trelleborg, 13,8 miljoner ton gods samma år (Sjöfartsverket, 2015; Trelleborgs Hamn, 2021).

Stockholms hamnar (Stockholm, Kapellskär, Nynäshamn och Norvik) driver Sveriges största passagerarhamn och är också en av de största passagerarhamnarna i hela världen. Under 2021, då resmöjligheterna var begränsade på grund av coronapandemin, passerade 4,6 miljoner passagerare i Stockholms hamnar. Detta är en avsevärd nedgång jämfört med åren innan pandemin då antalet årliga passagerare låg närmare 12 miljoner samt ytterligare 4 miljoner passagerare i skärgårdstrafiken för en total av drygt 16 miljoner passagerare årligen. Stockholms hamnar är dessutom en av de största godshamnarna i Sverige med en årlig hantering av drygt 9,1 miljoner ton (Stockholms Hamnar, 2021).

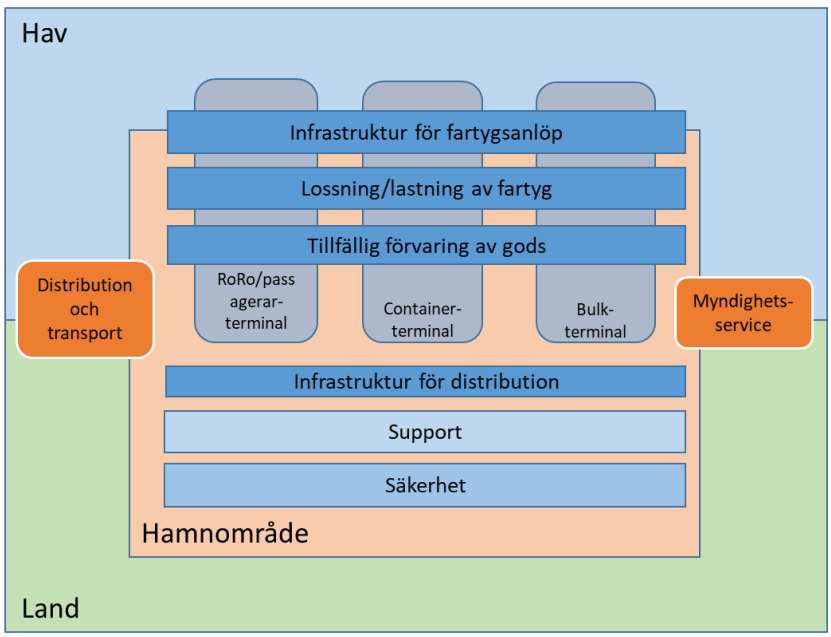
Inom EU investeras stora belopp i utbyggnaden av det Transeuropeiska transportnätet (TEN-T), vilket är ett trafikslagsövergripande nätverk inom EU och angränsande länder. Detta transportnätverk utgör noder och länkar som är av stor vikt för att flöden av gods och personer i Europa ska fungera. Inom detta finns ett stomnät inom vilket ett antal viktiga noder och länkar har valts ut. Länkarna, så kallade stomnätskorridorer, startar och slutar i en så kallad corehamn. I Sverige finns det fem hamnar som är utpekade som corehamnar: Göteborg, Luleå, Malmö/Köpenhamn, Stockholm och Trelleborg. Vidare finns ytterligare 21 viktiga hamnar i det övergripande TEN-T nätverket (Kjellsdotter Ivert, Merkel, Kalantari, Santén, Svanberg & von Wieding, 2021).

[3] Allmänna hamnar måste vara upplåtna för allmän trafik och vara av betydelse för den allmänna samfärdseln. Fritidsbåtshamnar, fiskehamnar eller hamnar som endast betjänar en viss industri anses inte ingå i begreppet allmän hamn. (Naturvårdsverket, 2022; Trafikanalys 2019)

3.1 Hamnverksamhet

Det finns olika typer av hamnar, såsom godshamnar, energihamnar och passagerarhamnar, vilka skiljer sig från varandra då olika typer har olika behov. Exempelvis behöver det finnas utrymme för mellanlagring av gods mellan transporter i godshamnar, medan en passagerarhamn har ett flöde av passagerare genom hamnen i samband med ett anlöp. Energihamnar är hamnar som är särskilt utformade för att ta emot energiprodukter såsom petroleumprodukter och LNG. Vidare kan det även finnas skillnader i hur olika godshamnar ser ut, beroende på vilken typ av gods som hamnen primärt hanterar. Därför är det vanligt att hamnen delas in i terminaler efter vilken typ av gods som hanteras. Beroende på hamnens karaktär finns det även skillnader mellan olika hamnar i de IT- och OT-system som används, vem som använder dem och hur de används (ENISA, 2019).

Större hamnar har även flera gemensamma beståndsdelar oavsett typ av hamn, se schematisk bild i figur 1. Alla stora hamnar har infrastruktur för anlöp samt lossning och lastning av fartyg, med kaj, trafikledning, lots, bogserbåtar, fartygsagenter samt personal för lastning och lossning av gods. För tillfällig förvaring av gods finns infrastruktur som lagringslokaler och uppställningsplatser inom hamnområdena. Hamnar har också ett antal stödfunktioner som support av hamnens olika servicefunktioner och säkerhet. För att underlätta hantering av alla dessa delar finns ett antal olika IT-system.



Figur 1. Beskrivning av en hamns större beståndsdelar. Illustrationen är gjord med inspiration från ENISA (2019).

3.2 Hamnaktörer

Inom en hamn finns flera olika aktörer representerade. I detta avsnitt beskrivs de som vanligtvis finns i en svensk hamn.

3.2.1 Hamnbolag

Hamnbolagen är de aktörer som äger hamnen och ansvarar för mark och infrastruktur. Svenska hamnar ägs och drivs på olika sätt. En del hamnar är en del av den kommunala förvaltningen och andra hamnar drivs genom kommunala bolag. I vissa fall sköter de kommunala bolagen hela verksamheten, i andra fall förvaltas bara hamnområdet medan driften sköts av andra aktörer. I tillägg finns även hamnar som drivs av privatägda bolag, vilket exempelvis gäller för flera av de industrihamnar som finns i landet (Trafikverket, 2021; Kjellsdotter Ivert m fl, 2021).

3.2.2 Terminaloperatörer

Terminaloperatörer är de aktörer som sköter driften av terminalerna, det vill säga hanterar godset som lossas och lastas i hamnen. Vanligtvis finns det endast en operatör men det kan finnas flera, särskilt om olika typer av gods hanteras. Inte sällan är operatörerna internationella företag som bedriver verksamhet i flera olika hamnar.

3.2.3 Varuägare

Varuägare eller transportköpare äger det gods som fraktas genom hamnen. Genom detta är de också kravställare på hamnen och den infrastruktur som krävs för att kunna frakta visst typ av gods och flödet för detta (Kjellsdotter Ivert m fl, 2021).

3.2.4 Transportörer

Rederier och speditörer är exempel på olika transportörer. Speditörerna hjälper varuägare att organisera en transporttjänst med hjälp av flera olika transportslag. Därmed genomför de inte enbart transporten utan även omlastningar, förtullningar etcetera som bland annat sker i hamnområdena. Vissa speditörer är specialiserade på ett transportslag medan andra hanterar flera. Rederier å andra sidan är företag som endast bedriver handelssjöfart (Kjellsdotter Ivert m fl, 2021).

3.2.5 Myndigheter

Det finns flera myndigheter som verkar i anslutning till hamnens verksamhet. Sjöfartsverket har ansvar för sjöfart och är en av aktörerna som är inblandade i anlöp av fartyg. Tullverket och Kustbevakningen ansvarar för kontroller av det

gods som ankommer till en hamn. Trafikverket ansvarar för infrastruktur på landsidan i en hamn såsom väg och järnväg. Utöver dessa finns ett antal myndigheter som genomför tillsyn av olika delar av hamnarnas verksamhet. Detta beskrivs vidare i kapitel 4.

4 Regelverk

I detta kapitel presenteras de lagar och regelverk som är relevanta för hamnanläggningar. Inledningsvis presenteras lagstiftning som rör skydd av fartyg och hamnar, varefter lagstiftning, föreskrifter och standarder som mer specifikt relaterar till cyber- och informationssäkerhet i hamnar presenteras.

4.1 Skydd av fartyg och hamnar

I detta avsnitt presenteras den lagstiftning som rör skydd av fartyg och hamnar. Lagstiftningen rör främst fysiskt skydd men innehåller vissa delar som relaterar till cyber- och informationssäkerhet.

4.1.1 International Ships and Port Facilities Security Code (ISPS) och Safety of Life at Sea (SOLAS)

Safety of Life at Sea (SOLAS) är en internationell konvention framtagen av Förenta Nationernas (FN) organ för sjösäkerhet, International Maritime Organization (IMO). Konventionen gäller säkerhet för människor till sjöss och har sitt ursprung i efterdyningarna av Titanic som sjönk 1912 (Konventionen antogs år 1914). Sedan dess har konventionen uppdaterats successivt (år 1929, 1948, 1960 samt 1974) och är idag generellt erkänd som det viktigaste internationella fördraget gällande handelsfartyg (IMO, 2019a).

SOLAS delas in i 14 kapitel som specificerar bland annat konstruktion av fartyg, kommunikation och navigation, brandskydd och andra livräddande apparater, särskilda säkerhetskrav för specifika typer av fartyg, transport av gods och även ISPS-koden.

International Ships and Port Facilities Security Code (ISPS) specificerar säkerhetskrav för fartyg och hamnar. ISPS är en del av SOLAS-konventionen och beskrivs i kapitel XI-2 i SOLAS. Kapitlet specificerar vilka säkerhetskrav som måste uppfyllas för att efterleva konventionen och ger rekommendationer kring hur man kan uppnå de beskrivna säkerhetskraven.

Varken ISPS eller SOLAS i övrigt specificerar explicit hur cybersäkerhet bör hanteras. Fokus ligger istället framförallt på fysisk säkerhet för fartyg och hamnar. IMO hänvisar på sin hemsida (IMO, 2019b) till ett antal andra standarder och dokument för hur cybersäkerhet och cyberrisk kan hanteras, exempelvis ISO/IEC 27001 (ISO, 2022), IAPH:s rapport om cybersäkerhet (IAHP, 2020) och rekommendationer från IACS om cyberresiliens (IACS, 2022).

I Sverige ansvarar Transportstyrelsen, Polismyndigheten samt Kustbevakningen för att det internationella regelverket för förbättrat sjöfartsskydd på fartyg och i hamnanläggningar (ISPS) följs.

4.1.2 Lagen om sjöfartsskydd (SFS 2004:487)

Lagen om sjöfartsskydd innehåller kompletterande bestämmelser till Europaparlamentets förordning EG 725/2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar. Syftet med EG725/2004 är att genomföra gemenskapsåtgärder vilka förbättrar sjöfartsskyddet på fartyg som används för internationell handel och nationell sjöfart inför hot om avsiktliga olagliga handlingar. Förordningen syftar även till att skapa en grund för harmoniserad tolkning, genomförande och kontroll av de särskilda åtgärder för förbättrat sjöfartsskydd vilka antogs i december 2002 vid IMO:s diplomatkonferens.

Utöver lagen om sjöfartsskydd och EG 725/2004 finns även förordningen om sjöfartsskydd (2004:283) samt Sjöfartsverkets föreskrifter (SJÖFS 2004:13) som båda kompletterar EG 725/2004 respektive lag (2004:487) om sjöfartsskydd. Reglerna om sjöfartsskydd syftar till att skydda sjöfartssektorn mot grova våldsbrott, däribland terrorism.

Lagstiftningen berör både lastfartyg med en bruttodräktighet[4] av 500 ton eller mer såväl som passagerarfartyg, flyttbara oljeplattformar samt de hamnar som betjänar fartyg som går i internationell fart samt mellan Gotland och fastlandet. Fartyg som avser att anlöpa en svensk hamn måste lämna en förhandsanmälan med information av sjöfartsskyddskaraktär, exempelvis hur säkerheten är organiserad på fartyget. Vidare innehåller lagen om sjöfartsskydd flera bestämmelser gällande beslut om skyddsnivå, kroppsvisitation, ansvar och straff. Dessutom beskrivs vilket ansvar som Polismyndigheten och Transportstyrelsen har i relation till sjöfartsskyddet.

4.1.3 Fartygssäkerhetslagen (SFS 2003:364)

Lagen om fartygssäkerhet gäller för alla fartyg som används inom Sveriges territorium samt för svenska fartyg som opererar i sjöfart utanför svenskt territorium. I tillägg gäller lagen även både svenska och utländska rederier som opererar inom svenska vatten.

Fartygssäkerhetslagen (2003:364) innehåller allmänna krav som ställs på fartyg, bemanning och rederiverksamhet och särskilda krav på olika typer av fartyg. De allmänna kraven inkluderar bland annat krav på sjövärdighet, lastning, certifikat, bemanning och skyldigheter. De särskilda kraven kan exempelvis utgöras av passagerarcertifikat för passagerarfartyg som specificerar det högsta tillåtna antalet passagerare för passagerarnas säkerhet inte ska äventyras. Det finns även andra typer av certifikat för andra typer av fartyg.

I tillägg finns i fartygssäkerhetslagen en rad olika bestämmelser som relaterar till tillsyn, besiktning, straff och skyldigheter. Bland dessa finns bestämmelser att

[4] Fartygets totala inneslutna volym

hamninnehavare och lotsar som i sin normala verksamhet uppmärksammar allvarliga avvikelser på ett fartyg, har en skyldighet att rapportera detta till en utpekad myndighet vilken är Transportstyrelsen om inget annat anges. Vidare får regeringen enligt fartygssäkerhetslagen meddela föreskrifter om utvisning från svensk hamn och förbud för fartyg att anlöpa svensk hamn.

Kustbevakningen utför sjösäkerhetstillsyn för att förebygga, hindra och begränsa skador på liv, hälsa, miljö och egendom som kan orsakas av brister inom sjötransporten. Myndigheten genomför kontroller av transporter av farligt gods i hamnarna och av säkring av last för sjöfärd. Kontrollerna sker självständigt, men också i samverkan med Polismyndigheterna, Tullverket, Strålsäkerhetsmyndigheten, Transportstyrelsen och MSB. När Kustbevakningen arbetar i hamnarna kontrolleras även nykterheten hos förarna (KBV, 2022).

4.1.4 Lagen om hamnskydd (SFS 2006:1209)

Denna lag innehåller bestämmelser om hur hamnskydd ska organiseras och bedrivas. Hamnskydd innebär att åtgärder vidtas inom hamnen så att människor, infrastruktur och utrustning skyddas mot allvarliga olagliga handlingar. Exempel på sådana åtgärder kan vara fysiskt skydd såsom staket och kameraövervakning. De åtgärder som vidtas ska även samordnas med åtgärder som vidtas med stöd av sjöfartsskyddslagarna, se ovan.

I lagen om hamnskydd specificeras vidare ett antal olika roller och aktiviteter som ska ingå i hamnskyddsarbetet. Detta inkluderar bland annat ett hamnskyddsorgan, att en hamnskyddutredning och hamnskyddsplan genomförs, samt att hamnskyddsövningar hålls.

Lagen om hamnskydd specificerar dock inte specifikt hur hamnskyddet ska uppnås och nämner således inte heller informationssäkerhet eller cybersäkerhet. Informationssäkerhet och cybersäkerhet bedöms dock som relevanta att beakta i relation till lagen i denna studie. Under intervjuerna framkom det att informationssäkerhet i regel finns med som en del av hamnskyddsplanen även om fokus för skyddsplanen ligger på den fysiska säkerheten.

4.2 Cyber- och informationssäkerhet

I detta avsnitt beskrivs specifik lagstiftning, föreskrifter och standarder som relaterar till cyber- och informationssäkerhet i hamnar.

4.2.1 NIS-direktivet (216/1148)

NIS-direktivet är ett EU-direktiv (2016/1148) som syftar till att säkerställa en hög nivå på säkerhet i nätverks- och informationssystem inom unionen. Direktivet ställer säkerhetskrav och riktar sig till leverantörer av digitala och samhällsviktiga

tjänster[5] inom sju olika sektorer varav transport utgör en. Inom ramen för transportsektorn ingår sjöfart som i sin tur omfattar hamnar och hamnanläggningar liksom rederier, fartyg och sjötrafikinformationstjänster. Enligt MSB:s rådande föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2021:9) omfattas hamnar som årligen hanterar minst 2 500 000 ton gods, minst 200 000 passagerare eller ingår i det transeuropeiska transportnätet och hanterar minst 100 000 ton gods. NIS-direktivet är dock under omarbetning och i NIS2 blir urvalskriterierna istället baserade på företagens storlek i termer av omsättning och antal anställda. Dessutom beräknas fler aktörer jämfört med idag komma att omfattas.

I Sverige har NIS-direktivet implementerats i lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster samt i förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Med lagstiftningen (2018:1174) följer en skyldighet för tjänsteutövarna att:

- bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem,
- göra en riskanalys som ska ligga till grund för val av säkerhetsåtgärder,
- vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem,
- vidta lämpliga åtgärder för att förebygga och minimera verkningar av incidenter som påverkar nätverk och informationssystem, och
- utan onödigt dröjsmål rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller.

Incidentrapporteringen sker till den nationella CSIRT-enheten[6] vid MSB, som i sin tur tillgängliggör informationen i incidentrapporteringen till tillsynsmyndigheterna. För transportområdet är det Transportstyrelsen som har tillsynsansvaret och inom energiområdet är det Energimyndigheten. Detta innebär att samma verksamhet kan komma att vara föremål för tillsyn av flera aktörer vilka i största utsträckning försöker samordna sig med varandra. I skrivande stund har Transportstyrelsen inte genomfört någon tillsyn över hamnar än. För de leverantörer som inte uppfyller NIS-kraven har tillsynsmyndigheterna möjlighet att meddela förelägganden, samt ta ut en sanktionsavgift.

4.2.2 Säkerhetsskyddslagen (2018:585)

Verksamhet som omfattas av säkerhetsskyddslagen (2018:585) undantas ovan beskrivna NIS-lagstiftning. Säkerhetsskyddslagen gäller för aktörer som till någon

[5] Inkluderar internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster (lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster).
[6] Computer Security Incident Response Team

del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.

Jämfört med NIS-direktivet ställer säkerhetsskyddslagen högre och mer detaljerade krav på säkerhetsskydd, som förutom informationssäkerhet också inkluderar fysisk säkerhet och personalsäkerhet. Det sistnämnda, personalsäkerhet, syftar här på att minska risken för att icke tillförlitliga personer får tillgång till säkerhetskänslig verksamhet och att kunskapsnivån kring säkerhetsskydd är tillräckligt hög inom organisationen. I den kompletterande säkerhetsskyddsförordningen (2021:995) anges bland annat åtgärder som en verksamhet måste vidta inför driftsättning av ett informationssystem, och säkerhetskrav för de informationssystem som används i säkerhetskänslig verksamhet. Liksom för NIS-direktivet är Transportstyrelsen tillsynsmyndighet vad gäller hamnverksamhet och Energimyndigheten för energihamnar. I händelse av en IT-incident i ett informationssystem som allvarligt kan påverka säkerheten i systemet ska detta skyndsamt anmälas till Säkerhetspolisen.

4.2.3 Transportstyrelsens föreskrifter (TSFS 2022:14)

Transportstyrelsen har tagit fram föreskrifter och allmänna råd om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom transportsektorn (Transportstyrelsen, 2022). Föreskrifterna gäller oavsett transportslag och beskriver ett antal säkerhetshöjande åtgärder som verksamheter bör genomföra. Enligt en intervju med en respondent från transportstyrelsen bygger föreskrifterna bland annat på ENISAs vägledning *Minimum Security Measurements*.

4.2.4 Standarder och rekommendationer

Utöver lagstiftning och föreskrifter finns också olika standarder och rekommendationer som adresserar cybersäkerhetsfrågor.

ENISA, den europeiska myndigheten för cybersäkerhet, arbetar aktivt gentemot hamn- och sjöfartssektorn och har de senaste åren publicerat flera rapporter på temat cybersäkerhet. År 2020 presenterades rapporten Cyber Risk Management for Ports i syfte att ge hamnaktörer förslag på god praxis inom säkerhetsområdet för både OT- och IT-system (ENISA, 2020). I denna introduceras en fyrstegsmetod till cybersäkerhetshantering specifikt riktad till hamnaktörer, som både följer EU:s lagstiftning, gängse riskhanteringsprinciper och går i linje med ISPS riskvärderingsmetodik. De fyra stegen är 1) identifiering av cyberrelaterade tillgångar och tjänster, 2) identifiering och värdering av cyberrelaterade risker, 3) identifiering av säkerhetsåtgärder, och 4) bedömning av cybersäkerhetsmognad. För varje steg presenterar rapporten riktlinjer, utmaningar och god praxis som kan anpassas utifrån respektive hamnaktörs förutsättningar i termer av storlek, cybersäkerhetsmognad, informationssäkerhetsbudget och operativ omfattning.

Utöver ENISAs rekommendationer finns två ytterligare standarder för informationssäkerhet. Den ena är standarden ISO 27001 om hantering av informationssäkerhet vilken beskriver krav för att skapa, implementera, vidmakthålla och utveckla ett informationssäkerhetssystem. Inom systemet ska organisationerna bland annat kunna utvärdera informationssäkerhetsrisker och vidta riskreducerande åtgärder samt skapa en process som säkerställer att informationssäkerhetskontroller möter organisationens behov löpande (ISO, 2022). Den andra är standardserien ISA/IEC 62443 vilken bland annat ger information om detaljerade tekniska krav och säkerhetsnivåer för industriella kontrollsystem (ISA, u.å.).

5 Informationsflöden och cyberfysiska system

Som tidigare beskrivits finns det ett stort antal aktörer som på ett eller annat sätt verkar i en hamn, från hamnägare, till operatörer, transportörer och myndigheter. Därtill hanteras flera olika typer av gods för vilka olika processer och system nyttjas. Att beskriva alla de informationsflöden som används för att godsflödet genom hamnen ska fungera är med andra ord inte en helt okomplicerad uppgift.

I ett försök att förtydliga den stora mängd data som utbyts mellan hamnens aktörer och övriga aktörer, som exempelvis rederier och myndigheter, delar ENISA (2019) upp informationsflödet i fem olika kategorier:

1. De obligatoriska deklarationerna (information som rederier eller andra intressenter måste rapportera till hamnbolaget eller myndigheter, med hänsyn till den internationella, europeiska och nationella lagstiftningen).
2. Den kontroll och tillstånd som myndigheterna ger de kommersiella intressenterna (exempelvis tillstånd för tillträde till hamnen, tillstånd att lossa godset).
3. Operativa data relaterade till hamntjänster och processer (exempelvis behov av fartygstankning, schemaläggning av lastoperationer).
4. De finansiella uppgifterna (exempelvis fakturering från hamnen till sin kund, betalning).
5. Navigationsdata (exempelvis GPS-position för ett fartyg i hamnområdet, AIS-data).

Detta kapitel innehåller en generell beskrivning av informationsflöden och cyberfysiska system som är centrala för olika godsflöden genom en hamn. Beskrivningarna i avsnitten nedan tar till stora delar upp det som finns med i ENISAs kategorier ovan och baseras på information som erhållits genom studiens intervjuer och genomförda studiebesök. För tydlighets skull presenteras de informationsflöden och system som används *inför* att godset anländer till hamnen, och de som finns *på själva hamnområdet* i två separata avsnitt. Kapitlet innehåller vidare en beskrivning av informationsflödet med myndigheter, och avslutas med några övergripande iakttagelser om hamnarnas IT- och OT-system.

5.1 Inför att godset anländer till hamnen

Bokningar av transporter kring vilket gods som ska skickas, samt vart och när det ska skickas, sker genom elektroniska kontakter mellan hamnen eller hamnoperatören och rederier och speditörer. Exakt vilken information som skickas och till vilken aktör kan variera något beroende på typ av gods och om det handlar om att ta emot eller skicka gods. Många bokningar och mycket av informationsflödet mellan hamnen och kunder/rederier/speditörer sker via mejl och kräver manuell

hantering. Den information som skickas ligger till grund för hamnens planering för hur godset ska hanteras inom hamnområdet och vilka resurser som behövs för lossning och lastning. Inför leveranser till en energihamn kopplas också oberoende inspektörer in med uppgift att kontrollera att de levererade volymerna är korrekta.

För att effektivisera hanteringen av upphämtning och avlämning av gods finns det föraviseringssystem att tillgå, exempelvis *Preadvice*. Med system som detta föranmäler åkerier, antingen centralt eller via enskilda chaufförer, sin ankomst till hamnen. Utifrån den föranmälda informationen kan hamnen därefter planera mottagandet liksom lastning av godset som ska lämna hamnen. Preadvice kan integreras med olika typer av terminalsystem, exempelvis *PortIT* som nämns nedan (Stamford, u.å.).

Fartyg som är på väg till en svensk hamn eller ankarplats är skyldiga att inför anlöpet göra en elektronisk ankomstanmälan till webbportalen MSW Reportal, *The Swedish Maritime Single Window*. Portalen är ett samarbete mellan Kustbevakningen, Tullverket, Transportstyrelsen och Sjöfartsverket och har varit i bruk sedan 2015. Med portalen förenklas fartygsrapporteringen genom att relevant information till berörda myndigheter lämnas vid en enda kontaktpunkt som sedan för informationen vidare in i respektive myndighets system. Uppgifter som ska rapporteras in i systemet rör bland annat ankomstanmälan, faktisk ankomst- och avgångstid, om fartyget innehåller farligt gods och avfall samt om fartyget är föremål för utökad inspektion. Rapporteringskraven gäller för alla handelsfartyg med en bruttodräktighet av minst 300 ton, samt fiskefartyg och traditionsfartyg (kulturhistoriskt värdefulla fartyg). Den som ansvarar för att detta blir gjort är fartygets befälhavare.

I dagsläget är anmälningssystemen för Göteborgs hamn och Gävle hamn integrerade i MSW Reportal, vilket innebär att hamnarna automatiskt får viss anlöpsinformation från fartygen via ett API[7]. Flera hamnar står idag på tur att få ansluta sig till MSW Reportal. Information från fartygen rapporteras annars direkt från fartygen/rederierna till hamnaktörerna, ofta via mejl. Hamnaktörerna uppges därför inte vara beroende av MSW Reportal då informationen kan hanteras manuellt av hamnaktörerna. Enligt respondenten vid Sjöfartsverket pågår det idag ett utvecklingsarbete på EU-nivå där samtliga EU-länder ska ha en gemensam MSW Reportal. Detta innebär att informationen som ska rapporteras in i systemet är densamma i samtliga länder samt att aktörer i hamnarna ska få direkt information om anlöpen från systemet. Sjöfartsverket kommer dock fortsatt ha ansvar för drift av systemet inom Sverige.

Det pågår idag flera digitaliseringsinitiativ med syfte att skapa mer effektiva hamnanlöp. Sjöfartsverket medverkar tillsammans med aktörer inom sjöfartsbranschen för att underlätta och kunna dra nytta av informationsväxling mellan de

[7] API, Application Program Interface, är ett protokoll som används för kommunikation mellan program, system och applikationer.

aktörer som är involverade i ett fartygsanlöp (Sjöfartsverket, 2022b). Som exempel utvecklas ett kösystem för just-in-time-anlöp som förväntas driftsättas under 2023 (Sjöfartsverket, 2022a). Med den digitala applikationen Port Activity App, som börjat installeras vid Gävle hamn och som samlar och delar information om fartygens planerade rutter, ska fartygskön visualiseras. Med kösystemet är förväntningen att fartygens väntetider vid smala passager i skärgården ska elimineras, att fartygen kan anpassa sin hastighet för att anlända hamnen när det finns kajplats och därmed också minska användningen av fartygsbränsle.

5.2 På hamnområdet

Anlöpsinformationen från fartygen registreras i ett IT-system hos hamnen. Enligt respondenterna använder en stor majoritet av svenska hamnar, och även andra nordiska hamnar, PortIT som är ett kombinerat affärs- och verksamhetssystem. Systemet samordnar information om fartygsanlöp, godshantering och kundfakturering och kan kombineras med olika moduler för att även hantera exempelvis inpassering, behörighetskontroller och utfärdande av kort och koder (Stamford, u.å.). Systemet uppges av flera hamnrespondenter vara kritiskt för hamnens verksamhet.

Information från PortIT kan matas in i ett kajplaneringsverktyg som registrerar när och var fartygen ligger vid kaj. Utifrån den informationen kan de logistikföretag som verkar i hamnen positionera kranar efter fartygens lokalisering.

Kranar används för att lossa och lasta både containers och bulkvaror. Graden av automation varierar stort mellan olika typer av kranar. Äldre kranar och små kranar som exempelvis används för att hantera bulkvaror, varor som transporteras i större mängd utan emballage, styrs oftare förarstyrt på plats, det vill säga manuellt utan någon automatisering. För att hitta rätt container kan de dock använda sig av ett positioneringssystem. För nyare kranar förekommer det att dessa helt fjärrstyrs från ett manöverrum, exempelvis över fiber. Under intervjuerna lyftes att det allmänt inte finns så många uppkopplade enheter inom de intervjuade hamnarnas verksamhet, och att de också har en försiktig inställning till att koppla upp enheter mot internet. En respondent uppger att individuella OT-system för exempelvis kranar inte är uppkopplade.

Automatisering förekommer också i samband med lagring av varor på hamnens område. Ett exempel på det är ett lager för pappersrullar där själva lagerhanteringen, förflyttningen av rullarna till och från sin lagerplats, är automatiserad. Lossningen av rullarna till lagret från inkommande tåg, liksom lastningen av rullarna i containers för vidare uttransport till fartygen, sker dock i detta fall manuellt med en truck.

Beroende på vilken typ av gods som hanteras kan information om lastning och lossning om varan registreras i olika system. Som en respondent uttrycker det lästes exempelvis information rörande ståltransporter med tåg in i ett system, och

pappersleveranser in i ett annat. Systemen är i en del fall integrerade med varandra, i andra fall inte. I ett fall uppges att hamnoperatören och kunden är så nära sammankopplade att hamnoperatören använder sig av kundens system fram till dess att godset är lastat på fartyget.

För energihamnar används till del OT-system för att styra pumpar och ventiler och hantera lossning och depåförflyttningar av petroleumprodukter i ett rörledningsnät. Själva lossningen uppges vara en relativt icke-automatiserad process, öppning och stängning av ventiler kan hanteras manuellt. Här kan styrsystemen ha en mer övervakande funktion, som ett extra lager av säkerhet. System finns också för funktioner som nivåmätning, volymhantering, överfyllnadslarm, utrymningslarm och brandvattenpumpar (Stenérus Dover, Lindgren & Andersson, 2018). Autonoma system som kan vara integrerade i processkontrollsystemen uppges finnas för exempelvis gasåtervinning. För att hantera information rörande pumpning, typ av petroleumprodukt och klassning etc. uppges det vid en av intervjuerna att applikationen *New Pipe* används, ett IT-system av mer administrativ karaktär som integreras med hamnens andra system och skickar information till ekonomisystemet och vidare ut till kund för fakturering. Från New Pipe får både hamnen och fartyget information om statistik och kostnadsuppgifter för det som pumpats (Kentor, 2017). Under intervjuerna framkommer att både vissa styrsystem och IT-system av mer administrativ karaktär bedöms vara kritiska för verksamheten i en energihamn.

För utlastning av petroleumprodukter till tåg används också styrsystem, som exempelvis visar med vilken frekvens lastningen sker och att säkerhetslarmen är påkopplade (Stenérus Dover, Lindgren & Andersson, 2018). En respondent nämner att de använder ett halvautomatiskt utlastningssystem som hanteras av en extern aktör.

För att hantera säkerhetsansvaret nämner en av hamnarna att de nyligen infört ett digitalt system, *Hamnsäkerhetsjournalen*, för hantering av data och kontroller i checklisteformat. För att säkerställa den fysiska säkerheten, så att inte obehöriga kommer in på hamnområdet, använder hamnarna också digitala säkerhetssystem. För att ytterligare förbättra skalskyddet uppger en av respondenterna att de funderade på möjligheten att använda sig av drönare som kan patrullera längs med hamnområdets stängsel. Kameror används inte bara i övervakningssyfte, utan även för att dokumentera i vilket skick som godset har levererats. Därför fotograferas och filmas både fordon och gods och skickas till rederier och kunder.

Vid en av hamnarna uppges ett GIS-system[8] användas som exempelvis märker ut tillstånd i hamnen. Med systemet får man en ögonblicksbild av vilka aktörer och

[8] Ett GIS-system är ett geografiskt informationssystem, en programvara för hantering, insamling, lagring, bearbetning, analys och presentation av geografisk information.

entreprenörer som finns i hamnen ifall det skulle ske en olycka på området. Systemet har också en direktkoppling till SOS Alarm.

5.3 Kommunikation med myndigheter

De myndigheter som framförallt är en del av informationsflödet i hamnarna är Sjöfartsverket, Tullverket, Transportstyrelsen och Kustbevakningen. Informationen de behöver kommer främst från MSW Reportal som beskrivs i avsnitt 6.1.

Sjöfartsverket är utsedd som kontaktpunkt för den fartygsanmälan som fartygen gör i MSW Reportal. Krav för såväl fartygsanmälan som att myndigheter ska tillhandahålla en kontaktpunkt ställs utifrån EU-direktiv 2002/59/EG som har införlivats i föreskrifter från Transportstyrelsen. Vissa av de uppgifter som rapporteras in via MSW Reportal rapporteras i sin tur vidare till EU-gemensamma system som exempelvis SafeSeaNet (SSN) där flera myndigheter kan ta del av dessa (Transportstyrelsen, u.å). Sjöfartsverket har även ett särskilt ansvar att rapportera vidare information om exempelvis avfall och farligt gods till European Maritime Safety Agency (EMSA) som arbetar med fartygssäkerhet.

Sjöfartsverket ansvarar också för lotsning av fartyg in till hamnar. Fartygen anlitar i regel lotsningstjänster via MSW Reportal, men kan också beställa dem direkt av lotsningsservice. På Sjöfartsverkets webbsida går det också att finna information om pågående lotsningsuppdrag.

Tullverket har ett behov av att få information om vilka varor som ankommer eller avgår från hamnarna men delar inte vidare information till andra aktörer. Enligt intervju med respondent från myndigheten skiljer man på två olika typer av gods, sådant gods som kommer med en passagerare och sådant gods som inte är knutet till en person. För personburet gods får Tullverket tillgång till passagerarlistor från rederierna. Detta sker antingen genom tillgång till rederiernas system eller genom att rederierna skickar listor. Övrigt gods ska anmälas av speditörerna via en tulldeklaration i ett system som ägs av Tullverket. Detta ska dock endast göras för gods som ankommer från tredje land och inte för gods inom EU. Informationen om gods och när det ankommer används av Tullverket för att planera deras kontrollverksamhet.

För att Tullverket ska kunna genomföra sina kontroller finns det en skyldighet att sätta upp lokaler för detta inom hamnområdet. Kravet ställs på transportören men i praktiken är det hamnbolaget som är dialogpart i egenskap av ägare till infrastruktur i hamnar. I lokalen använder Tullverket sitt ett eget nätverk men blir i övrigt servade av hamnbolagen.

Tullverkets datasystem är mest kritiskt för att kunna prioritera var kontroller ska genomföras. Om systemet inte fungerar skulle det i värsta fall kunna innebära ett importstopp från tredje land eftersom Tullverket inte får kännedom om vilket

gods som importeras. Samtidigt är inte själva kontrollerna beroende av systemet utan kan utföras ändå.

5.4 Allmänt om hamnens system och hur kritiska de är

Sammantaget behövs det ett betydande antal IT-system för att driva den dagliga verksamheten vid Sveriges större hamnar. Som en av respondenterna uppger används mellan 45 och 50 olika IT-system i hamnen. Majoriteten av dessa är dock inte verksamhetskritiska och för alla hamnar uppges att verksamheten kan fortsätta upprätthållas en längre period utan tillgång till dessa icke-kritiska system. De system som av respondenterna lyfts fram som mest kritiska rör informationssystem, system som hanterar hamnens skalskydd, samt processkontrollsystem för hantering av energihamnars verksamhet. Även utan dessa system bedömer dock respondenterna att stora delar av verksamheten kan upprätthållas och hanteras manuellt, även om det skulle vara mycket mer komplicerat, tidskrävande, dyrare och medföra logistiska utmaningar jämfört med normal drift.

Mellan de IT-system som används i en hamn uppges det finnas flera beroenden, både mellan de interna systemen och med externa tjänster. En respondent uppger att integrationen av system sker över en integrationsplattform som idag bygger på molntjänster, även om de mer och mer går mot att använda ett eget API. I de fall det finns flera aktörer som verkar i en hamn, verkar det variera i vilken utsträckning aktörerna delar system och information med varandra. För en av de kontaktade hamnarna finns exempelvis inget samröre kommunikationsmässigt mellan hamnen och operatören med undantag för att hamnmyndigheten har tillgång till bilder från operatörens övervakningskameror.

Hur driften av systemen hanteras varierar från hamn till hamn och aktör till aktör. Driften av administrativa IT-system är i högre grad utlokaliserad. En del system finns fysiskt hos leverantören. För andra system kan infrastrukturen finnas lokalt och driftas in-house av hamnen men med extern support. I denna kategori hamnar de OT-system som nyttjas i verksamheten. Som en hamnaktör uttrycker det sker deras drift mestadels in-house för att det ska vara korta kommunikationsvägar. Generellt används en blandning av inköpta färdiga produkter och egenutvecklade system i hamnen. Det IT-säkerhetsarbete som bedrivs vid hamnarna inkluderar segmentering av system, att hålla olika IT-miljöer åtskilda och att skapa redundans med dubbel fiber till kritiska system. Samtidigt lyfter aktörerna att de kanske inte riktigt nått så långt som de hade önskat.

IT-säkerhetsfrågor är också något som inkluderas i hamnaktörernas beslut om att automatisera verksamheten, något som ligger högt på många hamnaktörers agenda och beskrivs närmare i nästföljande kapitel.

6 Digitalisering

I detta kapitel beskrivs vilket genomslag digitaliseringen fått i de fyra svenska hamnar som ingår i denna studie och hur den sannolika utvecklingen ser ut framöver. Vidare görs en mindre internationell utblick kring hur digitaliserade utländska hamnar är.

6.1 Digitalisering i svenska hamnar

Digitalisering är något som det pratats om inom flera områden. Ibland handlar det endast om att föra över information från papper in i ett digitalt system. Detta är dock bara en del av digitalisering och i en bred bemärkelse är digitalisering ”processer som förändrar eller skapar något nytt genom användning och integrering av digital teknik” (Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s.13)

Ingemarsdotter, Eidenskog och Hedtjärn Swaling (2020) lyfter tre digitala förändringsparadigm när det gäller digitalisering som handlar om hur det fysiska och det digitala kopplas samman allt mer. Det första handlar om cyber/fysiskt och att fysiska saker kopplas upp allt mer vilket också gör att verksamheter blir allt mer exponerade för cyberhot. Det andra är människa/maskin vilket handlar om artificiell intelligens (AI) och där utvecklingen handlar om exempelvis autonoma robotsystem eller där datorer är med i vissa beslutsprocesser. Det tredje, data/-individ, handlar om den mängd data som finns lagrad om olika individer.

Trafikverket (2021) beskriver att sjöfarten generellt ligger efter i sitt digitaliseringsarbete i jämförelse med övriga transportslag. Detta beror delvis på en lång livscykel för fartyg samt infrastruktur och utrustning i hamnar. För hamnar specifikt upplevs branschen som fragmenterad där varje hamn i regel är en enskild aktör. Utbytet av information mellan hamnar har länge varit begränsat och har i hög grad hanterats av andra berörda aktörer som exempelvis transportörer eller rederier. Utvecklingsarbeten utförda av hamnoperatörer är ofta fokuserade på den fysiska infrastrukturen i hamnen snarare än informationsflöden mellan hamnar (Trafikverket, 2021).

En del större hamnar har dock på senare tid börjat överta drift för andra hamnar och terminaler, vilket innebär en ökad möjlighet till implementation av gemensamma system mellan hamnar (Trafikverket, 2021).

6.1.1 Digitaliseringsarbetet idag

De hamnar som deltagit i studien arbetar samtliga med digitalisering i någon form och menar att det står högt upp på agendan. Graden av digitalisering skiljer sig mellan olika typer av hamnar. Till exempel är passagerartrafik mindre teknikberoende än gods, vilket beror på att det är fler steg för gods än för passagerare.

Passagerare ska bara få sin biljett och kliva på medan gods inte kan stå hursomhelst eller varsomhelst och måste lastas på ett visst sätt. Ett annat exempel är energihamnar där det genomförts en del automatisering men att osäkerheter kring branschens vara eller icke vara i framtiden inte motiverar till allt för stora investeringar.

Utveckling sker hos både hamnbolag och de terminaloperatörer som är verksamma i hamnarna. Vissa operatörer uppges ligga långt före i digitaliseringsarbetet, exempelvis DFDS och Stena Line. Samtidigt varierar det stort mellan olika operatörer och även om företaget i sig satsar på digitalisering är det inte säkert att man har en enskild hamn som sitt primära fokus och det blir ofta så att större internationella hamnar prioriteras när det gäller införande av digitaliseringsprocesser. Ett av hamnbolagen som deltagit i studien har tagit ett helhetsgrepp om digitaliseringsfrågor för hamnen för att få med sig samtliga aktörer som är verksamma där.

Ett särskilt fokus för digitaliseringsarbete i svenska hamnar de senaste åren har varit att nyttja de data och den funktionalitet som redan finns i systemen. Ett annat område som fler intervjuade lyfter är att öka effektiviteten i anlöpen. Ett exempel på ett projekt för att utveckla dessa är *EfficientFlow*, ett EU-finansierat projekt som syftar till att möjliggöra informationsdelning mellan fartyg och hamnaktörer. Bland annat skapar man ett system av köbrickor så att fartygen kan anpassa sin fart i god tid istället för att så snabbt som möjligt komma till hamnen och sedan vänta på sin tur (Sjöfartsverket, 2022a). Utöver EfficientFlow har Sjöfartsverket flera pågående projekt som syftar till att göra anlöpen smidigare (Sjöfartsverket, 2022b).

Vidare sker en del utveckling kopplat till den fysiska säkerheten där framförallt inpassering och kameraövervakning gjorts både säkrare och mer automatiserat. Vid intervjuerna lyftes också funderingar kring att kunna använda drönare för övervakning av området, något som idag finns i vissa utländska hamnar.

6.1.2 Utvecklingen framöver

Samtliga hamnaktörer som deltagit i studien framhåller att digitaliseringen av hamnar kommer öka framöver. Alla vill ha tillgång till mer information och det ska gå mycket snabbare. De argument som framförs för att titta mer på autonoma eller delvis autonoma system är att det: (1) är billigare i längden, (2) minskar risken för skador, (3) ger högre effektivitet, exempelvis eftersom hamnen kan vara aktiv dygnet runt, (4) möjliggör distansarbete för användning av exempelvis kranar eller lastare, (5) förbättrar arbetsmiljö då exempelvis kranförare slipper sitta i icke-ergonomiska ställningar samt (6) bidrar positivt till att minska miljöpåverkan, till exempel lösningar som gör att fartyg kan anpassa sin hastighet och spara bränsle.

Ett intervjuat hamnbolag uppgav att deras kommande digitalisering sker utifrån tre perspektiv:

1) Godsflödet. Hamnen är kontaktpunkten mellan sjö och land. Med digitalisering vill hamnbolaget kunna tillgängliggöra information om godset mer än vad de gör idag mellan olika aktörer, och hamnen ska vara en globalt integrerad hamn. De vill synliggöra och tydliggöra transporter från sjö och landsida.
2) Fartygsanlöpet. Hamnen ska tillsammans med Sjöfartsverket se till att hamnanlöpen är säkra. Här vill hamnbolaget ha ett så bra informationsflöde som möjligt mellan de aktörer som är involverade i anlöpet. Det ger också mer effektiva hamnanlöp. Digitalisering kan underlätta just-in-time-leveranser, och minska tiden som fartygen ligger i hamn. Här går minskad miljöpåverkan och digitalisering hand i hand. Med digitalisering kan man, exempelvis genom bättre planering som leder till hastighetsreducering och därför mindre bränsleanvändning för fartygen, minska fartygens miljöpåverkan.
3) Digital tvilling[9]. Hamnen har idag inte hittat några bra tillämpningsområden för digitala tvillingar, men man ser att det kommer att bli viktigt framöver i och med automatisering och digitalisering.

En viktig aspekt för att kunna digitalisera mer framöver är standardisering. Av den anledningen betonade flera av respondenterna vikten av att samarbeta med andra hamnar så att de börjar använda samma standarder för att lättare kunna kommunicera med varandra. Eftersom de svenska hamnarna är relativt små i internationell jämförelse nyttjar de ofta samma lösningar, plattformar och system som andra hamnar, svenska och utländska, använder. Men hamnen måste också anpassa systemen utifrån den egna hamnens specifika förutsättningar.

6.1.3 Utmaningar

Digitaliseringen är dock inte utan utmaningar. Även om digitalisering kan medföra stora kostnadsbesparingar kan det vara dyra investeringar att göra, särskilt för små hamnar. Som nämnts tidigare kan det för energihamnar också vara svårt att se värdet av investeringar då deras produkter förväntas fasas ut på sikt.

En annan utmaning är tillgång på information då det ofta är flera olika bolag som verkar inom hamnarnas område, och de olika bolagen kanske inte får delge information om sina transporter. Informationsdelning mellan hamnar skapar därför en flaskhals i arbetet med digitalisering. Privata terminaloperatörer är många gånger en del av ett utländskt bolag vilket styr över de investeringar och utveckling som det lokala bolaget kan göra.

[9] Ett fysiskt objekt avbildat i en digital miljö.

En av de intervjuade hamnaktörerna menar att även om mycket av hamnens verksamhet hanteras digitalt så är det för det mesta möjligt att falla tillbaka på manuell hantering om de digitala systemen inte skulle fungera. En farhåga som lyftes var att manuell hantering fungerar med nuvarande personal men skulle kunna vara svårare att hantera för en yngre generation. Detta gör att hamnarna på sikt riskerar att tappa den robusthet det innebär att kunna driva verksamheten manuellt.

Fler av de intervjuade hamnaktörerna lyfte även säkerhetsaspekten och att digitalisering skulle kunna innebära en ökad känslighet för störningar och risk för angrepp. Samtidigt anger samtliga intervjuade att de aktivt arbetar med att inkludera säkerhetsfrågor i digitaliseringsprocessen.

6.2 Internationella exempel

I relation till andra länder ligger Sverige efter när det gäller digitalisering av hamnar enligt respondenterna. En anledning kan vara att svenska hamnar är relativt små och att investeringar därmed blir mer kostsamma. Samtidigt uppger en respondent att utmaningarna är ungefär desamma även utomlands, det vill säga att informationsdelning är en flaskhals.

Ett exempel på en hamn som kommit långt i sin digitaliseringsprocess är Los Angeles hamn (*Port of Los Angeles*), den största containerhamnen i USA. En drivkraft för just Los Angeles hamn är att de har utrymmesbrist vilket leder till att fartyg får ligga på kö onödigt länge. Därför finns det stora effektivitetsvinster med digitalisering och att fartyg exempelvis kan få en ”digital köplats” för att på så sätt kunna anpassa sin hastighet. I takt med att hamnen har digitaliserats har frågan om cybersäkerhet också aktualiserats. Hamnen driver därför sedan 2021 ett *Cyber Resilience Center* för att skydda hamnen och dess intressenter mot cyberattacker (Port of Los Angeles, 2022).

Ett annat exempel som lyfts fram är Rotterdams hamn (*Port of Rotterdam*) som är en av de största hamnarna i Europa och beskrivs som ledande inom digitalisering. Bland annat beskrivs användandet av en digital tvilling och att strävan är att hela hamnen ska finnas i en digital motsvarighet. Vidare beskrivs den framtida smarta hamnen som helt uppkopplad där sensorer talar om var olika gods befinner sig och möjliggör att kranar, gods, fartyg och andra transporter kan utbyta information direkt med varandra (Port of Rotterdam, 2022). Som ett konkret exempel har Port of Rotterdam bland annat utvecklat systemet *PortXchange*, vilket sedan 2019 drivs som ett eget företag. Systemet används för att planera anlöp så att fartyg inte behöver ligga på kö utanför hamnarna utan kan anpassa farten till sin tilldelade tid (PortXchange, 2022). PortXchange nyttjas idag av flera andra hamnar, däribland Houstons hamn (*Port of Houston*). Houstons hamn är en av USAs största hamnar med över 200 olika aktörer. Arbetet med digitalisering drivs därför av en intresseorganisation vilka har startat ett utbyte med företaget som driver PortXchange (Port of Houston, 2022).

Ovanstående exempel handlar alla om att hamnaktörer eller intressentorganisationer anslutna till hamnarna har tagit initiativ till effektivisering genom digitalisering. Framförallt handlar det om informationshantering i samband med anlöp vilket förutom effektivisering och lägre kostnader kan bidra till lägre klimatpåverkan från växthusgasutsläpp då mindre bränsle förbrukas av fartygen. När det kommer till digitalisering av cyberfysiska system såsom exempelvis kranar lyfts inte exempel fram av hamnarnas ägare. Detta kan bero på att denna utveckling sköts av internationella terminaloperatörer, vilka gör investeringar i flera hamnar som de opererar i.

7 Cyberhot och -angrepp

Under de senaste två decennierna har det inträffat ett antal uppmärksammade cyberangrepp som riktats direkt mot hamnar, eller som indirekt fått påverkan på deras verksamhet. Sannolikt finns det också ett mörkertal med angrepp som inte nått fram till media. I detta kapitel beskrivs kortfattat de konsekvenser som cyber-relaterade incidenter kan resultera i för hamnar och en generell beskrivning av olika typer av hotaktörer. Kapitlet avslutas med ett urval av några kända angrepp som drabbat hamnverksamhet.

7.1 Angreppets effekter

Hamnar ställs idag inför ett antal cyberrelaterade hot och utmaningar. En del av dessa är vad som kan anses generiska för IT- och OT-miljöer, medan andra är mer specifika för just hamnar. ENISA (2019) sammanställer vilken påverkan, som cyberrelaterade incidenter kan ha på hamnarna och deras funktion:

- Nedstängning av verksamheten
- Fara för liv och hälsa
- Stöld av gods
- Stöld av data
- Smuggling
- Fysisk ödeläggelse av utrustning
- Försämrat rykte och varumärke
- Miljökatastrof

Följande avsnitt beskriver kortfattat ovanstående effekter.

En *nedstängning av verksamheten* som varar längre än ett fåtal timmar kan få stora konsekvenser. Dels ekonomiska konsekvenser för de organisationer som påverkas, men det kan även få stora konsekvenser för en hel nation om transporter av bränsle, mat och andra nödvändiga produkter stannar av. En nedstängning kan även få säkerhetsmässiga konsekvenser i de fall då flera fartyg får köa för att komma in i hamnen, vilket ökar risken för olyckor i form av kollisioner.

Vid hamnar finns utrustning och verksamhet (såsom kranar, truckar, lastbilar, containrar som lyfts och staplas samt farligt gods) som vid manipulation kan innebära *fara för liv och hälsa*. Inom passagerarhamnar måste man även hantera flödet av människor och fordon på ett säkert sätt, vilket kan riskera att försvåras vid en cyberrelaterad incident där utrustning har manipulerats.

Stöld av gods kan innebära ekonomiska förluster för den påverkade organisationen och kan påverka andra organisationer och individer i senare steg av leveranskedjan. Detta utfördes exempelvis av angripare i Antwerpens hamn år 2011, vilket beskrivs i avsnitt 7.3.1.

I hamnar hanteras mycket värdefulla data som kan vara av intresse för en antagonist, exempelvis data gällande containerinnehåll. *Stöld av sådana data* kan användas av angripare för att hitta containrar med värdefullt innehåll, som i sin tur kan stjälas. Även detta var en del av angreppet mot Antwerpens hamn år 2011 (se avsnitt 7.3.1).

Smuggling var också ett syfte med angreppet mot Antwerpens hamn år 2011. Smuggling av exempelvis narkotika kan få betydande negativa konsekvenser för samhället i stort, men även smuggling av andra typer av varor såsom livsmedel eller kläder kan få negativa konsekvenser för ett samhälle då det finns potential för ekonomisk manipulation.

Fysisk ödeläggelse av hamnutrustning kan naturligtvis få ekonomiska konsekvenser om ny utrustning måste införskaffas, men ödeläggelse av hamnutrustning kan även påverka hamnens möjlighet för lastning och lossning av gods vilket i sin tur kan skapa förseningar och ekonomiska påföljder.

Ett försämrat rykte på grund av påverkan från cyberangrepp kan snabbt få stora konsekvenser för organisationer och hamnar då kunder kan dirigera om sin godstrafik till andra närliggande hamnar. Detta kan få ekonomiska konsekvenser för hamnen och dess anställda då tjänster kan försvinna på grund av minskad efterfrågan.

På hamnområden förekommer miljöfarliga ämnen. Cyberrelaterade incidenter som leder till fysisk skada i form av exempelvis oljespill, gasexplosioner, utsläpp av föroreningar och förlisning av fartyg, har potential att orsaka svåra *miljökatastrofer*, med konsekvenser för liv både på land och i hav.

7.2 Hotaktörer

Generellt finns två olika typer av hot: avsiktliga och oavsiktliga. Oavsiktliga hot involverarar misstag eller handhavandefel som kan resultera i olyckor eller att sårbarheter uppstår, vilka sedan kan utnyttjas av en angripare. Avsiktliga hot involverar en aktör som aktivt försöker åsamka skada på en organisation, system, grupp eller individ.

Hotaktörer kan delas in i olika kategorier baserat på vilken teknisk och ekonomisk förmåga samt vilken motivation de har.

En indelning baserat på ovanstående aspekter resulterar ofta i en hotaktörslista med fyra olika nivåer, från låg förmåga och motivation till hög förmåga och motivation. Den lägsta nivån utgörs av de aktörer som ofta benämns som *script-kiddies*. Dessa individer eller grupper av individer är ofta opportunistiska och har en relativt låg kompetens och små ekonomiska tillgångar. Motivationen för script-kiddies varierar och kan exempelvis vara att de vill testa något de lärt sig eller ekonomisk vinning.

På nästa nivå återfinns så kallade *hacktivister* vars kompetens och ekonomiska tillgångar kan variera. Det som framförallt skiljer denna hotaktör från script-kiddies är motivation, då hacktivister generellt är politiskt eller ideologiskt motiverade.

På de två högsta nivåerna återfinns kriminella organisationer samt statliga aktörer. Dessa två aktörer har generellt högre förmåga och ekonomiska tillgångar än tidigare beskrivna hotaktörer och utgör således ett allvarligare hot. Kriminella organisationer är i regel motiverade av ekonomisk vinning. Statliga aktörer utgör det största hotet då de har störst förmåga och tillgångar till att utföra framgångsrika cyberangrepp. Statliga aktörer kan ha flera syften för att utföra cyberangrepp ofta används de dock som ett sätt att bland annat destabilisera eller underminera en annan nation och utgör då en typ av hybridhot eller gråzonsproblematik (se exempelvis angreppet mot Shahid Rajaee 2020).

Alla ovanstående hotaktörstyper kan utgöra potentiella hot mot hamnar och hamnverksamhet. I kommande avsnitt beskrivs några kända angrepp mot hamnar under de senaste åren. De exempel som presenteras där pekar framförallt ut de två mer avancerade hotaktörerna, statsaktörer och kriminella organisationer. Detta betyder dock inte att övriga aktörer inte utgör ett hot mot hamnar.

7.3 Tidigare angrepp mot hamnar

I detta avsnitt beskrivs några av de mest allmänt kända av de angrepp som riktats direkt mot hamnar, eller haft en indirekt påverkan på hamnar, som inträffat de senaste åren. Beskrivningen av angrepp är endast övergripande och avsnittet är inte heller uttömmande för alla cyberangrepp som har riktats eller påverkat hamnanläggningar. Syftet med avsnittet är att illustrera att cyberangrepp mot hamnanläggningar har inträffat och fortsätter att inträffa samt att belysa vilka konsekvenser sådana angrepp kan medföra.

Av följande beskrivna incidenter involverar en majoritet användandet av ransomware (gisslanprogram). Dessa program är en typ av skadlig kod vars syfte är att utpressa organisationer och individer på pengar genom att kryptera hårddiskars innehåll. Vanligen möts den legitima användaren av någon typ av meddelande på skärmen när de försöker starta sin dator som beskriver att deras dator krypterats och att de mot betalning, ofta i kryptovaluta, kommer att få nyckeln för att låsa upp datorn och dess innehåll igen.

7.3.1 Antwerpen 2011

Antwerpen i norra Belgien har en av Europas största hamnar. År 2011 utsattes hamnen för ett utstuderat cyberangrepp. Hamnarbetare började upptäcka att hela containrar försvann från hamnområdet utan någon förklaring. Det visade sig att en grupp narkotikahandlare anlitat hackare för att ta sig in i datornätverken för minst

två olika organisationer som var verksamma inom hamnen i Antwerpen. Intrånget ska ha inneburit att man fick tillgång till detaljerad information om containrar, vilket i sin tur innebar att narkotikahandlarna kunde skicka in lastbilschaufförer i hamnområdet för att stjäla containrar, innan ägaren hade hunnit hämta dem. Genom den information som narkotikahandlarna fick tillgång till via nätverksintrånget kunde de börja smuggla narkotika i containrar med legitimt gods, som sedan hämtades upp när det anlände till hamnen i Antwerpen (Bateman, 2013; Nicaise 2022).

7.3.2 Maersk 2017

A. P. Møller Mærsk A/S, vanligen omnämnt Maersk, är ett av världens största rederier och fraktföretag. Under 2017 utsattes de för ett av de mest uppmärksammade ransomware-angreppen som hittills inträffat. Den skadliga kod som nyttjades i samband med angreppet, NotPetya[10], har blivit starkt förknippat med just Maersk. Detta trots att Maersk varken var det företag som drabbades värst eller var ett utstuderat mål för angreppet (Greenberg, 2018).

NotPetya är en skadlig kod som primärt byggs upp av EternalBlue[11] och Mimikatz[12]. NotPetya fick sitt namn från ransomware-koden Petya, som utpressade angripna organisationer på pengar för att återställa de låsta systemen. Till skillnad från Petya är dock NotPetya bara destruktiv, eftersom det krypterar angripna systems MBR[13] (Master Boot Record) på ett sätt så att de förstörs och inte är möjliga att återställa (Greenberg, 2018).

Via en enda dator i Maersks kontor i Odessa, infekterades hela organisationens nätverk. Drygt 45 000 datorer och 4 000 servrar infekterades med NotPetya och blev därmed obrukbara. Angreppet resulterade i att Maersks centrala verksamhet slutade fungera, kunder kunde inte boka frakt och gods kunde inte hämtas upp. Detta fick i sin tur konsekvenser både för Maersks kunder och för andra företag i leveranskedjan. Exempelvis påverkades även transportföretag som transporterar gods mellan kund och hamn, kunder till kunder och så vidare. Den uppskattade totala kostnaden för angreppet är över 100 miljarder SEK. För bara Maersk var kostnaden 30 miljarder SEK, enligt dem själva (Greenberg, 2018).

7.3.3 Long Beach 2018

Hamnen i Long Beach är USAs näst största hamn sett till transportvolym efter Hamnen i Los Angeles. I juli 2018 utsattes en aktör i hamnen för ett ransomware-angrepp. Angreppet påverkade företagets e-postsystem och hemsida. Den lokala

[10] https://attack.mitre.org/software/S0368/
[11] https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf
[12] https://attack.mitre.org/software/S0002/
[13] MBR utgörs av den första sektorn av en hårddisk och innehåller bland annat exekverbar kod som används för att ladda datorns associerade operativsystem.

organisationen valde så fort angreppet uppdagades att isolera sig från företagets kontor i andra regioner i syfte att minimera risken för att ransomware-angreppet spred sig dit (Paris, 2018).

Enligt företaget påverkade angreppet inte fraktverksamheten men innebar att kommunikation med kunder försvårades (Mongelluzzo, 2018).

7.3.4 San Diego 2018

Hamnen i San Diego är en av USA:s viktigaste hamnar och är utpekad som en ”strategisk hamn för USA:s försvarsdepartement” (Senzee, 2019). Den 25 september 2018 utsattes hamnen för ett cyberangrepp. Hamnens IT-avdelning började få rapporter från användare om att deras datorer hade låst sig och visade ett meddelande om lösensumma för att låsa upp datorn igen. IT-avdelningen agerade genom att be alla anställda att stänga av sina datorer. Enligt ett press-meddelande dagen efter angreppet uppgav hamnkontoret att man utsatts för ett cyberangrepp och att man arbetade tillsammans med experter samt lokala och federala partners för att minimera effekterna av angreppet. Vidare specificerades att angreppets påverkan endast var på administrativa system och att hamn-verksamheten i stort fungerade som normalt (Senzee, 2019).

Det är okänt vilken ekonomisk påverkan som angreppet orsakade. Hamnens respons har dock hyllats i USA som ett framgångsfall sett till hur man bör hantera ett ransomware-angrepp. Att de anställda snabbt stängde av sina datorer minskade sannolikt angreppets potentiella konsekvenser (Senzee, 2019).

7.3.5 Shahid Rajaee 2020

I maj 2020 utsattes hamnen Shahid Rajaee i Iran för ett sofistikerat cyberangrepp. Enligt uppgifter i Washington Post kraschade alla datorer som hanterar trafikflöde och godshantering i hamnen samtidigt, vilket resulterade i stora förseningar och köer både på land och till havs, då gods varken kunde lastas eller lossas (Warrick & Nakashima, 2020).

Israel anklagades senare för att ligga bakom cyberangreppet och att angreppet skulle vara ett svar i en cyberangreppskedja som gått fram och tillbaka mellan Israel och Iran. Cyberangreppet mot Shahid Rajaee skulle enligt dessa uppgifter specifikt ha varit ett svar på ett cyberangreppsförsök mot vattendistributionen på den israeliska landsbygden (Warrick & Nakashima, 2020).

7.3.6 Transnet 2021

Transnet, ett Sydafrikanskt företag som bedriver verksamhet inom hamnar, tåg och rörledningar (pipelines) utsattes i juli 2021 för ett cyberangrepp. Senare identi-fierades angreppet som ett ransomware.

Enligt företaget var det endast containerhamnarna, och inte den totala verksamheten som påverkades så pass mycket att de fick stänga ner. Detta då ett av de system som påverkades av angreppet hanterade lastning, lossning och lagring av gods (ett så kallat Terminal Operating System, TOS). Angreppet ledde även till att företaget deklarerade *force majeure*, vilket är en vanlig klausul i avtal som innebär att ett företag inte kan åta sig sina avtalsenliga förpliktelser på grund av en händelse utom deras kontroll. Som ett resultat av angreppet och en del i att återställa funktion till verksamheten återgick företaget tillfälligt till manuell hantering av gods och fartyg (Toyana, 2021; Njini & Viljoen, 2021).

7.3.7 Houston 2021

Den 19 augusti 2021 tog sig hackare, som uppgavs vara finansierade av främmande makt, in i en webbserver i Houstons hamn. Angriparna utnyttjade en tidigare oupptäckt sårbarhet i en mjukvara för lösenordshantering. Väl inne i webbservern planterade de skadlig kod vilket skulle ha kunnat leda till ytterligare tillgång till interna IT-system. Inom två timmar efter det initiala intrånget stal angriparna alla inloggningsuppgifter till ett lösenordhanteringssystem, men kort därefter upptäcktes detta av hamnens IT-avdelning som svarade med att isolera den kompromitterade servern. Således kunde företaget låsa ut angriparna från interna system och förhindra beständig åtkomst (Lyngaas, 2021).

8 Generell bedömning av cybersäkerhetsmognaden

I detta avsnitt presenteras ett resonemang för bedömning av cybersäkerhetsmognad hos hamnar. På grund av intervjustudiens urvalsstorlek görs ingen individuell mognadsbedömning för respektive hamn inom studien. I de fall där texten inte uppger att alla respondenter svarat på samma sätt (exempelvis: Majoriteten av respondenter…) betyder det inte nödvändigtvis att en del hamnar uppfyllt en aspekt och andra inte. Det är istället mer troligt att frågan inte besvarades, vilket kan bero på att de tillfrågade inte hade kunskap att besvara en specifik fråga på ett tillfredställande sätt eller att frågan helt enkelt inte ställdes. Varken intervjustudien eller studien i övrigt har inkluderat en ingående och systemspecifik analys av respektive hamnorganisation, varpå en individuell bedömning troligtvis skulle rendera ett missvisande resultat. Istället görs en övergripande bedömning som primärt baseras på ENISA:s (2020) rapport om cybersäkerhetshantering för hamnverksamhet.

ENISA (2020) förser hamnoperatörer med praxis för bedömning av cyberrelaterade risker. ENISA:s modell går i linje med riskbedömningsmetodologin som beskrivs i ISPS-koden (se avsnitt 4.1.1) och mot annan relevant EU-lagstiftning för hamnar och hamnverksamhet. ENISA:s modell utgår från en uppsättning åtgärder som bedöms vara betydelsefulla för en god cybersäkerhetsutveckling. I vilken utsträckning som en organisation vidtagit dessa åtgärder ger en bild av dess cybersäkerhetsmognad. En beskrivning av åtgärderna återfinns i Bilaga B – ENISA rekommendationer.

I studiens intervjuer inkluderades frågor som baserats på ett urval av åtgärderna från ENISA (2020). Alla åtgärder representeras dock inte explicit av de frågor som ställdes. Därav kan frågorna och svaren liknas vid ett stickprov snarare än en fullständig genomgång. Det är även så att alla frågor relaterade till aspekterna inte ställdes under varje intervju, eftersom målet inte var att bocka av alla aspekter utan att istället få en bättre känsla för hur organisationen i fråga arbetar kring cybersäkerhet.

Nedan presenteras de åtgärder från ENISA som på olika sätt besvarades under intervjuerna. Detta ämnar ge en indikation om huruvida de intervjuade hamnarna uppfyller aspekten eller inte, vilket sedan sammantaget kan leda till en form av övergripande bedömning av cybersäkerhetsmognaden.

Den första åtgärden i ENISA (2020) är *Säkerhetspolicy*. Denna åtgärd beskriver att en organisation, för att uppfylla aspekten ska ha en informationssystemssäkerhetspolicy (ISSP), som inkluderar alla organisatoriska och tekniska processer och system, inklusive OT. Alla intervjuade hamnar har någon form av policy om

IT-säkerhet, antingen en separat policy för informationssäkerhet och IT-säkerhet eller en eller flera policyer som på annat sätt inbegriper dessa områden.

Åtgärden *Hot- och riskhantering* inbegriper att organisationen ska säkerställa att risker identifieras och hanteras, att säkerhetsplaner beaktar cybersäkerhetsaspekter, att en process finns för att kontinuerligt samla in information om sårbarheter och nya hot och risker, samt att en metod finns för att utvärdera hur väl hamnen lever upp till säkerhetspolicyn. Respondenternas svar kring denna fråga har varierat, en del uppgav att de inte aktivt på egen hand samlar in information kring sårbarheter och nya hot och risker. En del uppgav att de utför en viss omvärldsbevakning där information spridits inom organisationen. I de fall där hamnen inte själv utför aktiv omvärldsbevakning om nya sårbarheter, samt hot och risker, görs detta istället genom kommunen som sedan för informationen vidare till hamnen.

Gällande ENISA:s åtgärd *Molntjänster* svarade alla respondenter att de i största möjliga mån vill undvika sådana lösningar. Ibland är detta dock inte möjligt, vilket bland annat beror på att en del hamnar är beroende av kommunens IT-avdelning och de beslut som fattas för kommunen som helhet. Hamnarna är dock noga med att hamnens IT-system inte placeras i molnet. Åtgärden inkluderar bland annat att organisationen har en process för att utvärdera effekter och risker med att välja molnlösningar.

Åtgärden *HR-säkerhet* beskriver delvis att organisationer utvecklar obligatoriska cybersäkerhetsutbildningar för nyckelpersonal samt har ett program för att öka säkerhetsmedvetenheten hos hamnens aktörer. Alla medverkande uppger att de har genomfört utbildningar med sin personal. I vissa fall ges sådan utbildning i regi av kommunen, i andra fall är det hamnen själv som upprättat utbildningen. Dessutom genomförs i vissa fall säkerhetskontroller på personal som arbetar med kritiska IT- och OT-system. En del respondenter uppgav att de önskar ytterligare utbildning inom cyberområdet.

I relation till åtgärden *Cyberresiliens* ställdes frågan *finns det en plan för kontinuitets- och krishantering relaterat till cyberrelaterade händelser?* Flera hamnar har genomfört övningar för krishantering och samverkan med myndigheter. Vidare beskriver alla respondenter att hamnens verksamhet till stor del kan hanteras manuellt, men påpekar samtidigt att arbetet i sådant fall skulle gå långsamt. Problemet blir istället större om rederiernas system för godshantering fallerar, som vid angreppet som drabbade Maersk 2017. Eftersom information kring gods, var det är och vart det ska inte finns tillgängligt i sådana fall försvåras hamnens arbete med lastning, lossning och omlastning. Hamnarna uppgav även att det finns viss redundans för kritiska system exempelvis för vissa servrar och även redundant fiberanslutning.

Åtgärden *Inventering av tillgångar* innebär att utföra kontinuerlig inventering av tillgångar, vilket i detta fall bland annat avser applikationer, mjukvaruplattformar,

nätverk, nätverkskomponenter, servrar och datorer. Syftet med detta är att säkerställa att endast godkända enheter och programvara används i organisationens nätverk. Majoriteten av de tillfrågade utför sådan kontinuerlig inventering.

Åtgärden *Ändpunktsskydd och livscykelhantering* innebär att organisationen i fråga ska ha en strategi för att skydda hamnens klientenheter. Strategin bör inkludera implementering av säkerhetsåtgärder på klientenheter som bland annat inkluderar antivirus, kryptering, härdning och andra liknande åtgärder. Dessutom bör det finnas en säker process för att introducera nya enheter i hamnens nätverk samt vitlistning av hård- och mjukvara. Majoriteten av de tillfrågade uppger att de har en strategi för att hantera och introducera nya enheter.

Åtgärden *Åtkomstkontroll* avser i sammanhanget att hamnen ska vidta åtgärder för att begränsa obehörig tillgång till hamnens system digitalt och avser således inte fysisk åtkomstkontroll vilket istället täcks av den sista åtgärden *Fysiskt skydd av IT- och OT-system*. Där kan sägas att alla hamnar i studien har ett fysiskt skalskydd till hamnområdet med omringande stängsel samt kontrollerad in- och utpassering. Gällande digital åtkomstkontroll finns åtgärder och rutin för att hantera detta, däremot uppger en del respondenter att de upplever att de varit lite för generösa med tillgång för externa konsulter till interna system. Samtidigt uppgavs att detta är något de jobbar på att åtgärda.

Sammanfattningsvis kan sägas att hamnarna som deltagit i studien har ett påbörjat cybersäkerhetsarbete utifrån ENISA:s rekommendationer vilket kan ge en viss indikation på deras cybersäkerhetsmognad. Dock har inte respektive punkt studerats i detalj så det är oklart hur långt de har kommit i arbetet. Överlag bedömer hamnaktörerna själva att de kommit en bit på vägen men att det fortfarande finns mycket kvar att göra.

9 Cyberövning och träning inom hamnsektorn

En majoritet av de aktörer från svenska hamnar som intervjuats i denna studie uppger att de har utfört eller regelbundet utför någon form av cyberträning inom sina respektive organisationer. Dessutom utför flera svenska hamnar andra typer av övning och träning, ibland tillsammans med andra organisationer och myndigheter som exempelvis Försvarsmakten.

När det gäller storskaliga övningar och utbildning kring cybersäkerhet relaterat till hamnar har denna studie inte funnit några svenska exempel. Däremot genomförs övning och träning som inte direkt relaterar till eller fokuserar på cybersäkerhet, vilka istället lägger fokus på krishantering och myndighetssamverkan. Internationellt finns ett fåtal dokumenterade exempel på övning och träning inom cybersäkerhet och hamnar. Två sådana exempel inkluderar nyttjandet av en så kallad cyber range eller cyberanläggning (Potamos, Peratikou och Stavrou, 2021; Jacq, Salazar, Parasuraman, Kuusijärvi, Gkaniatsou, Latsa och Amditis, 2021), vilka kan liknas med cyberanläggningen Crate[14] hos FOI i Linköping. Dessa anläggningar består av virtualiseringsservrar som kan nyttjas för att skapa virtualiserade miljöer. Miljöerna kan i sin tur användas för såväl forskning som övning och träning inom cyberområdet.

I Potamos m. fl. (2021) beskrivs en digital infrastruktur som av författarna kallas Maritime Cyber Range (MCR). MCR beskrivs bestå av två olika delar, en del som simulerar ett eller flera skepp och en del som simulerar ett landbaserat kommunikationscenter för sjöfart. Det virtualiserade kommunikationscentret består av olika enheter och verktyg som är nödvändiga för att kommunicera med fartyg. I tillägg finns system som flottledningssystem, kustövervakningssystem och diverse integrationer från tredje part. Den andra delen av MCR består av segmenterade nätverk med diverse subnätverk. Detta inkluderar bland annat ett administrativt nätverk uppdelat i tre subnätverk (operationellt, logistik och intern kommunikation). Därutöver finns ett nätverk för fartygets kommandobrygga, som i sin tur är uppdelat i tre subnätverk. Det finns även kontrollsystem för att hantera cyberfysiska aspekter såsom motorstyrning (Potamos, Peratikou och Stavrou, 2021).

Författarna beskriver att MCR kan nyttjas i cybersäkerhetsträning och forskning. Ett sådant användande skulle kunna öka situationsmedvetenheten relaterat till cyberområdet för både hamnarbetare och besättningen för ett skepp. Det framstår dock som att MCR är mer fokuserat på fartyg snarare än hamnverksamhet och det beskrivs inte heller om infrastrukturen faktiskt har nyttjats praktiskt i övning eller träning.

[14] https://foi.se/crate

Jacq m fl. (2021) beskriver Cyber-MAR projektet, ett EU-projekt inom H2020[15], i vilket en cyberanläggning utvecklades. Den utvecklade cyberanläggningen har designats och utvecklats i nio olika lager. Dessa lager inkluderar bland annat ett lager för simulering av fartyg, ett utbildningslager, ett lager för nätverksövervakning och ett ekonomiskt modelleringslager för att uppskatta kostnader till följd av angrepp som leder till att hamnverksamheten stannar av. I tillägg nyttjas även riktiga cyberfysiska system och enheter som exempelvis PLC[16]:er.

Till skillnad från cyberanläggningen som presenteras i Potamos, Peratikou och Stavrou (2021) ligger fokus i Jacq m fl. (2021) på att utveckla en cyberanläggning som fokuserar på hamnarna och hamnverksamheten. I tillägg har Jacq m fl. (2021) utvecklat och använt ett angreppsscenario i anläggningen där man lyckats uppnå en hög grad av realism både i infrastrukturen för simulering i cyberanläggningen och i det scenario som nyttjats. Syftet med att utveckla denna cyberanläggning har varit att möjliggöra upptäckt av angrepp, minimera eller hantera risk samt att utbilda och träna personal. Författarna uppger att infrastrukturen är mogen nog att börja användas praktiskt.

[15] https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_en

[16] *Programmable Logic Computer* (PLC) är en särskild dator som används för att automatisera funktioner inom ett industriellt nätverk.

10 Diskussion och slutsatser

Denna studie har undersökt och kartlagt aktörer och system i svenska hamnar i syfte att stödja MSB i deras arbete att stärka skyddet för samhällsviktig verksamhet. Kartläggningen ska dock endast ses som en första överblick av området och inte som en fullständig genomgång. Detta beror till stor del på att studien endast inkluderat en handfull hamnar av de drygt hundra som finns i landet.

Den bedömningen av cybersäkerhetsmognad som beskrivits i kapitel 8 ska inte heller ses som någon form av absolut bedömning, utan som en indikation på status för svenska hamnar i stort. En del av aktörerna i de intervjuade hamnarna har kommit längre i sitt cybersäkerhetsarbete än andra. Detta kan delvis bero på skillnader i hamnarnas storlek och i deras respektive ekonomi, vilket innebär att det helt enkelt finns större utrymme för sådant arbete i vissa hamnar. Generellt kan dock sägas för alla hamnar inom studien att man är medvetna om den problematik som existerar gällande cybersäkerhet och vilka hot som finns. Samtliga hamnar inom studien bedriver även ett arbete för att öka sin cybersäkerhet och förmåga att möta cyberhot.

Det ska även påpekas att arbete kring cybersäkerhet och informationssäkerhet i stort inte är en enkel utmaning att tackla. Det finns en myriad av problem och svårigheter kring sådant arbete som existerar för alla typer av organisationer. ENISA (2019) specificerar ett antal problemområden relaterat till arbete med cybersäkerhet i hamnar. Dessa områden inkluderar bland annat avsaknad av tid och budget för cybersäkerhetsrelaterade aktiviteter, avsaknad av medvetandehöjande aktiviteter och behovet att hitta rätt balans mellan effektivitet och cybersäkerhet. Flera av respondenterna uppgav dock att de känner ett gott stöd från sina respektive hamnledningar kring arbetet med cybersäkerhet, vilket kan ses som ett av de viktigaste stegen för att överkomma de utmaningar som finns relaterat till området.

Under intervjuerna har informationsflöden efterfrågats i relation till flöden för gods och passagerare. Utifrån genomförda intervjuer har det varit svårt att konkretisera specifika informationsflöden, vilket bland annat beror på att det kan finnas skillnader i hur information flödar beroende på typ av gods eller aktör, men även på att det kan finnas skillnader i flödet för samma typ av gods. Vidare hanteras delar av flödet ofta manuellt i form av telefonsamtal eller e-post, vilket ytterligare försvårar skapandet av en konkret och sammanhängande modell av informationsflöden för rapporten.

En majoritet av respondenterna påpekade att de gärna vill ha mer styrning, riktlinjer och råd från myndigheter, däribland MSB. Detta i syfte att strukturera och förbättra arbetet kring områden som bland annat cybersäkerhet. Under sommaren 2022 publicerade Transportstyrelsen TSFS 2022:14 om föreskrifter och allmänna råd om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster

inom transportsektorn. I föreskrifterna finns bland annat information kring hantering av aspekter såsom härdning, segmentering, kryptering och behörigheter. Således är TSFS 2022:14 ett steg i rätt riktning kring att hjälpa hamnar med råd och riktlinjer i arbetet med cybersäkerhet.

Gällande digitalisering finns, som med arbetet kring cybersäkerhet, skillnader mellan olika svenska hamnar. Det finns även skillnader mellan svenska och utländska hamnar. En del svenska hamnar har kommit längre i sitt arbete än andra, men ur ett internationellt perspektiv ligger svenska hamnar generellt i början av digitaliseringsarbetet. Även gentemot andra transportslag i Sverige ligger sjöfarten generellt efter i digitaliseringsarbetet enligt Trafikverket (2021).

För utbildning, övning och träning inom cybersäkerhet har denna studie inte funnit några svenska exempel på övningar relaterat till cybersäkerhet i hamnar. Det finns ett fåtal internationella exempel på sådana övningar. De som tagits upp i denna rapport har nyttjat cyberanläggningar vilka kan liknas vid Crate hos FOI. Dessa exempel skulle kunna nyttjas som en utgångspunkt om det i framtiden blir relevant att inom Crate utveckla hamnspecialiserad övning och träning. I alla hamnar inom studien har man utfört medvetandehöjande träning för sina medarbetare, en del utför även sådan träning kontinuerligt.

Sammanfattningsvis kan sägas att hamnars informationsflöden är fragmenterade och svåra att få en helhetsbild av. Dock är påverkan på IT- och OT-system inte avgörande för hantering av gods utan det mesta kan hanteras manuellt även om det skulle innebära lägre hastighet i godsflödet. Cybersäkerhet är en viktig fråga för hamnars aktörer och uppges ligga högt på agendan hos hamnarnas ledningsgrupper. Detta är en viktig aspekt att få med i det framtida arbetet med digitalisering av hamnarnas verksamheter.

Referenser

Bateman, T. (2013). Police warning after drug traffickers' cyber-attack. *BBC News.* 16 oktober. https://www.bbc.com/news/world-europe-24539417 [Hämtad 2022-05-31]

ENISA. (2019). Port Cybersecurity – Good practices for cybersecurity in the maritime sector. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector [Hämtad: 2022-06-13].

ENISA. (2020). Guidelines - Cyber Risk Management for Ports. https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports [Hämtad: 2022-06-13].

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *WIRED.* 22 augusti. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Hämtad: 2022-06-20]

Greig, J. (2022). Prosecutors investigating cyberattacks affecting multiple Belgian and Dutch ports. *ZDNet.* 3 februari. https://www.zdnet.com/article/cyberattack-affecting-belgian-port-operations/ [Hämtad: 2022-06-20].

Gävle hamn. (2022). Gävle hamn. https://gavlehamn.se/en/home/ [Hämtad:2022-09-21]

Göteborgs hamn AB. (2022). Om Göteborgs hamn AB. https://www.goteborgshamn.se/om-hamnen/om-goteborgs-hamn-ab/ [Hämtad: 2022-09-21]

IACS. (2022). Recommendation on Cyber Resilience. https://iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr2-cln/ [Hämtad: 2022-09-29]

IAHP. (2020). Port community cyber security. https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf [Hämtad: 2022-09-29]

IMO. (2019a). SOLAS. https://www.imo.org/en/KnowledgeCentre/ConferencesMeetings/Pages/SOLAS.aspx [Hämtad: 2022-09-29]

IMO. (2019b). Maritime Cyber risks. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx [Hämtad: 2022-09-29]

ISA. (u.å.) ISA/IEC 62443 Series of Standards. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards [Hämtad: 2022-09-30]

ISO. (2022) ISO/IEC 27001. https://www.iso.org/standard/54534.html [Hämtad: 2022-09-29]

Jacq, O., Salazar, P. G., Parasuraman, K., Kuusijärvi, J., Gkaniatsou, A., Latsa, E., & Amditis, A. (2021, July). *The Cyber-MAR Project: First Results and Perspectives on the Use of Hybrid Cyber Ranges for Port Cyber Risk Assessment*. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (s. 409-414). IEEE.

KBV. (2022). Vår verksamhet. https://www.kustbevakningen.se/var-verksamhet/sjoovervakning/sjosakerhet/ [Hämtad: 2022-09-29]

Kentor. (2017). Ny app effektiviserar Göteborgs Hamn. https://mb.cision.com/Main/10935/2207469/639570.pdf [Hämtad: 2022-12-13]

Kjellsdotter Ivert, L., Merkel, A., Kalantari, J., Santén, V., Svanberg, M. & von Wieding. (2021). Intressentanalys av Sveriges hamninfrastruktur. Lighthouse.

Lyngaas, S. (2021). Hackers breached computer network at key US port but did not disrupt operations. *CNN*. 23 september. https://edition.cnn.com/2021/09/23/politics/suspected-foreign-hack-houston/index.html [Hämtad: 2022-06-07]

Mongelluzzo, B. (2018). Cosco's pre-cyber attack efforts protected network. *The Journal of Commerce Online.* 30 juli. https://www.joc.com/maritime-news/container-lines/cosco/cosco%E2%80%99s-pre-cyber-attack-efforts-protected-network_20180730.html [Hämtad: 2022-06-07]

Nagurney, A. (2021). Our economy relies on shipping containers. This is what happens when they're 'stuck in the mud'. World Economic Forum. https://www.weforum.org/agenda/2021/10/global-shortagof-shipping-containers/ [Hämtad: 2022-09-29]

Naturvårdsverket. (2022) *Hamnar – Vägledning om miljöfarlig verksamhet.* nv-vagledning-om-miljofarlig-verksamhet.pdf [Hämtad: 2022-12-15].

Nicaise, V. (2022). *Cybermarétique: a short history of cyberattacks against ports.* Stormshield. https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/ [Hämtad 2022-05-31]

Njini, F. & Viljoen, J. (2021). Transnet declares force majeure at SA ports over cyberattack. *Fin24.* 27 juli. https://www.news24.com/fin24/companies/transnet-declares-force-majeure-at-sa-ports-over-cyber-attack-20210727 [Hämtad: 2022-06-07].

Norrköpings hamn. (2022). Kort om Norrköpings hamn. https://www.norrkopingshamn.se/kort-om-oss [Hämtad: 2022-09-21]

Paris, C. (2018). China's Cosco Shipping Hit by Cyberattack in U.S. *The Wall Street Journal*. https://www.wsj.com/articles/chinas-cosco-shipping-hit-by-cyberattack-in-u-s-1532548557 [Hämtad: 2022-06-07]

Port of Houston. (2022). Smart port of Houston. https://www.smartportofhouston.com/ [Hämtad: 2022-09-15]

Port of LA. (2022). Cybersecurity. https://www.portoflosangeles.org/business/cybersecurity [Hämtad: 2022-09-25].

Port of Rotterdam. (2022). The digital port. https://www.portofrotterdam.com/en/to-do-port/futureland/the-digital-port [Hämtad: 2022-09-15].

SO. (2022). Svensk ordbok. https://svenska.se/so/?id=129291&pz=7 [Hämtad: 2022-11-21]
Senzee, T. (2019). What happened in ransomware attack on Port of San Diego. *San Diego Reader.* 10 april. https://www.sandiegoreader.com/news/2019/apr/10/city-lights-happened-ransomware-port-san-diego/ [Hämtad: 2022-06-07].
Sjöfartsverket. (2022a). EfficientFlow. https://www.sjofartsverket.se/sv/framtidens-sjofart/efficient-flow/ [Hämtad: 2022-09-13].
Sjöfartsverket. (2022b). Smarta anlöp. https://www.sjofartsverket.se/sv/framtidens-sjofart/smarta-anlop/ [Hämtad: 2022-09-13].
Stamford. (u.å.). Våra tjänster. https://hem.stamford.se/v%C3%A5ra-tj%C3%A4nster/ [Hämtad: 2022-09-30].
Stenérus Dover, A,. Lindgren, J. & Andersson, P. (2018). *NCS3 – Styrsystem i drivmedelskedjan*. FOI Memo 6387.
Stockholms Hamnar. (2021). Stockholms Hamnar Års- och hållbarhetsredovisning 2021. https://www.stockholmshamnar.se/siteassets/trycksaker/stockholms_hamnar_2021.pdf [Hämtad: 2022-08-04].
Stockholms Hamnar. (2022). Om oss. https://www.stockholmshamnar.se/om-oss/ [Hämtad: 2022-09-21].
Trafikanalys. (2019). Hamnar i fokus. PM 2019:7. pm2019_7-hamnar-i-fokus.pdf (trafa.se) [Hämtad: 2022-12-15].
Trafikanalys. (2021). Sjötrafik 2021. https://www.trafa.se/globalassets/statistik/sjotrafik/sjotrafik/2021/sjotrafik-2021.pdf [Hämtad: 2022-09-29].
Trafikverket. (2021). Hamnen som digital nod: Slutrapport. https://fudinfo.trafikverket.se/fudinfoexternwebb/Publikationer/Publikationer_005701_005800/Publikation_005764/Hamnen%20som%20digital%20nod_slutrapport%20(2021-09-30)%20TRV%202020%2050902.pdf [Hämtad: 2022-09-13].
Transportstyrelsen. (u.å). Frågor och svar om rapporteringskrav för fartyg. https://www.transportstyrelsen.se/sv/sjofart/Sjotrafik-och-hamnar/rapportering/Fragor-och-svar-om-rapporteringskrav-for-fartyg/ [Hämtad: 2022-11-21]
Toyana, M. (2021). Transnet cyberattack puts employees' salaries at risk while backlogs at ports mount. *Daily Maverick.* 26 juli. https://www.dailymaverick.co.za/article/2021-07-26-transnet-cyberattack-puts-employees-salaries-at-risk-while-backlogs-at-ports-mount/ [Hämtad: 2022-06-07].
Trelleborgs Hamn. (2021). Års- och hållbarhetsredovisning 2021. https://www.trelleborgshamn.se/wp-content/uploads/2022/04/Arsredovisning-2021_komprimerad-storlek.pdf [Hämtad: 2022-08-04].

Warrick, J. & Nakashima, E. (2020). Officials: Israel linked to a disruptive cyberattack on Iranian port facility. *The Washington Post.* 18 maj. https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html [Hämtad: 2022-06-07].

Lagstiftning

Europaparlamentets förordning om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar. (EG 725/2004). Europaparlamentet. https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32004R0725 [Hämtad: 2022-10-17]

Förordning om sjöfartsskydd. (2004:283). Infrastrukturdepartementet. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2004283-om-sjofartsskydd_sfs-2004-283 [Hämtad: 2022-10-17]

Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster. (2018:1175). Justitiedepartementet. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20181175-om-informationssakerhet_sfs-2018-1175 [Hämtad: 2022-10-17]

Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. (2018:1174). Justitiedepartementet. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174 [Hämtad: 2022-10-17]

Lagen om sjöfartsskydd. (SFS 2004:487). Infrastrukturdepartementet. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2004487-om-sjofartsskydd_sfs-2004-487 [Hämtad: 2022-09-29]

Lagen om fartygssäkerhet. (SFS 2003:364). Infrastrukturdepartementet. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/fartygssakerhetslag-2003364_sfs-2003-364 [Hämtad:2022-09-29]

Lagen om hamnskydd. (SFS 2006:1209). Infrastrukturdepartementet. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20061209-om-hamnskydd_sfs-2006-1209 [Hämtad: 2022-09-29]

Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. (MSBFS 2021:9). Myndigheten för samhällsskydd och beredskap. https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2021-9-anmalan-och-identifiering-av-leverantorer-av-samhallsviktiga-tjanster.pdf [Hämtad: 2022-10-17]

Sjöfartsverkets föreskrifter om sjöfartsskydd. (SJÖFS 2004:13). Sjöfartsverket. https://sjofartsverket.se/globalassets/om-oss/lagrum/sjofs/2000-2009/004-013.pdf [Hämtad: 2022-10-17]

Säkerhetsskyddslag (2018:585). Justitiedepartementet. https://riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-2018585_sfs-2018-585 [Hämtad: 2022-09-29]

Säkerhetsskyddsförordning. (2021:995). Justitiedepartementet. https://riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddsforordning-2021955_sfs-2021-955 [Hämtad: 2022-10-17]

Transportstyrelsens föreskrifter och allmänna råd om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom transportsektorn (TSFS 2022:14). Transportstyrelsen. https://www.transportstyrelsen.se/tsfs/tsfs%202022_14.pdf [Hämtad: 2022-09-29]

Bilaga A – Intervjuguider

Intervjuguide Hamnar

Inledande frågor

1. Vilken roll har du/ni i din organisation?
2. Vilken roll har ditt företag/organisation i hamnen?

Aktörer och regelverk

1. Vilka olika aktörer verkar i hamnen och vad är deras roller? (alt. Vilka olika aktörstyper finns generellt i en hamn?)
    a. Vem har ansvaret för hamnens övergripande funktion?
    b. Vilka andra aktörer i hamnen interagerar ni med?
2. Vilka aktörer och myndigheter är relevanta för hamnverksamheternas arbete med informations- och cybersäkerhet?
    a. Vem/vilka utför tillsyn?
    b. Berörs cybersäkerhet vid tillsyn? Hur?
3. Finns det specifika regelverk eller riktlinjer som reglerar informations- och cybersäkerhet i er verksamhet? Vilka krav ställs på de olika aktörerna inom hamnområdet?
4. Det ställs krav på IT-säkerhetsarbete (enligt säk.skyddslag, NIS…) för er som hamn att vidta säkerhetshöjande åtgärder – hur ser ni på dessa krav?
5. Lag om hamnskydd
    a. Hur arbetar er hamnsskyddsorganisation med informations- och cybersäkerhet?
    b. Vilket område innefattar en hamnskyddsplan? I hur stor utsträckning finns informations- och cybersäkerhet med i era hamnskyddsplaner?
    c. Finns det annan lagstiftning om säkerhet som tar vid, vid omlastning till annat transportslag? Vilken?
6. Finns det någon annan lagstiftning som är relevant för er verksamhet avseende informations- och cybersäkerhet?

Övergripande om system

1. Vilka informationsflöden finns för att hantera godsflödet (från väg/järnväg förvar/lastning/omlastning till sjöfart) genom hamnen?

2. Hur ser varje steg ut och vilka IT-system eller cyberfysiska system används?
    a. Vilken funktion har systemet?
    b. Leverantör? Vilka leverantörer har ni för era system?
    c. Vem driftar systemet? Inhouse eller externt?
    d. Hur gammalt är systemet? Hur ser omsättningen av systemet ut?
    e. Hur isolerat/skyddat är systemet? (uppkoppling mot Internet, central övervakning, skyddsprinciper etc.) patchning?
    f. Hur beroende är verksamheten av systemet (manuell styrning, redundans)?
3. Finns det IT-system som är generella? Vilka? (System som kan anses som en del av hamnen snarare än en aktör)
4. Vilka typer av OT-system finns i hamnen?
5. Finns andra typer av system?
6. Interagerar era system med system från andra organisationer i hamnen?
7. Finns det beroenden till externa system?
8. Vilka av de system ni har tagit upp är viktigast för hamnens funktion?
9. Finns det några generella skillnader mellan godshamnar och passagerarhamnar när det gäller vilka system som nyttjas?
    a. Vilka systemtyper är det i så fall som skiljer?
10. Hur arbetar din organisation med säkerhetsfrågor relaterat till era cyberfysiska system?
    a. Finns riktlinjer/strategier/policys?
    b. Utbildas personalen etc. kring sårbarheter för att upprätthålla och förbättra säkerheten? Har ni genomfört några övningar relaterat till cybersäkerhet?
    c. Sker kontinuerlig hot- och riskidentifiering?
    d. Sker kontinuerlig inventering av tillgångar (i termer av applikationer, mjukvaruplattformar, nätverk, nätverkskomponenter, servrar, OT-system, administrativa komponenter etc.)?
    e. Finns process för att hantera hamnens ändpunkter (genom säkerhetsåtgärder som antivirus, kryptering, härdning etc.), och process för säker introduktion av nya enheter (som acceptanstester)?
    f. Finns en plan för kontinuitets- och krishantering relaterat till cyberrelaterade händelser?
    g. Genomförs säkerhetskontroller för personal som arbetar med hamnens IT- och OT-system?
    h. Vidtas åtgärder för att begränsa obehörig tillgång till hamnens system? Och behörigas, som externa konsulter etc.

   i. Utvärderas effekt och risker med molntjänster?
   j. Finns backup för (de mest kritiska av) hamnens system?
11. Finns det någon aspekt kring skydd av cyberfysiska system som du känner dig bekymrad för, idag och i framtiden, för din egen organisations del/för branschens del? Hur utsatta är cyberfysiska system inom branschen, dvs hamnar?

Digitalisering

1. På vilket sätt sker digitalisering inom er hamn?
2. Hur tror du att hamnar kommer digitaliseras framöver? Vilka cybersäkerhetsaspekter kommer behöva beaktas i och med digitaliseringen?
3. Hur viktig är en fortsatt digitalisering av hamnens verksamhet? Vilka för- och nackdelar ser du med en fortsatt digitalisering?
4. Finns det exempel som du vet på utländska hamnar som kommit längre? Vilka?
5. Finns det några generella skillnader mellan godshamnar och passagerarhamnar när det gäller grad av digitalisering?

Övrigt

1. Är det något annat som vi inte har tagit upp som du vill tillägga?

Intervjuguide Myndigheter

Inledande

1. Vilken roll har du i din organisation?
2. Vilken roll har din myndighet gentemot hamnars verksamhet?

Myndighetens arbete

1. Hur arbetar myndigheten med tillsyn av hamnar? Ingår frågor om informations- och cybersäkerhet i tillsynsarbetet? Om inte, varför? Vilka är de centrala frågeställningarna vid en tillsyn?
2. Skiljer tillsynsarbetet beroende på vilken typ av hamn det är? Person, containrar etc
3. Finns det några krav att anmäla incidenter som rör cyberfysiska system till er eller till någon annan aktör? Hur går det till?
4. Bedöms cybersäkerhetsmognaden som en del i tillsynen? På vilket sätt görs det i så fall?

Aktörer och regelverk

1. Vilka aktörer och myndigheter är relevanta för arbetet med informations- och cybersäkerhet i hamnar?
2. Finns det specifika regelverk eller riktlinjer som reglerar informations- och cybersäkerhet i hamnar? Vilka krav ställs på de olika aktörerna inom hamnområdet?
3. Lag om hamnskydd
    a. Hur bör hamnsskyddsorganisationer arbeta med informations- och cybersäkerhet?
    b. Vilka områden innefattar hamnskyddsplaner? I hur stor utsträckning finns informations- och cybersäkerhet med i hamnskyddsplanerna?
    c. Finns det annan lagstiftning om säkerhet som tar vid, vid omlastning till annat transportslag? Vilken?

Digitalisering

1. Är myndigheten på något sätt involverad i digitalisering av hamnar eller påverkas myndighetens arbete av det?
2. Hur tror du att hamnar kommer digitaliseras framöver?
3. Finns det exempel på utländska hamnar som kommit längre?
4. Vilka säkerhetsaspekter kommer behöva beaktas i och med digitaliseringen?
5. Finns det några generella skillnader mellan godshamnar och passagerarhamnar när det gäller grad av digitalisering?

Övrigt

1. Är det något annat som vi inte har tagit upp som du vill tillägga?

Bilaga B – ENISA rekommendationer

Säkerhetspolicy – organisationen har en informationssystemssäkerhetspolicy (ISSP), som inkluderar alla organisatoriska och tekniska processer och system, inklusive OT, och

- är godkänd av högsta ledningen
- beskriver roller och ansvar för alla berörda parter (intressenter)
- delas med alla berörda parter som verkar i hamnen
- årligen uppdateras utifrån säkerhetstester och riskanalyser för att hantera nya hot och risker.

Hot- och riskhantering – organisationen har en riskbaserat tillvägagångssätt i utvecklingen av hamnens cybersäkerhetsstrategi och

- säkerställer kontinuerligt att identifierade risker hanteras och att nya risker identifieras i tid
- att organisationens säkerhetsplaner (fysisk säkerhet och säkerhet kopplad till människor) beaktar cybersäkerhetsaspekter
- regelbundet uppdaterar riskanalyser för att identifiera nya hot och risker, framför allt i samband med nya projekt
- en metod för att bedöma och utvärdera hur väl hamnen lever upp till säkerhetspolicyn
- Har en process för att kontinuerligt samla information från interna och externa källor om sårbarheter och nya hot och risker.

Säkerhet och integritet genom design – organisationen har en metodik för säkerhetsbedömning och kontrollpunkter (riskanalys, arkitektursäkerhetsgranskning, säkerhetstester, säkerhetsgodkännande etc.) rörande befintliga och nya projekt, som

- tar hänsyn till hur kritiskt systemet är och dess exponering
- inkluderar cybersäkerhetsfrågor från design till implementeringsstadiet
- hanterar personuppgifter i linje med GDPR
- innehåller en process för att klassificera och identifiera kritisk information och kartlägga informationsflöden.

Inventering av tillgångar – organisationen har ett centraliserat och uppdaterat system för inventering av tillgångar (i termer av applikationer, mjukvaruplattformar, nätverk, nätverkskomponenter, servrar, OT-system, administrativa komponenter etc.) samt en policy som säkerställer att endast godkända enheter och programvara introduceras till nätverket.

Cyberresiliens – organisationen har en plan för kontinuitets- och krishantering som

- inkluderar definierade mål för krishantering och återställning av hamnens system, även parametrar som recovery time objective (RTO), recovery point objective (RPO), maximum tolerable outage (MTO) and minimum business continuity objective (MBCO)
- identifierar olika aktörers roller och ansvar vid krishantering och återställning
- fastställer en krisorganisation
- kontinuerligt övas med alla inblandade aktörer.

Ändpunktsskydd och livscykelhantering – organisationen har en strategi för att skydda hamnens klienter som inkluderar

- implementering av säkerhetsåtgärder som antivirus, kryptering, härdning etc.
- vitlistning för hård- och mjukvara som årligen uppdateras
- en process för säker introduktion av nya enheter i hamnens system (med exempelvis acceptanstester och valideringssteg)
- en policy som säkerställer att alla anställda och konsulter återlämnar sina klienter vid kontraktsavslut.

Sårbarhetshantering – organisationen har en implementerad process för att identifiera sårbarheter i sina system och för att sprida informationen till berörda parter samt vidta snabba motåtgärder. Därutöver finns nära samarbete mellan IT- och OT-avdelningar som säkerställer en homogen cybersäkerhetsnivå för hamnens system.

HR-säkerhet – organisationen genomför säkerhetskontroller för nyckelpersonal som arbetar med hamnens IT- och OT-system, utvecklar obligatoriska cybersäkerhetsutbildningar för nyckelpersonal samt har ett program för att öka säkerhetsmedvetenheten hos hamnens aktörer.

Supply chain management – organisationen hanterar tredje part genom att

- åtkomst till hamnens system fås genom beviljad begäran, under en specificerad tid och för ett specifikt ändamål
- tydligt definiera relationen mellan hamnen och tredje part i avtal som inkluderar säkerhetsaspekter, inklusive upptäckt och hantering av incidenter

Kontroll och revision – organisationen utför regelbundet cybersäkerhetsrevisioner (som penetrationstester) för att kontrollera tillämpning och effektivitet i implementerade säkerhetsåtgärder samt bedöma hamnsystemens säkerhetsnivå.

Fysiskt skydd av IT- och OT-system – organisationen säkerställer att hamnens IT- och OT-system har adekvat fysiskt skydd samt att all underhållsverksamhet som görs på fysiska IT- och OT-system är spårbar.

Nätverkssäkerhet – organisationen arbetar med nätverkssegmentering för att begränsa spridning av attacker mot hamnens system och undvika direktåtkomst till kritiska system från internet, samt utför regelbundna nätverksscanningar för att upptäcka obehöriga och skadliga nätverk.

Åtkomstkontroll – organisationen vidtar åtgärder för att begränsa obehörig tillgång till hamnens system genom att

- ha ett centraliserat system för att hantera personalens åtkomsträttigheter till hamnens olika system och en process för att hantera och regelbundet se över åtkomsträttigheter (som automatisk avstängning av konton och riktlinjer för lösenord)
- där det är möjligt implementera individuella konton och förbjuda användningen av generiska konton
- ha regler för komplexa lösenord för åtkomst till hamnens system och införa flerstegsautentisering för åtkomst till kritiska system och kritisk data
- definiera specifika åtgärder för fjärråtkomst till hamnens system.

Administration och konfigurationshantering – organisationen har en policy för hantering av konfigurationer och administratörskonton och –rättigheter som inkluderar att endast nödvändiga tjänster och funktioner installeras.

Hothantering – organisationen har adekvata och uppdaterade anti-malware, anti-spam och anti-virusprogram installerade på hamnens alla system.

Molnsäkerhet – organisationen har en process för att utvärdera effekten och riskerna med att välja molnlösningar och inkluderar i största möjliga mån säkerhets- och tillgänglighetsaspekter i samband med avtal som rör molntjänster.

Maskin-till-maskin-säkerhet – organisationen har implementerat mekanismer för säkra utbyten maskin-till-maskin och tillhandahåller ömsesidig autentisering, integritet och konfidentialitet men hamnens system såsom kryptering, PKI eller digitala certifikat, digitala signaturer etc.

Skydd av data – organisationen har implementerat kryptografiska procedurer och mekanismer för att skydda konfidentialitet, riktighet och tillgänglighet för data i hamnens system.

Uppdateringshantering – organisationen har en process för att säkerställa att hamnens IT- och OT-system är uppdaterade som också säkerställer att uppdateringarna kommer från verifierade källor och att automatiska uppdateringar endast görs baserat på en riskanalys.

Detektion och övervakning – organisationen övervakar inloggning till och aktivitet vid hamnens kritiska system.

Backup – organisationen har backups, framför allt för hamnens mest kritiska system, som regelbundet underhålls och testas.

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se