DNV·GL

DIGITALE SÅRBARHETER LYSNEUTVALGET

Digitale Sårbarheter Maritim Sektor

Lysneutvalget

Rapport nr.: 2015-0569, Rev. 1
Dokument nr.: 1Q3LIZS-4
Dato: 2015-10-21

Prosjekt navn:	Digitale Sårbarheter Lysneutvalget	DNV GL AS DNV GL Oil & Gas
Rapport tittel:	Digitale Sårbarheter Maritim Sektor	Security & Information Risk
Kunde:	Lysneutvalget, C/O Fakturamottak Postboks	Management
	4900, Vika	P.O.Box 408
	8608 Mo i Rana	4002 Stavanger
	Norway	Norway
Kontaktperson:		Tel: +47 51 50 60 00
Dato:	2015-10-21	
Prosjekt nr.:	PP133089	
Organisation unit:	Security & Information Risk Management	
Rapport nr.:	2015-0569, Rev. 1	
Dokument nr.:	1Q3LIZS-4	

Kontrakt for leveranse av denne rapport:

Hensikt:

Utarbeidet av:	Verifisert av:	Godkjent av:
Pål Børre Kristoffersen Principal Consultant	Tore Hartvigsen Principal Consultant	Petter Myrvang Head of Section, Security & Information Risk Management
Arild Torjusen Principal Specialist		

DNV GL Distribution:

☒ Unrestricted distribution (internal and external)
☐ Unrestricted distribution within DNV GL
☐ Limited distribution within DNV GL after 3 years
☐ No distribution (confidential)
☐ Secret

Keywords:
Cybersecurity, Security, Digital Vulnerabilities, ,
Maritime, Information Risk Management,
Lysneutvalget

Rev. Nr.	Dato	Formål	Utarbeidet av	Verifisert av	Godkjent av
0	2015-05-26	Etter Høring	Pål Kristoffersen		
1	2015-10-21	Liten korrigering etter nye høringssvar	Pål Kristoffersen		

INNHOLD

1 SAMMENDRAG

Transport av varer med skip og import/eksport av disse varene via landets havner utgjør en kritisk funksjon i samfunnet. De fleste varer i internasjonal handel transporteres med skip, og utviklingen mot leveranser rett før produksjon («just in time») gjør at vitale samfunnsfunksjoner vil stoppe opp dersom sjøtransport eller havnefunksjoner stopper. Analyser i europeisk bilindustri viser at 48 timer etter en eventuell varestopp i havnene, vil produksjon bli berørt. En rekke næringer og enkeltpersoner vil bli berørt.

Maritim sektor har oppnådd en vesentlig rasjonalisering og forbedring av tjenestene ved å ta i bruk digital teknologi. Et moderne skip er avhengig av en rekke digitale systemer for navigasjon, motorkontroll, lastkontroll, sikkerhet og kommunikasjon. Offshoreflåten er eksempelvis avhengig av kompliserte systemer for dynamisk posisjonering. Samtidig forventer passasjerer og ansatte tilgang på internett om bord. Logistikk knyttet til vare- og passasjertransport er helt avhengig av sentrale IKT systemer og kommunikasjon mellom et stort antall aktører.

Digitale systemer har sårbarheter både i forhold til ikke villede feil og uhell, men også i forhold til villede handlinger som terror, sabotasje og hackeraktivitet. Norsk maritim sektor har ikke vært berørt av alvorlige hendelser knyttet til digitale sårbarheter, men flere mindre hendelser er identifisert, og alvorlige hendelser har skjedd i andre land. Det er kjent hvordan ondsinnet modifikasjon av navigasjonssignaler og identifikasjonssignaler kan medvirke til grunnstøting og kollisjon.

Det transporteres store mengder farlig last og ulykker med f.eks. eksplosiv last kan gi store skader på liv/helse og miljø. De verst tenkelige tilfeller vil være kollisjon mellom et fullastet cruise-skip og et skip med farlig last eller kollisjon mellom skip og oljeinstallasjoner.

Maritim sektor har nedlagt store ressurser i sikkerhet og beredskap i forhold til ulykker som grunnstøting, brann, eksplosjon etc. Det er også lagt ned store ressurser i fysisk sikring av bl.a. havneområder. Det er i liten grad lagt ned ressurser i sikkerhet i forhold til digitale sårbarheter. Det benyttes eksempelvis vitale systemer innen navigasjon og kommunikasjon som ikke er sikret mot digitale sårbarheter.

Tilsynsmyndigheter fører ikke tilsyn med sikring mot digitale sårbarheter.

1.1 Topp 10 digitale sårbarheter i maritim sektor

For å oppsummere observasjonene er det laget en overordnet opplisting av de 10 antatt mest relevante digitale sårbarheter i sektoren. Disse sårbarhetene er ikke innbyrdes sortert i henhold til kritikalitet:

- Manglende oppmerksomhet og opplæring hos de ansatte og underleverandører på sjø og land
- Navigasjonssignaler fra satellitt er normalt ikke beskyttet mot modifikasjon
- System for identifikasjon av fartøy er normalt ikke beskyttet mot modifikasjon
- Fjernoppkobling mot kritiske systemer for vedlikehold
- Et stort antall aktører utveksler mye informasjon på usikret e-post om skip, last og passasjerer
- Separasjon av datanett om bord og i havner
- Bruk av mobile lagringsenheter
- Bookingsystemer og administrasjonssystemer for passasjerer, last og havneanlegg er sårbare

- Manglende fysisk sikring av datarom, kablingsskap, m.m. på skip
- Begrenset autentisering av brukere mot systemer for offentlig innrapportering. System for autentisering av utenlandske borgere mangler.

1.2 Avhengigheter

Sjøtransporten er avhengig av en rekke systemer basert på digital teknologi:

- Globale posisjoneringssystemer (GNSS)
- Elektroniske kart og informasjonssystemer (ECDIS)
- Automatisk identifisering av skip (AIS/LRIT)
- Nettverksbaserte kontrollsystemer om bord for bl.a. styring og propulsjon
- Radiokommunikasjon (satellitt, MF/HF, VHF, UHF, mobiltelefon, kabel(i havn))
- Datakommunikasjon (Primært via satellitt, men også via WIFI og mobildata)
- Administrative systemer (Rapportering til myndigheter, rederi, lasteier, med flere)
- Landbaserte systemer for administrasjon av havneanløp, last, passasjerer mm.

1.3 Samarbeid

Varetransport med skip involverer en rekke aktører, og digitale media spiller en viktig rolle i dette samspillet. Fra en vare eksempelvis ankommer en havn i et fremmed land til den leveres ut av en norsk havn, har det foregått digital informasjonsutveksling med et stort antall parter.

Noen av Sjøfartsdirektoratets hovedoppgaver er å føre tilsyn med norskregistrerte fartøy og deres rederier samt å føre tilsyn med utenlandske skip i norske havner. Direktoratet ivaretar også funksjonen som realregister, og forvalter Norsk Internasjonalt Skipsregister (NIS) og Norsk Ordinært Skipsregister (NOR).

For NIS-fartøy er klasseselskaper gitt myndighet til å opptre på vegne av Sjøfartsdirektoratet.

Kystverket er en nasjonal etat for kystforvaltning, sjøsikkerhet og beredskap mot akutt forurensing. Kystverket arbeider aktivt for en effektiv og sikker sjøtransport gjennom å ivareta transportnæringens behov for fremkommelighet og effektive havner. Kystverket gjør forebyggende arbeid og reduserer skadeeffektene ved akutt forurensing, og medvirker til en bærekraftig utvikling av kystsonen.

Nasjonale etater som har et sterkt fokus på digitale sårbarheter som f.eks. NSM, PST og E-tjenesten har i varierende grad etablert samarbeid med maritim sektor.

Rederiene ønsker ikke et detaljert regelverk og tilsynsregime for digitale sårbarheter, men vil ha risikobasert tilnærming.

1.4 Beredskap

Maritim sektor er en foregangssektor i forhold til beredskapsplaner og øving av beredskap. Dette arbeidet fokuserer på utilsiktede hendelser om bord som grunnstøting, havari og brann. Disse planene har i liten grad innarbeidet digitale sårbarheter, og det er ikke identifisert øvelser som involverer slike hendelser.

1.5 Fremtidige problemstillinger og trender

Digitaliseringen av maritim sektor pågår kontinuerlig, og vil få økte muligheter etter hvert som høyhastighetsløsninger basert på satellitt og mobilnett blir mer tilgjengelig. Et stort utvalg forskjellige kommunikasjonsløsninger forsøkes å samordnes i prosjektet «maritim sky».

Det er gjennomført forsøk med ubemannede skip, noe som setter store krav til digitale systemer. Fokus på miljø og forurensing vil også sette større krav til avanserte kontrollsystemer for framdriftssystemer.

«The internet of things» vil spille en viktig rolle innen logistikksystemer for varetransport.

1.6 Overordnede risikoreduserende tiltak

Å sikre navigasjonssystemer og identifikasjonssystemer mot digitale sårbarheter vil være en omfattende prosess som vil involvere hele sektoren. Det mest brukte navigasjonssystemet (GPS) er kontrollert av USA, og dette systemet er ikke sikret mot ondsinnet modifikasjon av signalene. Andre systemer som f.eks. det russiske GLONASS må tas mer i bruk for å sikre redundans.

For å redusere digitale sårbarheter om bord på skip i havner og innen logistikk-kjeden for varehandel, trengs et økt fokus på dette i sektoren. IT-sikring har primært fokus i IT-avdelinger og innen deler av sikkerhetsmiljøet. Slike sårbarheter må få fokus i bedriftsledelse, bransjeorganisasjoner, standardiseringsorganisasjoner, forsikringsbransje og i offentlige tilsyn.

Beredskapsrutiner knyttet til digitale sårbarheter må innarbeides og må øves.

2 INNLEDNING

2.1 Bakgrunn

Titanic ulykken for over 100 år siden satte et stort fokus på sikkerhet innen maritim sektor. Dette var forløperen til at den første internasjonale konvensjonen om sikkerhet til sjøs, SOLAS (Safety of Life at Sea) ble utarbeidet. Etter dette har det vært en signifikant bedring av sikkerheten. Mens det i årene 1890-99 forliste 2050 norske seilskuter hvor det omkom hele 2716 norske sjøfolk, ble det i 2013 registrerte i alt 499 norskregistrerte fartøy som har vært involvert i en ulykke. Av disse er 251 registrert som arbeids- og personulykke hvor det omkom åtte personer.

Den første automatiske styremaskinen for skip ble utviklet i 1911. Dette var forløperen til en kontinuerlig automatisering av sektoren. Et moderne skip er avhengig av en rekke digitale systemer for navigasjon, motorkontroll, lastkontroll, sikkerhet og kommunikasjon.

Logistikk knyttet til vare- og passasjertransport har oppnådd en vesentlig rasjonalisering og forbedring av tjenestene ved å ta i bruk digital teknologi. Logistikk-kjeden involverer en rekke aktører og er helt avhengig av IKT systemer og kommunikasjon.

Passasjerer og ansatte forventer i dag tilgang på internett om bord og i havneområder.

Digitale systemer har sårbarheter både i forhold til ikke villede feil og uhell, men også i forhold til villede handlinger som terror, sabotasje og hackeraktivitet. Det er ikke kjent at norsk maritim sektor har vært berørt av alvorlige hendelser knyttet til digitale sårbarheter, men flere mindre hendelser er identifisert, og alvorlige hendelser har skjedd i andre land. Andre sektorer har opplevd alvorlige hendelser grunnet digitale sårbarheter.

For å angi konsekvensen av en grunnstøting, er ulykkene med Exxon Valdez, Full City og Costa Concordia beskrevet i faktabokser. Exxon Valdez ulykken angir en «verst tenkelig» miljøskade. For å angi «verst tenkelig» personskade, er brannen på Scandinavian Star beskrevet. For å angi de økonomiske konsekvensene dersom havner blir blokkert, er en arbeidskonflikt ved amerikanske havner omtalt. Ingen av disse uhellene er forårsaket av digitale sårbarheter, men de er tatt med for å angi mulige konsekvenser. (Etter disse ulykkene er det etablert en rekke risikoreduserende tiltak.)

Exxon Valdez ulykken regnes for å være en av de mest ødeleggende menneskeskapte miljøkatastrofer som har inntruffet. Ulykken inntraff den 24. mars 1989 da oljetankeren Exxon Valdez gikk på grunn på revet Bligh Reef i Prince William-sundet utenfor kysten av Alaska. Omlag 42 millioner liter olje lekket ut og spredte seg langs en 2000 km lang kystlinje. Avsides beliggenhet gjorde opprydningsarbeidet vanskelig. Arbeidet pågikk over 4 somre og på det meste deltok 10 000 personer. Exxon har estimert kostnaden for opprydningen til 2 milliarder dollar.

Det umiddelbare skadeomfanget for dyrelivet omfattet 250 000 sjøfugl, 2 800 havoter, 300 sel, 250 havørn, 22 spekkhoggere samt store mengder sild og laks. På lengre sikt er tallene betydelig høyere, mer enn 25 år etter ulykken er økosystemet rundt kysten av Alaska fremdeles påvirket av oljeutslippet og flere av de rammede dyrebestandene er ikke gjenopprettet. Det finnes fremdeles råolje fra ulykken på strender i området.

Faktaboks 1: Exxon Valdez ulykken /20/

Bulkskipet Full City grunnstøtte på Såstein utenfor Langesund natt til 31. juli 2009. Skipet var ankret opp utenfor Såstein 0,9 nautiske mil fra land. På grunn av sterk vind begynte skipet å drive mot land. Kapteinen klarte ikke å få kontroll over fartøyet og det grunnstøtte kort tid etter.

Skipet var da bunkret med om lag 1100 tonn tungolje og noe diesel. Ved grunnstøtingen fikk fartøyet omfattende skrogskader som medførte oljeutslipp. Dette forurenset kystlinjen, blant annet flere verneområder og fuglereservater, selv om mye av oljen ble tatt opp ble 191 tonn olje igjen i miljøet. Det ble levert ca 3000 tonn oljetilgriset avfall til deponering. Utslippet medførte forurensning i området fra Stavern i Vestfold til Lillesand i Aust-Agder, og ca 200 posisjoner ble forurenset med olje. Blant annet ble 37 vernede natur- og fugleområder og geologisk vernede områder tilsølt av olje. I tillegg ble mange friluftsområder og private eiendommer tilgriset av olje. Mer enn 2000 sjøfugl døde som en direkte årsak av hendelsen. Oljevernaksjonen ble pr 27. november 2009, estimert til ca. 234 millioner norske kroner.

Faktaboks 2: Full City /4/

Den 13. januar 2012 kl 21:45 traff cruiseskipet Costa Concordia en undersjøisk grunne ved øya Giglio utenfor Toscana i Italia. Skipet fikk et 50 meter langt hull under vannlinjen, tok raskt inn vann og fikk slagside. Skipet gikk en time senere på grunn på 20 meters dyp og evakuering ble beordret. Skipet hadde 4 252 personer ombord, 32 omkom. Skipets kaptein ble senere dømt til 16 års fengsel for uaktsomt drap, for å ha forårsaket en ulykke og for å ha forlatt skipet før alle passasjerer var evakuert.

Faktaboks 3: Costa Concordia /29/

MS «Scandinavian Star» var en havgående bilferge. Natt til 7. april 1990 var fergen underveis fra Oslo til Frederikshavn med 99 besetningsmedlemmer og 383 passasjerer ombord. Mellom kl. 01:45 og 02:00 begynte det å brenne i en bylt sengetøy på bildekket, denne brannen ble slukket. Noe etter startet en ny brann. Denne var i følge undersøkelseskommisjonen "overveiende sannsynlig antent ved bruk av bar ild". Ild og giftig røyk spredde seg deretter meget hurtig inn i lugarseksjonene og videre opp i skipet. 158 mennesker omkom i brannen. En person døde senere av skader fra ulykken. Ca. kl 03:20 oppgir kapteinen skipet og besetningen forlater det. Skipet tas under slep til Lysekil hvor brannen blir slukket den 8. april.

Faktaboks 4: Scandinavian Star /25/

En ti dagers lockout ved 29 havner på den amerikanske vestkysten i 2002 ble estimert til å koste USA 1 milliard dollar pr. dag. Det tok seks måneder før forsyningskjedene var tilbake i normal funksjon.

Faktaboks 5: Arbeidskonflikt ved amerikanske havner /5/

2.2 Hensikt

Digitalt sårbarhetsutvalg (Lysneutvalget) ble nedsatt av regjeringen den 20. juni 2014, og er ledet av professor Olav Lysne. Utvalget skal foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Utvalget skal levere sin utredning i form av en NOU til Justis- og beredskapsdepartementet innen utgangen av september 2015.

Mandatet til Lysneutvalget er omfattende og spenner over områder som sårbarhet i kritisk infrastruktur og samfunnsfunksjoner, datakriminalitet, personvern og sikring av informasjon. Lysneutvalget skal blant annet beskrive og analysere de digitale sårbarhetene som Norge står overfor i dag og nærmeste fremtid innen kritiske samfunnsfunksjoner og kritisk infrastruktur. Utvalget skal videre vurdere hvilke konsekvenser denne sårbarheten kan få for enkeltmennesker, næringsliv og samfunnssikkerhet, samt se på samarbeid mellom offentlige og private aktører.

DNV GL bistår Lysneutvalget med dette arbeidet innen maritim sektor.

2.3 Avgrensning

Grunnet kort tid til arbeidet, er følgende områder ikke behandlet:

- Konsekvenser for enkeltmenneske
- Fiskeri
- Havbruk
- Lystbåt
- Sjøforsvaret
- Olje & Gass installasjoner (Dette er behandlet i egen rapport /32/)
- Innsjø/Kanaler

2.4 Metodikk

For å kartlegge digitale sårbarheter innen maritim sektor har DNV GL benyttet følgende metodikk:

- Innsamling av relevant erfaring
- Gjennomføring av arbeidsmøter med relevante aktører:
    - Rederier
        - Service skip olje og gass
        - Passasjerskip
        - Generell frakt (RO-RO)
    - Rederiforeningen
    - Havneforeningen
    - Forsikringsbransjen
    - Leverandørindustri
    - Kystverket
    - Sjøfartsdirektoratet
    - Lysneutvalget
- Utarbeidelse av rapport

I arbeidsmøtene ble det benyttet kjent risikoanalysemetodikk. Deltakerne presenterte sårbarheter og årsaker, konsekvens og sannsynlighet ble diskutert. Risikoreduserende tiltak ble deretter diskutert.

2.5 Arbeidsgruppe

Følgende personer har bidratt på arbeidsmøter, samt kvalitetssikring av rapport:

- Nils Petter Andersen, Kystverket
- Olaf Gundersrud, DNV GL
- Janne Hagen, Lysneutvalget
- Bente Hjelle, Kystverket
- Elisabeth Hynne, Sjøfartsdirektoratet
- Knut Morten Johansen, Colorline

- Lene B. Kaland, Lysneutvalget
- Pål Kristoffersen, DNV GL
- Tor Langrud, Wilh. Wilhelmsen Holding
- Morten Alsaker Lossius, Sjøfartsdirektoratet
- Børge Nakken, Farstad Shipping
- Sofie Nystrøm, Lysneutvalget
- Line Falkenberg Ollestad, Rederiforbundet
- Oddbjørn Olsen, Colorline
- Knut Omberg, DNV GL
- Knut Svein Ording, DNV GL
- Svein Ringbakken, Den Norske Krigsforsikring for Skib
- Johanne Solheim, Norsk Havneforening
- Stein Susrud, Kongsberg Maritime
- Arild B. Torjusen, DNV GL
- Amir Zangeneh, Kongsberg Maritime

DNV GL har organisert arbeidet, og er ansvarlig for rapporten.

2.6 Forkortelser og definisjoner

AIS	Automatic Identification System
CERT	Computer Emergency Response Team
DP	Dynamic Positioning
DGPS	Differential Global Positioning System
ECDIS	Electronic Chart Display and Information System
GLONASS	Globalnaja navigatsionnaja sputnikovaja sistema, «Globalt navigasjonssatellittsystem»
GMDSS	Global Maritime Distress Safety System
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
HF	High Frequency
IKT	Informasjon- og kommunikasjonsteknologi
IMO	International Maritime Organization
ISPS	International Ship and Port Facility Security
IT	Informasjonsteknologi
JD	Justis- og beredskapsdepartementet

LRIT	Long Range Identification & Tracking
MF	Medium Frequency
NIS	Norsk Internasjonalt Skipsregister
NOR	Norsk Ordinært Skipsregister
NOU	Norsk Offentlig Utredning
NSM	Nasjonal Sikkerhetsmyndighet
OD	Oljedirektoratet
OT	Operasjonsteknologi
PST	Politiets Sikkerhetstjeneste
RO-RO	Roll On – Roll Off
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented System
SOLAS	Safety Of Life At Sea
TCP/IP	Transmission Control Protocol/Internet Protocol
UHF	Ultra High Frequency
USB	Universal Serial Bus
VHF	Very High Frequency
VPN	Virtual Private Network
VTS	Vessel Traffic Service
WIFI	WIreless FIdelity

3 DIGITALE SÅRBARHETER I MARITIM SEKTOR

Dette kapittelet fokuserer på digitale sårbarheter som er spesielle for maritim sektor. Det beskrives sårbarheter og det angis mulige konsekvenser. Disse sårbarhetene er ikke sortert i forhold til risiko. Risikoreduserende tiltak er beskrevet i kapittel 5.

Ettersom maritim sektor i stor grad benytter IKT, er sektoren selvsagt også eksponert for generiske digitale sårbarheter som sosial manipulering, fisking av informasjon, virus, tjenestenektangrep, inntrenging mm. Det benyttes i stor grad trådløse datanett i sektoren.

Norske maritime selskaper har ledende kompetanse, og det må forventes industrispionasje.

3.1 Navigasjon

Navigasjonsulykker (kollisjon, grunnstøting, kontaktskade) utgjør omtrent 50% av alvorlige skipsulykker /31/. Slike ulykker kan få store konsekvenser spesielt ved passasjertransport og ved transport av farlig last. Norskekysten har mange leder som er trange og krever presis navigering med hyppige kursendringer. Det er også betydelig transport av farlig eller forurensende last, blant annet i forbindelse med oljevirksomheten. Særlig Oslofjorden, Brevikstrømmen, Boknafjorden, Vatlestraumen og Fensfjorden er utsatte områder.

Seilaser i Norge med forhøyet risiko er generelt underlagt los-plikt, noe som reduserer mulige konsekvenser av sårbarheter i digitale systemer.

3.1.1 Posisjoneringssystemer

Globale posisjoneringssystemer spiller en stor rolle ved navigasjon. Det amerikanske GPS systemet har flere kjente sårbarheter. Signalene kan forstyrres (jamming), signalene kan modifiseres (spoofing) og amerikanske myndigheter kan degradere ytelse eller i spesielle tilfeller slå av tjenesten. Passasjerer kan benytte enkelt og rimelig utstyr til å forstyrre GPS signaler om bord. Erfaringer viser forøvrig at USA tilbyr en pålitelig tjeneste. De er selv avhengig av at det sivile GPS signalet fungerer.

Konsekvensen av utfall eller feil på globale posisjoneringssystemer kan være stor for eksempelvis offshorefartøy som holder posisjon tett inn til oljeinstallasjoner. For navigasjon i ledene langs kysten i god sikt, er konsekvensen mindre. Undersøkelser blant seilende navigatører viser at observasjon av land og navigasjonsinnretninger visuelt eller ved hjelp av radar, eventuelt også med los, er den viktigste navigasjonsmetoden. Denne metoden brukes oftest i kombinasjon med elektronisk stedfesting på elektroniske kart. Navigasjon basert på informasjon fra to separate kilder som kontinuerlig verifiseres opp mot hverandre anses som "best practice". Det er da viktig at begge kilder fungerer, men det blir ikke sikkerhetsmessig kritisk før begge kildene svikter samtidig.

GPS modifikasjon ("spoofing") er en type angrep der genuine GPS data modifiseres slik at fartøy mottar feilaktige GPS data. En navigatør ombord vil kunne tro at fartøyet er på korrekt kurs mens det ikke er det. Dette kan medføre feil-navigering og i verste fall kollisjon eller grunnstøting. GPS modifikasjon kan også påvirke havneoperasjoner ettersom GPS brukes i automatiserte løsninger for sporing og håndtering av containere og annen last.

GPS er sårbart for modifikasjon fordi signalene (i sivil GPS) ikke er sikret mot modifikasjon og fordi GPS protokollene ikke støtter sikker autentisering av avsender.

I et eksperiment i Juni 2013 viste forskere ved University of Texas (Austin) hvordan GPS modifikasjon kan påvirke et fartøys navigasjon. Ombord i skipet ble en innretning på størrelse med en koffert brukt for å sende falske signaler til skipets GPS mottakere. Skipets navigasjonssystem var ikke i stand til å avsløre at signalene var falske. Mannskapet ble lurt til å korrigere kursen i henhold til de falske GPS signalene slik at skipet kom ut av kurs uten at dette ble oppdaget. Utstyret som ble brukt kostet ca 20 000 kroner å produsere.

Faktaboks 6: GPS Digitale sårbarheter /6//8/

GPS blokkering ("jamming") vil si at en ondsinnet aktør blokkerer fartøyets mulighet til å motta GPS signaler. Utstyr for GPS jamming er lett tilgjengelig og finnes i ulike varianter fra håndholdte enheter til et par tusen kroner, til større enheter med en rekkevidde på 3-400 meter som kan anskaffes for rundt 100 000 kr. Til forskjell fra GPS modifikasjon vil man typisk lett oppdage at et blokkeringsangrep foregår, men konsekvensene kan være omfattende.

I en test med fartøyet Pole Star utført av "The General Lighthouse Authorities of the United Kingdom and Ireland" (GLA) så man at i tillegg til bortfall av GPS ble også andre systemer påvirket: DGPS mottakere, AIS transpondere, DP system og gyro kalibrering. På grunn av bortfall av GPS ble heller ikke ECDIS systemet oppdatert. GLA's hovedkonklusjon er at bortfall av GPS tjenester har betydelige konsekvenser for maritim sikkerhet.

Faktaboks 7: Digitale sårbarheter GPS – blokkering, *Pole Star* /7//8/

GPS blokkering har vært brukt av nasjonalstater i militær konflikt. Nord-Korea utførte tre slike angrep mot Sør-Korea mellom 2010 og 2012. I disse angrepene ble det brukt kraftig utstyr montert på lastebiler. Angrepene førte til flere rapporter om forstyrrelser for navigasjon og tidsberegning for fartøy, blant annet ble et amerikansk militært rekognoseringsfly tvunget til å nødlande. Angrepet i 2012 varte i 16 dager og påvirket i alt 1 016 fly og 254 skip.

Faktaboks 8: Nord-Korea blokkerer GPS signaler /8/

Magasinet The Economist" (July 13, 2013) presenterte et eksempel på GPS jamming. Nær «London Stock Exchange» skjedde det daglig en 10 minutters blokkering av GPS-signalene.

Navigasjonssystemet i biler stoppet opp og tidsangivelsene for finansielle transaksjoner ble påvirket. Årsaken viste seg å være en budbil hvor sjåføren benyttet en jammer for «å gjemme seg» for sentralen.

GPS jammere benyttes også av kriminelle for å "gjemme" bilen.

Faktaboks 9: GPS jamming i London /26/

I Januar 2007 ble GPS-signalene blokkert over hele San Diego, California. Dette påvirket «Naval medical Center», personsøkere sluttet å virke, havnevesenets trafikkovervåkingssystem feilet, fly trafikkontrollen måtte bruke sitt «back-up» system og bankautomater sluttet å virke. Det tok 3 dager å avdekke årsaken;
-to marinefartøyer utenfor San Diego gjennomførte en øvelse som involverte jamming av radiosignaler. Utilsiktet blokkerte dette GPS signalene over det meste av byen.

Faktaboks 10: GPS jamming i San Diego /26/

GPS sporsystemer benyttes for lokalisering og overvåking av last (containere) i transportkjeden. Dette gir forutsigbare ankomsttider og kan virke avskrekkende på potensielle tyver. Sporsystemet inneholder også informasjon om type last (klokker, tobakk, kjemikalier. osv.) En jammer kan «gjemme» containeren.

3.1.2 Elektronisk kart og informasjonssystem

Electronic Chart Display and Information System (ECDIS) er et navigasjonsinformasjonssystem som oppfyller krav som er fastsatt av den internasjonale maritime organisasjonen (IMO).

En kan benytte ECDIS som lovlig erstatning for papirkartet dersom det brukes offisielle kartdata som er produsert etter gitte internasjonale standarder og kravspesifikasjoner. I tillegg må en ha et godkjent back-up-system. Det betyr at man må ha to ECDIS-er om bord som er tilknyttet hver sin strømkilde. Det stilles også krav om at et ECDIS skal være typegodkjent.

Et ECDIS skal vise all sjøkartinformasjon som er nødvendig for sikker og effektiv navigasjon, og data skal være levert og godkjent av en autorisert sjøkartmyndighet. I Norge er Kartverket sjøkartmyndighet og deres sjødivisjon leverer og godkjenner sjøkartdataene.

Elektroniske kart og informasjonssystem må holdes løpende oppdatert. Dette skjer ved bruk av minnepinner, CD, e-post eller nettbaserte tjenester. Under oppdatering kan det spres virus, og det kan innføres tilsiktede og utilsiktede feil i kart og informasjon. Det ble på arbeidsmøte (Ref. kap. 2.4) omtalt et tilfell der nye nedlastede kart manglet dybdeinformasjon.

En ECDIS arbeidsstasjon tar inn navigasjonsdata fra en rekke sensorer som sammen med elektroniske kart gir et kraftig navigasjonsverktøy. Siden ECDIS er et knutepunkt som kobler sammen mange navigasjonssystemer vil en angriper som får tilgang til ECDIS ha mange muligheter til å villede navigatøren: modifisering av sensor data slik at operatøren får et feilaktig bilde; manipulasjon/tyveri av elektroniske kart; eller bruk av ECDIS som et tilgangspunkt for videre inntrengning. Sikkerhetsfirmaet NCC group har vist at man kan trenge inn i ECDIS systemer med enkle teknikker.

Faktboks 11: Digitale kart og ECDIS /14/

3.1.3 Digitale forstyrrelser på bro.

Antall grunnstøtinger med lasteskip i kystseilas har økt de senere år. Sjøfartsdirektoratets analyse av disse hendelsene viser at blant de mest sentrale årsakene til grunnstøting er feilvurdering av fart og kurs. Viktige årsaker til feilvurderingene er uoppmerksomhet eller manglende situasjonsbevissthet, utmattelse og trøtthet samt mangler ved fartøyets seilasplanlegging. Det fremheves at uoppmerksomhet kan skyldes at navigatøren er opptatt med andre aktiviteter enn de som er knyttet til jobbutførelse. Økt tilgang til internett om bord og bruk av for eksempel sosiale medier kan være en utfordring denne sammenhengen.

Faktaboks 12: Digitale forstyrrelser på broen /11/

Det er pålegg om innrapportering til havnemyndigheter og andre myndigheter bl.a. før ankomst. Slik innrapportering kan også virke forstyrrende på broen.

3.1.4 Overdrevet tillit til digitale navigasjonssystemer

Det finnes flere eksempler på at overdrevet tillit til digitale navigasjonssystemer kan medvirke til å svekke årvåkenheten hos navigatør eller skipsfører. Dette forsterker konsekvensen av angrep rettet mot slike systemer. En mulig fare er at operatørene enten ikke merker at et system er satt ut av spill eller ikke er tilstrekkelig beredt til å ta i bruk alternative navigasjonsmidler.

17 januar 2013 grunnstøtte minesveiperen USS Guardian på Tubbataha revet ved Filipinene. For å unngå ytterligere skade på revet, som er en UNESCO World Heritage Site, ble fartøyet kuttet opp og fjernet og gikk derfor tapt. US Navy betalte 2 millioner dollar i erstatning til Filipinene etter hendelsen. En granskningsrapport fant ingen enkeltårsak til hendelsen, men konkluderte med at ulykken kunne vært unngått og var et resultat av «poor voyage planning, poor execution, and unfortunate circumstances.» Spesielt påpekes det at for stor tillit til elektroniske kart var en medvirkende årsak: «the leadership and watch teams relied primarily on an inaccurate Digital Nautical Chart (DNC)® coastal chart during planning and execution of the navigation plan.» Selv om denne hendelsen skyldes menneskelig svikt og ikke ondsinnete handlinger viser den at den store tilliten til slike systemer er en risikofaktor.

Faktaboks 13: USS Guardian /23/

10. juni 1995 grunnstøtte det panamaregistrerte passasjerskipet Royal Majesty øst for Nantucket Island, Massachusetts. Skipet var da ca. 27 kilometer fra der offiserene trodde skipet var. Skipet, med 1509 personer om bord, var på vei fra St.George, Bermuda, til Boston, Massachusetts. Det var ingen dødsfall eller personskader som følge av denne ulykken. Skade på fartøy og tapte inntekter ble anslått til ca. 7 millioner dollar.

The National Transportation Safety Board fastslår at den sannsynlige årsaken til grunnstøtingen av Royal Majesty var offiserenes overdrevne tillit til de automatiske funksjonene i det integrerte brosystemet. Majesty Cruise Linje hadde ikke sikret at dets offiserer var tilstrekkelig opplært i de automatiserte funksjonene. Antenneledningen til GPS var dratt ut ved ett uhell.

Faktaboks 14: Royal Majesty /9/

3.2 Identifikasjonssystemer

Automatisk identifikasjonssystem («Automatic Identification System», AIS), er et antikollisjonshjelpemiddel for skipsfarten. Fartøyer som har utstyr for AIS om bord sender ut og utveksler informasjon om sin identitet, posisjon, fart, kurs, osv. over frekvenser på VHF-båndet. AIS brukes også av maritime trafikksentraler for å holde oversikt over skipstrafikken innen sine ansvarsområder.

Rekkevidden varierer, men kan være opp til omkring 40+ nautiske mil. Etter krav fra IMO skal fartøyer over 300 brutto registertonn i internasjonal fart ha utstyr for sending og mottak av AIS-signaler. Med visse unntak har de aller fleste skip har i dag AIS, det anslås at over 40 000 skip har AIS-utstyr klasse A om bord.

AIS er sårbart fordi systemet i liten grad er designet med tanke på digitale sårbarheter. Det er ingen kontroll av meldingers autentisitet og heller ingen kryptering. I en sikkerhetsevaluering utført av Trend Micro i 2013 ble det vist hvordan AIS kan angripes. Med enkelt utstyr kunne en angriper blant annet realisere følgende trusler:

- Endring av all AIS informasjon som sendes ut fra et fartøy.
- Forfalskning av fartøysinformasjon slik at ikke-eksisterende skip blir oppfattet av andre som faktiske fartøy. Dette kan også gjøres for å igangsette søk- og redningsfartøy (SAR) herunder helikoptre.
- Generere falske værmeldinger.
- Utløse falske kollisjonsvarsler (CPA)
- En angriper kan utgi seg for å være sjøfartsmyndigheter for å kunne manipulere fartøyets mannskap
- Utsending av falske mann over bord meldinger (SAR) meldinger for å lure et fartøy inn i et fiendtlig område.
- Ulike former for tjenestenekt-angrep for å hindre legitim AIS trafikk.

Realisering av en av disse eller flere i kombinasjon kan ha ulike og omfattende konsekvenser.

Faktaboks 15: AIS Digitale sårbarheter /12/

Det er ikke kjent tilfeller der modifiserte AIS-signaler har ført til ulykker, men manipulerte AIS signaler kan medføre kollisjonsfare, selv om en bemannet bro skal reagere på slike hendelser. Trafikksentraler benytter dypgang informasjon i AIS signalene for å dirigere fartøy. Modifiserte data om dypgang kan medføre grunnstøting.

Modifiserte AIS signaler er ikke lett synlige for bruker og kan gi feilaktig vurdering av den aktuelle kollisjons- og/eller grunnstøtingsrisikoen og derigjennom bidra til en gal beslutning.

AIS signalene benyttes av Kystverket, Hovedredningssentral, Kystvakt, Trafikksentraler, Toll, Politi og Sjøfartsdirektoratet. Kystverkets trafikksentral i Vardø benytter AIS informasjon til å identifisere skip som passerer grensen mot Russland. Falske AIS signaler kan benyttes for å skjule et skips identitet.

AIS data er tilgjengelig på åpne websider og fra mobile applikasjoner (apper). Dette utgjør en sårbarhet ved at «alle» kan vite et skips identitet, dimensjoner, hastighet mm.

For ikke land-nære områder ble et satellittbasert langdistansesystem for identifisering og sporing av fartøy innført i Norge i 2009 (LRIT).

3.3 Industriell automasjon-, kontroll- og sikkerhetssystemer

Tradisjonelt har skip vært bygget med enkeltstående og autonome kontroll- og sikkerhetssystemer hvor skipets viktige hovedfunksjoner (f.eks. framdrift, styring, kraftproduksjon, dynamisk posisjonering, kran, ROV systemer, og ballastering) var kontrollert og overvåket av enkle, ikke-programmerbare systemer. Slike skip var i liten grad utsatt for fellesfeil som kunne påvirke flere hovedfunksjoner samtidig. Gjeldende internasjonale regelverk er basert på at skipets mannskap skal ha kapasitet, kunnskap og mulighet til å styre skipets hovedfunksjoner med enkle lokale og manuelle metoder dersom en feil skulle oppstå.

Som et resultat av den teknologiske utviklingen er imidlertid dagens skip høyteknologiske installasjoner som er avhengige av programmerbare og nettverksbaserte systemer. I tillegg blir skipets viktige automasjon-, kontroll- og sikkerhetssystemer i økende grad integrert med nettverksløsninger. Dette innebærer økt risiko for at digitale feil, skadeprogrammer og angrep vil kunne slå ut enkelte eller flere av skipets viktige funksjoner samtidig. Selv om skipet fremdeles skal kunne styres og kontrolleres lokalt/manuelt vil dette i mange tilfeller være en krevende oppgave grunnet manglende kunnskap, manglende øvelse, begrenset mannskap, kompliserte brukergrensesnitt, osv.

Tidligere var industrielle automasjon-, kontroll- og sikkerhetssystemer proprietære, mens systemene i dag i stor grad er basert på kommersielt tilgjengelige komponenter som f.eks. PC med Microsoft Windows operativsystem. Det betyr at kjente sårbarheter for slike kommersielle standardprodukter også vil være eksponert i sektoren. For å sikre seg mot slike sårbarheter, må systemene løpende oppdateres med rettelser fra produsentene. Dette er utfordrende i maritim sektor fordi datakommunikasjon til skipene kan ha begrenset kapasitet og fordi oppdateringer som kan påvirke systemer som er i drift må planlegges nøye og kanskje gjøres når skipet ikke er i normal operasjon. Mange skip benytter digitale systemer som ikke har oppdaterte sikkerhetsrettelser.

3.4 Overvåkningssystemer

Det benyttes i stor grad overvåkningssystemer (CCTV) både ombord i skip, i trange passasjer og i havn. Slike systemer samler mye informasjon som kan ha betydning både i forhold til personvern, men også i forhold til ondsinnede handlinger. Systemene kan settes ut av drift og de kan benyttes til å innhente informasjon. Slike systemer er benyttet for å stjele brukeridentiteter og passord. Det er varierende praksis for sikring av data og sletting.

3.5 Kommunikasjon

Logistikk kjeden ved transport av varer og personer involverer et stort antall aktører, og det er utstrakt bruk av usikret e-post. Bl.a. utveksles passasjerlister, og ved en ulykke vil informasjon om skadede personer utveksles. Skadeinformasjon er sensitiv personinformasjon, og usikret e-post er ikke et medium som er egnet til dette.

Åpen kommunikasjon gjennom VHF har en sikkerhetsfunksjon ved at det gjør det mulig å initiere kommunikasjon uten nærmere kunnskap om identiteten til den man vil kommunisere med og ved at alle fartøy som er involvert i en trafikksituasjon får tilgang til lik informasjon ved å overhøre kommunikasjon mellom andre skip, eller mellom andre skip og VTS. Dette har utfordringer i forhold til personvern, men også ved utveksling av sikkerhetsinformasjon i havner etc. I dag kommuniseres sensitiv informasjon mellom skip og aktører på land i stor grad ved hjelp av mobiltelefoni når fartøy er nær land eller ved hjelp av satellittbasert telefoni til havs. Med utviklingen av små, håndholdte VHS enheter, har det oppstått en ny sårbarhet: Disse enhetene kan bli «liggende på sendeknappen» og dermed jamme oppkallings- og nødkanalen.

Kommandoforhold om bord kan medføre sårbarheter. Dersom en kaptein beordrer sammenkobling av systemer eller nett, er det vanskelig for en elektriker/serviseteknikker å sette seg imot dette ut ifra sikkehetsbetraktninger.

3.6 Underholdning og velferdstilbud

Underholdning og velferdstilbud om bord har blitt digitalisert og passasjerer og ansatte forventer internett-tilgang. Slike nett må separeres fra de kritiske nettene om bord. Det har i den siste tiden vært stor fokus på slike sårbarheter i fly (Se faktaboks 16), men sårbarhetene kan være like relevante på skip. Noen skip har fysisk adskilte nett og noen har virtuelt adskilte nett. Det er variabel kvalitet på separasjonsmekanismer, og ofte bare enkle brannveggfunksjoner.

I en rapport skrevet for amerikanske luftfartsmyndigheter (Federal Aviation Administration, FAA) publisert i april 2015 påpekes det at fly med trådløst passasjernettverk kan være sårbart for inntrengning. Flere moderne flytyper slik som Boeing 787 Dreamliner, Airbus A350 og A380 er designet med trådløse passasjernettverk som ikke er fysisk separert fra nettverket som flyets kontrollsystem bruker. Dette gjør det mulig for en angriper å få tilgang til og kompromittere flyets kontrollsystem. Angrepet kan komme fra passasjerer ombord, men også fra bakken via internett. Denne sårbarheten foreligger så lenge separasjonen av nettene er basert på brannmurer eller andre programvare-komponenter som kan angripes. Et mer sikkert design, som finnes i andre typer fly og kontrollsystemer er å bruke fysisk separate nett.

Faktaboks 16: Nyhet om trådløse nett på fly. /18//19/

3.7 Vedlikehold

Næringen har i liten grad IT-teknisk personell ombord, og ofte gjøres IT-teknisk arbeid av ikke-IT-faglige personer. Skipene er derfor i stor grad avhengige av fjernarbeid utført av leverandører og landbaserte IT-teknikere. De digitale systemene om bord muliggjør fjernvedlikehold, diagnostikk og oppdateringer over nett. Det betyr ofte at systemene åpnes for tilgang fra internett noe som også åpner for en rekke digitale sårbarheter. Det er varierende fokus på sikring mot dette. Noen rederier har innført nøkkelbrytere for å kontrollere slik tilgang, men sektoren har i liten grad innført dedikerte systemer for kontroll. Det ble i arbeidsmøte (ref. kap. 2.4) omtalt et tilfelle der personell som gjør vedlikehold via en nettforbindelse har resatt digitale systemer på feil skip.

Når skip ankommer havner, kommer det ofte servicepersonell og inspeksjonspersonnell om bord. Det er varierende kontroll med identitet og kompetanse på slikt personell. Disse har ofte med seg minnepinner o.l., som utgjør en sårbarhet ved at de kan installere feil programvare, spre ondsinnet kode, eller utføre feilkonfigurasjon av systemer.

3.8 Fysisk sikring

Det er varierende fysisk sikring av serverrom, kommunikasjonsrom og kablingsskap på skip. Det er også varierende grad av merking av kabling. Spesielt på eldre skip kan datakabling for kritiske nett være tilgjengelig for mannskap og passasjerer. Dersom uautoriserte datamaskiner kobles til slike segmenter innføres en rekke sårbarheter.

3.9 Havner

Transport av varer på skip og import/eksport av disse varene via landets havner utgjør en kritisk funksjon i samfunnet. Cirka 90 % (målt i vekt) av varer som importeres/eksporteres til EU transporteres med skip. Utviklingen mot leveranser rett før produksjon («just in time») gjør at vitale samfunnsfunksjoner vil stoppe opp dersom sjøtransport eller havnefunksjoner stopper. Analyser i europeisk bilindustri viser at 48 timer etter en eventuell varestopp i havnene, vil produksjon bli berørt. En rekke næringer og enkeltpersoner vil bli berørt.

Mens havnene har hatt økt produktivitet på grunn av IKT i leverandørkjeden, har også omkringliggende funksjoner som handelspartnere, befraktere og tollbehandling med mer hatt en vesentlig innsparing og prosessforbedring. Omløpstiden på skip har blitt vesentlig forbedret. Avhengighet til IKT gjør at stopp i IKT løsninger grunnet uvillede eller villede handlinger vil kunne få dramatiske konsekvenser.

I august 2011 ble det iranske rederiet IRISL (the Islamic Republic of Iran Shipping Lines) utsatt for flere cyberangrep. Angrepene ødela lastinformasjon: om rater, last, cargo nummer, datoer og steder og rederiet hadde ikke lenger informasjon om hvor containere befant seg, om de var blitt lastet eller ikke og om de var ombord på et skip eller på land. Rederiets interne kommunikasjonsnettverk ble også slått ut. Selv om man klarte å gjenskape informasjonen medførte angrepet betydelig forstyrrelse av rederiets operasjon, feilsending og tap av last og betydelige økonomiske tap.

Faktaboks 17: Cyberangrep mot iransk rederi /10/

I mai 2013 avslørte Europol at hackere helt siden sommeren 2011 hadde hatt tilgang til Antwerpen havns logistikksystem for å understøtte narkotikasmugling. Angriperne brukte utstyr for fjerntilgang som var kamuflert som annet utstyr, slik som mini PCer gjemt inni elektriske koblinger, disker, USB keyloggere og trådløse kort. Utstyret ble brukt til å stjele bruker-akkreditiver men også til å overvåke og få tilgang til logistikksystemet i sanntid.

Med denne tilgangen var smuglerne i stand til å gjemme narkotika i containere med annet gods og deretter ved å stjele tilgangskoder få tilgang til å hente disse før de virkelige eierne dukket opp. Ved et tilfelle kapret også smuglerne en forsendelse etter at den hadde forlatt havnen. Også forsendelser til Rotterdam har vært omfattet av saken.Ved opprullingen ble det gjort beslag på flere hundre kilo kokain og heroin. Omfanget av smuglingen er ikke kjent, men gateverdien av stoffene kan være flere hundre millioner kroner.

Sjef for Europol, Rob Wainwright, uttalte til BBC at dette illustrerer hvordan organisert kriminalitet stadig blir mer sofistikert i cyber-domenet: «We have effectively a service-orientated industry where organised crime groups are paying for specialist hacking skills that they can acquire online.» Det ser ut til at narkotikasmuglerne har leid inn en separat gruppe med hackere for å utføre angrepet.

Faktaboks 18: Hacker-angrep på Antwerpen havn for smugling. /10/

3.10 Sentrale systemer

Kystverket utvikler og drifter SafeSeaNet Norway som en felles nasjonal meldeportal for skipsfarten. Dette systemet er basert på det europeiske Single Window konseptet som anbefaler utviklingen av en nasjonal portal hvor fartøy, rederier og operatører kan sende inn rapporteringspliktig informasjon til nasjonale myndigheter kun én gang. Informasjonen skal videreformidles automatisk til nasjonale myndigheter for å forenkle og øke kvaliteten på offentlig saksbehandling overfor maritime brukere. Informasjon om farlig eller forurensende last blir videreformidlet til det sentrale europeiske SafeSeaNet systemet.

SafeSeaNet har en stor og variert brukermasse, og det er utfordrende å sikre god brukerautentisering. En utenforstående kan lage seg en falsk konto og både hente ut og registrere feilaktig informasjon. Bl.a. ligger sikkerhetsinformasjon om skip i systemet.

SafeSeaNet spiller en viktig rolle ved losformidling, meldinger om farlig gods, trafikkontroll, tollkontroll, og grensekontroll. Bortfall av systemet eller feilaktig informasjon kan føre til at viktig informasjon ikke er tilgjengelig når kritiske situasjoner oppstår.

4 SÆRSKILTE TEMAER

4.1 Roller og ansvar knyttet til ivaretagelse av IKT-sikkerhet

I Norge er ansvaret for implementering av det internasjonale regelverket for maritim sikring delt mellom Samferdeselsdepartementet(SD) og Nærings- og handelsdepartementet (NHD). Myndighet og ansvar for implementering av regelverket er delegert til henholdsvis Kystverket for havner og havneanlegg, og til Sjøfartsdirektoratet for skip og personell om bord. Disse tilsynsmyndighetene fører ikke tilsyn med sikring mot digitale sårbarheter.

Nasjonale etater som har et sterkt fokus på digitale sårbarheter som f.eks. NSM, PST og E-tjenesten har i varierende grad etablert samarbeid med maritim sektor.

Rederiene ønsker ikke et detaljert regelverk og tilsynsregime for digitale sårbarheter, men vil ha risikobasert tilnærming. En slik tilnærming vil fungere godt for det store flertallet av seriøse aktører, men det er tvilsomt om useriøse aktører vil igangsette tilstrekkelig med tiltak. For å sikre seg mot slike useriøse aktører kreves et strengere tilsynsregime og et mer konkret regelverk.

Det er vanskelig å ha oversikt over hvilket regelverk innen informasjonssikkerhet, personvern mm. som gjelder for norske skip i utenlandske farvann, utenlandske skip i norske farvann, utenlandske eiere i norske registre etc. Regelverk etter ISPS-koden gjelder uavhengig av flagg, farvann, eier m.m.

4.1.1 Regelverk

Det internasjonale regelverket for maritim sikring er gjort gjeldende i norsk rett gjennom følgende forskrifter:

- Forskrift 29. mai 2013 nr. 538 om sikring av havneanlegg
- Forskrift 29. mai 2013 nr. 539 om sikring av havner
- Forskrift 22. juni 2004 nr. 972 om sikkerhet, pirat- og terrorberedskapstiltak og bruk av maktmidler om bord på skip og flyttbare boreinnretninger (Sikkerhetsforskriften fra Sjøfartsdirektoratet)

De nevnte forskriftene gjennomfører EU-forordning 725/2004, om forbedret sikkerhet for fartøyer og havneanlegg. Forordningen gjelder fullt ut som norsk forskrift, og brukerne må derfor forholde seg til kravene i denne direkte. SOLAS-konvensjonen kapittel XI-2 og ISPS-koden (International Ship and Port Facility Security Code) er vedlegg til forordning 725/2004. Forordningen gjør ISPS-koden del A obligatorisk i alle EUs medlemsland, i tillegg til at enkelte av bestemmelsene i del B også gjøres obligatoriske.

ISPS er en utvidelse av SOLAS-konvensjonen om sikkerhet for personell og skip på sjøen. Den trådde i kraft i 2004 og angir hvilke ansvarsområder forskjellige parter har for å detektere og hindre sikkerhetstrusler mot skip og havner i bruk til internasjonal handel. Hensikten med ISPS koden er:

- Å detektere sikkerhets trusler/risikoer og implementere nødvendige sikkerhets tiltak
- Å etablere roller og ansvar relatert til maritim sikkerhet for myndigheter, lokale administrasjoner og for skip og havner på nasjonalt og internasjonal nivå
- Å innhente og distribuere sikkerhets-relatert informasjon
- Å promotere en metode for sikkerhets gjennomganger for å etablere planer og prosedyrer tilpasset endrede sikkerhets-nivåer.
- Å sikre at nødvendige og passende maritime sikkerhetstiltak er på plass.

Faktaboks 19: ISPS

Forskriftene nr. 538 og 539 etablerer et begrep om sikringsnivå for havner hhv. havneanlegg. Tilsvarende etablerer forskrift nr. 972 et tilsvarende begrep om beredskapsnivå for skip. Denne graderingen gjør det mulig å tilpasse sikringstiltak til den gjeldende trusselsituasjonen. Myndighetene kan beslutte å iverksette et forhøyet beredskapsnivå. Kystverket fastsetter det maritime sikringsnivå som havner og havneanlegg skal operere på. Skip som befinner seg i disse eller i norsk farvann må forholde seg til dette sikringsnivå uavhengig av flagg. Sjøfartsdirektoratet fastsetter sikringsnivået for skip under norsk flagg, gjerne knyttet til spesielle farvann. Ingen av forskriftene nevner digitale sårbarheter eller IKT sikkerhet spesielt.

§ 5. Maritimt sikringsnivå
(1) Med maritimt sikringsnivå menes en angivelse av graden av risiko for at en sikringshendelse vil bli forsøkt utført eller vil inntreffe. Kystverket fastsetter det maritime sikringsnivå som havner skal operere på.

(2) Følgende maritime sikringsnivåer gjelder for havner:
a) Sikringsnivå 1: Det nivået hvor et minimum av relevante sikringstiltak skal opprettholdes til enhver tid.

b) Sikringsnivå 2: Det nivået hvor relevante tilleggstiltak for sikring skal opprettholdes for en viss tidsperiode på grunn av en midlertidig økt risiko for hendelser som kan true sikkerheten.

c) Sikringsnivå 3: Det nivået hvor ytterligere spesifikke sikringstiltak skal opprettholdes for en begrenset tidsperiode når en hendelse som kan true sikkerheten er umiddelbart forestående eller sannsynlig.

(3) Havnens sikringsleder skal umiddelbart etter å ha mottatt melding om endring i det maritime sikringsnivå, iverksette tiltakene i havnens sikringsplan for det gjeldende sikringsnivået.

Faktaboks 20: §5 Maritimt sikringsnivå for havner. /27/

4.1.2 Krav om sårbarhetsvurdering

Sikkerhetsforskriften fra Sjøfartsdirektoratet krever at det skal utarbeides en sårbarhetsvurdering (Ship security assessment, SSA) som beskrevet i ISPS-kodens del A, seksjon 8, og en sikkerhets- og terrorberedskapsplan (Ship security plan, SSP) som beskrevet i ISPS koden del A seksjon 9. Når det er verifisert at fartøyet oppfyller kravene i forskriften og i den godkjente sikkerhets- og terrorberedskapsplan, utsteder Sjøfartsdirektoratet eller klasseinstitusjon (RSO) et internasjonalt sikkerhets- og terrorberedskapssertifikat (ISSC). Dette har gyldighet på fem år med forutsetning av en mellomliggende verifikasjon mellom år 2 og 3.

Et minstekrav til sikkerhetsvurderingen i henhold til ISPS-kodens del A, seksjon 8 er at den skal identifisere: eksisterende tiltak, operasjoner det er særlig viktig å beskytte, mulige trusler og deres sannsynligheter, samt sårbarheter. ISPS koden nevner ikke digitale sårbarheter spesielt, men kravene til en sikkerhetsvurdering er formulert generelt slik at digitale sårbarheter også omfattes av forskriften.

Dette kravet om sårbarhetsvurdering og sikringsplan gjelder også for havner og havneanlegg.

Det er ikke kjent at Norsk Standard NS 5832:2014 «Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse» er i bruk i sektoren /17/.

4.2 Overordnet beskrivelse av IKT-infrastruktur

Det er et stort antall aktører i sektoren, med ulik IKT-infrastruktur. Det er i liten grad harmonisert IKT-infrastruktur. Noen rederier har tilstrebet like IKT-løsninger på sine skip for å forenkle bruk og vedlikehold.

4.3 Avhengigheten av øvrige innsatsfaktorer/infrastrukturer

Sjøtransporten er avhengig av en rekke system basert på digital teknologi:

- Globale posisjoneringssystem (GNSS)
- Elektroniske kart og informasjonssystem (ECDIS)
- Automatisk identifisering av skip (AIS/LRIT)
- Nettverksbaserte kontrollsystem om bord for bl.a. styring og propulsjon
- Radiokommunikasjon (satellitt, MF/HF, VHF, UHF, mobiltelefon, kabel(i havn))
- Datakommunikasjon (Primært via satellitt)
- Administrative system (Rapportering til myndigheter, rederi, lasteier, med flere)
- Landbaserte system for administrasjon av havneanløp, last, passasjerer mm.

Digitale sårbarheter for disse systemene er beskrevet i kapittel 3. Ved større avbrudd i disse tjenestene, vil varetransport kunne stoppe opp og medføre vesentlige kostnader for samfunnet, næringsliv og enkeltpersoner. Ref faktaboks 5.

4.4 Samarbeid mellom næring, interesseorganisasjoner og myndigheter

Det finnes en rekke interesseorganisasjoner som bl.a. er involvert i samarbeidet mellom næring og myndigheter. På arbeidsmøte (Ref. kap. 2.4), var Norges rederiforbund og Norsk Havneforening representert.

Norges Rederiforbund er en interesse- og arbeidsgiverorganisasjon for norsktilknyttede bedrifter innen skipsfart og offshore entreprenørvirksomhet. Rederiforbundets medlemmer sysselsetter over 55 000 sjøfolk og offshorearbeidere fra mer enn 50 forskjellige nasjoner. Rederiforbundet har en sentral rolle i samarbeidet mellom rederi og myndigheter.

Norsk Havneforening er en medlems- og interesseorganisasjon med 47 medlemshavner rundt hele norskekysten. Foreningen jobber med havnenes rammevilkår ved å jobbe med myndigheter og næringsaktører, samt ved å samarbeide med andre organisasjoner og aktører.

4.5 Beredskap/operativ håndtering av relevante tilsiktede og utilsiktede hendelser

Maritim sektor er en foregangssektor i forhold til beredskapsplaner og øving av beredskap. Offshore skip ligger kanskje lengst fremme på dette området innenfor skipsfarten. Dette arbeidet fokuserer på utilsiktede hendelser om bord som grunnstøting, havari og brann. Bl.a. setter SOLAS krav til at livbåter skal være på vannet hver 3. måned.

Disse planene har i liten grad innarbeidet digitale sårbarheter, og det er ikke identifisert øvelser som involverer slike hendelser. Det er etablert globale rutiner for varsling av hendelser eller systembortfall som kan gi fare for navigasjonssikkerhet (NAVTEX og NAVAREA meldinger).

Det øves på å styre skip «manuelt» ved bortfall av industrielle automasjon og kontrollsystemer, men systemene blir mer og mer avhengig av slike system. Det er tvilsomt om en flytende oljeplattform lar seg styre uten et funksjonelt DP system.

Det øves på utfall av elektroniske navigasjonssystemer.

Enkelte rederier opplyser om at de har beredskapsplaner for noen kritiske systemer (bl.a. bookingsystemer).

Kan skipsfart (skipene) karakteriseres som "Høypålitelige Organisasjoner"?	
- sterk media oppmerksomhet	Ja – for noen segmenter
- omfattende systemforståelse	Nei –utstrakt bruk av lavkostansatte
- god kommunikasjon	Nei – mange nasjonaliteter og kulturer
- delte visjoner, normer, verdier, osv.	Nei – utstrakt bruk av bemanningsbyråer
- Sikkerhetsengasjement fra toppen	Sjelden
- Maksimal proaktiv læring	Nei – flere ulykker enn nesten-ulykker
- Langtidsperspektiv	Sjelden
- Paranoia for feil – «alltid på vakt»	Nei – en selvtilfreds-/ gemyttlig kultur
- fleksibel/flat organisasjon	Nei - hierarkisk
- organisasjonsmessig redundans	Nei – minimum bemanning

Faktaboks 21: Ulykker skjer ikke – de forårsakes /28/

4.6 Beskrivelse av internasjonale problemstillinger

Etter 11. september 2001 angrepet på «Twin Tower» har det vært en økende fokus på mulige angrep som involverer skip med farlig last eller angrep på passasjerskip.

Den amerikanske kystvakten har en pågående vurdering av om de skal sette «cybersecurity» krav til skip som skal anløpe amerikanske havner.

EU gjorde en analyse av «cybersecurity aspects in the maritime sector i 2011 /30/. Noen hovedfunn i denne rapporten var at maritim bevissthet om informasjonssikkerhet (cyber security awareness) er lav til ikke eksisterende og at eksisterende maritimt regelverk og policy kun fokuserer på fysisk sikkerhet og ikke tar informasjonsaspektet i betraktning. Dette kan overføres på norske forhold. Videre anbefales det at IMO og EU skal sørge for en harmonisering av regelverket. Og at man bør forsøke å bygge plattformer for bedre informasjonsutveksling mellom medlemsstatene for dette domenet.

IMOs sjøsikkerhetskomité (Maritime Safety Committee) har satt i gang et arbeid for å se på behovet for retningslinjer for maritim cybersecurity under det stående agendapunktet «Measures to enahance maritime security» etter initiativ fra Canada og USA. Maritim industri ved Intertanko, Intercargo, BIMCO og ICS arbeider med en egen industriveiledning for risikobasert håndtering av informasjonssikkerhet. Arbeidet med veilederen er gjort kjent for IMO og MSC holdes informert og vil bli presentert endelig dokument. Et lignende arbeid er satt i gang av IMOs *Facilitation Committee (Lettelser i internasjonal sjøtransport).*

Det ble fremmet bekymring på Arbeidsmøte (ref. kap. 2.5) om at IMO er en stor og tung organisasjon der utarbeidelse av nye retningslinjer tar lang tid. Det var også bekymringer om at IMO's intensjon er å lage frivillige retningslinjer, mens man i EU favoriserer obligatoriske retningslinjer.

4.7 Fremtidige problemstillinger/trender

IMO har vedtatt en strategiplan (MSC94) for implementering av e-Navigasjon. Planen påpeker behovet for en autorisert kommunikasjonsinfrastruktur om bord i skip, -mellom skip, mellom skip og land og mellom myndigheter og andre maritime interessenter. Denne «Maritime Skyen» er definert som: «en kommunikasjonsinfrastruktur for effektiv, pålitelig og sømløs digital informasjonsutveksling mellom alle autoriserte maritime interessenter på tvers av alle tilgjengelige kommunikasjonssystemer».

Virtuelle seilingsleder; -erstatter bøyer og andre fysiske navigasjonsinnretninger med motsvarende virtuelle objekter som fremvises om bord på beslutningsstøttesystemer som ECDIS og RADAR. IALA/IEC har allerede utarbeidet standarder for presentasjon av virtuelle navigasjonsinnretninger (ikoner) på navigasjonsutstyr. Kystverket som har ansvar for merking av ledene i dag, legger ikke opp til en slik utvikling i Norge.

Ubemannede skip;- autonome og ubemannede skip anses som et element for en bærekraftig og konkurransedyktig (skips)industri i fremtiden. Jfr. EU-prosjektet «MUNIN» som undersøker både konseptet og teknologien som kreves for å operere et «industrielt autonomt skip» både kosteffektivt og sikkert i et reelt og kommersielt miljø.

4.8 Forsikring

Reassuransemarkedet innførte etter 11. september 2001 et unntak for bruk av datateknologi i skadelig hensikt, den såkalte Cyber Attack klausulen (CL 380). I det internasjonale forsikringsmarked for maritime enheter (skip, rigger etc.) gjelder CL 380 tilnærmelsesvis uten unntak.

Under krigsdekningen hos Den Norske Krigsforsikring for Skip gis det dekning av tap og skade som oppstår på basis av bruk av datateknologi i skadehensikt. Altså det CL 380 i hovedsak søker å ekskludere. Slik sett er norske skip og rigger bedre beskyttet enn resten av verdensflåten. Det er imidlertid også en risiko for at norske skip og rigger kan bli utsatt for skadeverk gjennom hacking eller lignende som ikke omfattes av krigsforsikringen fordi angrepet ikke kan betegnes som sabotasje eller politiske motivert skadeverk. Skal skadeverket henføres til sivildekningen vil det være et hull i dekningen. Med den praksis at denne risiko ekskluderes under sivil kasko, vil det være en ikke ubetydelig udekket risiko for rederne/sikrede, etter som slike risikoer bare i spesielle tilfelle vil være å regne som krigsfare etter Cl. 2-9.

5 RISIKOREDUSERENDE TILTAK

I dette kapittelet gis noen generiske tiltak for sektoren og deretter en overordnet beskrivelse av mottiltak i forhold til de topp 10 digitale sårbarheter som er beskrevet i kapittel 1.1. Det vises deretter eksempler på tekniske barrierer som er relevante for sårbarhetene.

5.1 Generiske tiltak

Det er behov for en felles rapporteringskanal både fra myndighetene til sektoren og fra sektoren til myndighetene i forhold til digitale sårbarheter. Når f.eks. NORCERT detekterer økning av internettbaserte angrep mot sektoren, må alle relevante aktører varsles. Et alternativ er at sektoren etablerer en egen CERT tjeneste, men det ar uklart hvem som evt. skal etablere og finansiere denne. Kystverket og norske etater har andre eksisterende varslingsmekanismer i dag både mot havner og skip. Disse kan vurderes benyttet også innen digitale sårbarheter.

5.2 Manglende oppmerksomhet og opplæring

Mottiltak mot denne sårbarheten er først og fremst å innarbeide en sikkerhetskultur med fokus på digitale sårbarheter i hele virksomheten som er forankret i ledelsen. Det bør gjennomføres oppmerksomhetstrening og mannskapet må bevisstgjøres om vanlige risikoer for informasjonssikkerhet slik som for eksempel tilkobling av uautorisert utstyr (minnepinner, smarttelefon, PC el.l.) til kritiske nettverk. Skipets mannskap bør ha forståelse for avhengigheter i skipets integrerte systemer som f.eks. navigasjon-, kommunikasjon- og automasjonssystemer.

Noen rederier har innført «like IT-systemer» på alle skip for å forenkle bruk og vedlikehold.

5.3 Navigasjonssignaler fra satellitt

5.3.1 Jamming

Det er velkjent i det maritime miljøet at det sivile GPS signalet enkelt kan blokkeres av en laveffekt jammer. Det er estimert at 1 watt jammer plassert i en drone kan blokkere GPS-signalene til en mottaker som allerede er låst til signalet innenfor en radius på 10 km og hindre låsing av ny satellitter (signaler) innenfor en avstand av 85 km.

For å motstå de billigste «GNSS-jammerene» finnes det imidlertid rimelig filtre basert på polarisering av satellittsignalene.

For å motstå de mer avanserte jammerene kreves teknikker som gjerne fordrer fler-element-antenner. Slike antenner er kostbare og anvendes primært for militære applikasjoner.

Signalprosesseringsteknikker, inkludert redusert båndbredde og økt prosesseringstid har blitt utarbeidet som prinsipielle antijammingstiltak men disse er mottakerspesifikke og krever revisjon av design.

USAs forsvarsdepartement har implementert tiltak i GPS som (kan) iverksettes i forbindelse med konflikter. Satellitt-signalene forstyrres da slik at sivile brukere ikke kan benytte GPS i konfliktområdet (benevnt NAVWAR). Tiltakene prøver å begrense forstyrrelsen utenfor konfliktområdet. NATO benytter en egen kryptert kode (P(Y)) og mottar derfor GPS-signaler også innenfor konfliktområdet.

Andre GNSS-nasjoner ser ut til å utvikle tilsvarende egenskaper for sine systemer.

GNSS alene er således sårbar for bevisst jamming og redundante (back-up) løsninger bør vurderes. Alternativer som treghetsnavigasjon, oppgradering av LORAN-C, og et maritimt distansemålingssystem for havneanløp og trange og trafikkerte farvann bør utredes.

Det finnes også alternative systemer som det russiske GLONASS systemet og det kinesiske BEIDOU, med myndighetene i disse landene kan også innføre begrensinger. Det pågår også utbygging av et europeisk system GALILEO.

5.3.2 Spoofing

Konvensjonelle sivile GNSS-mottakere er sårbare ved spoofing-angrep. Selv om en rekke teknikker for identifisering og avvisning av en spoofer er fremsatt er slike ikke implementert i sivile GNSS-mottakere.

NATO har sin krypterte P(Y)-kode og de militære mottakerene har også implementert flere mottiltak mot spoofing.

Implementering av en kryptografisk anti-spoofing teknikk også for sivile GNSS-signaler (=C/A for GPS) vil øke beskyttelsen av sivile GNSS-mottakere betraktelig. /33//34/

5.4 System for identifikasjon av fartøy

Den fundamentale egenskapen til AIS er en veldig nøyaktig tidssynkronisering som muliggjør en selvorganiserende datalink (TDMA) mellom alle AIS-mottakere. Tidssynkroniseringen til AIS baserer seg på GPS (sine atomklokker). Bortfall av GPS tid (UTC) vil således også stenge ned AIS.

For nærværende er det kun VHF og radar som er alternativer for identifikasjon av fartøyer i anti-kollisjonsøyemed med LRIT som «strategisk» ID-kilde for myndigheter.

Et alternativt(redundant) identifikasjonssystem blir tilgjengelig hvis(når) infrastrukturen benevnt «Maritime Cloud» blir implementert (se kap. 4.7). /35/

5.5 Fjerntilkobling

Mange leverandører av programmerbare systemer tilbyr i dag tjenester som brukerstøtte, diagnostikk, vedlikehold eller oppgradering via fjerntilkobling. Klare prosedyrer som ansvarliggjør leverandører og skipets mannskap, bør etableres. Sikringstiltak som sterk autentisering av bruker, sikre tuneller (VPN), tilgangsstyring, kryptering, validering av overført data, oppdaterte anti-virusprogrammer, direktekommunikasjon mellom leverandør og ansvarlig om bord bør benyttes.

Noen skip har fysisk bryter med nøkkel for å åpne for fjernarbeid.

5.6 Stort antall aktører utveksler mye informasjon på e-post om skip, last og passasjerer.

Systemer for sikring av e-post har vært tilgjengelig over lang tid, men er i liten grad tatt i bruk fordi systemene krever elektronisk id, og anskaffelse og bruk av slik id oppfattes som meget tungvint. Løsningene har også primært vært tilrettelagt for person-til person kommunikasjon. Det arbeides med løsninger for selskap-selskap kommunikasjon («Digipost for selskaper»).

Alternativet til bruk av e-post er å benytte program til program kommunikasjon. Da må kommunikasjonsmoduler innarbeides i applikasjonene. Det mest vanlige er å benytte «WEB-services», og denne kommunikasjonen kan sikres med «WEB-service security».

Et annet alternativ er å bruke sikret replisering av data fra båt til land i stedet for e-post.

5.7 Separasjon av datanett om bord og i havner

Det må minimum være separasjon mellom datanett for sikkerhetssystemer, kritisk infrastruktur, administrative systemer og underholdning/internett. Risikovurdering må avgjøre hvilke

separasjonsmekanismer som skal benyttes. En brannvegg kan være mangelfullt konfigurert og ha sårbarheter, og det kreves flere barrierer. NSM har laget en relevant veiledning «Hvordan forebygge, oppdage og håndtere dataangrep» /36/.

5.8 Bruk av mobile lagringsenheter

Oppmerksomhetstrening og opplæring er viktig for at brukere skal forstå risiko ved bruk av mobile lagringsenheter. Likeledes må det være etablert rutiner og veiledninger. Fysisk blokkering eller deaktivering av USB porter, blåtann og trådløse nett kan være nødvendig (herding).

5.9 Bookingsystemer og administrasjonssystemer er sårbare

WEB baserte bookingsystemer og administrasjonssystemer har en rekke digitale sårbarheter, og må sikres på samme måte som internett-butikker og nettbank. Det blir for omfattende å skissere disse sikringstiltakene her.

5.10 Fysisk sikring av datarom, koplingsskap, m.m. på skip

Maritime skip og innretninger er, med noen unntak, pålagt å følge IMO ISPS koden (The International Ship and Port Facility Security Code (ISPS Code)). ISPS koden stiller krav til fysisk sikring av kritiske områder for å begrense muligheter for sabotasje, kapring og terrorisme. Hvilke områder som skal være gjenstand for adgangskontroll er delvis definert i koden og videre spesifisert i sikkerhetsplaner utarbeidet for hvert skip. Dette vil også inkludere adgang til maskinrom, tavlerom osv. og bør omfatte andre kritiske fordelere.

5.11 Begrenset autentisering av brukere mot systemer for offentlig innrapportering.

Adgangskontroll er en vital del av et regime for informasjonssikkerhet. Et IT system kan få kjennskap til brukerens identitet basert på noe brukeren vet (f.eks et passord), noe brukeren har (f.eks et smartkort) eller noe brukeren er (biometri). To-faktor autentisering er når det kombineres to av disse faktorene. To-faktor autentisering lar seg enklest implementere for brukere innen en mindre organisasjon der man eksempelvis kan utlevere smartkort. For offentlige systemer som skal nås av publikum, bør det benyttes fellestjenester som f.eks. ID-porten. ID-porten støtter innlogging for personer som har et norsk fødselsnummer eller d-nummer. Det arbeides med løsninger for innlogging for utenlandske borgere, men dette er ikke tilgjengelig i dag. Dette er en spesiell utfordring for maritim sektor ettersom mange brukere ikke har en norsk nasjonal identitet. Det er viktig å finne en god avstemming mellom sikringstiltak og brukervennlige systemer.

5.12 Barrierer

De påfølgende faktabokser viser eksempler på barrierer som er relevante i forhold til topp 10 digitale sårbarheter som beskrevet i kapittel 1.1.

Barriere for å hindre en hendelse	Oppmerksomhet	Navigasjon (GPS)	Identifikasjon (AIS)	Fjernarbeid	Usikret e-post	Separasjon av nett	Mobil lagring	Bookingsystemer	Fysisk sikring	Brukerautentisering
Antenner/filter		**X**	**X**							
Anti-spionprogramvare	X			X	X	X	X	X		
Antivirus programvare	X			X	X	X	X	X		
Autentisering	X	**X**	**X**	**X**	X	X	X	X		**X**
Blokkere kjøring av ikke autoriserte programmer	X			X	X	X	X	X		
Blokkere/deaktivere USB porter	X			X	X	X	**X**	X	X	
Brannvegg	X			X	X	X	X	X		
Gjestenett	X			X	X	X	X	X		
Herding av programvare	X			X	X	X	X	X		
Klassifisering av utstyr, dokumenter mm.	X			X	X	X	X	X	X	X
Kontroll av enheter som kobles til nett (NAC/NAP)	X			X	X	X	X	X		X
Kryptering med integritetskontroll	X	**X**	**X**	X	**X**		X	X		X
Krypterte disker på mobilt utstyr	X			X	X	X	X	X		
Krypterte minnepinner	X			X	X	X	**X**	X		
Ledelsesforankring / Etablering av sikkerhetskultur.	**X**			X	X	X	X	X	X	X
Merke kritikalitet på rom, utstyr, kabler mm	X			X	X	X	X	X	**X**	
Minste privilegiers prinsipp / Oppdeling av oppgaver	X			X	X	X	X	X	X	X
Oppdatering av programvare	X			X	X	X	X	X		
Oppdeling av datanett	X				**X**	**X**	X	X		
Oppmerksomhetstrening	**X**			X	X	X	X	X	X	X
Penetrasjonstest	X			X	**X**	X	X	**X**		X
Revisjon fysisk sikring	X					X	X	X	**X**	
Rutiner for behandling av klassifisert utstyr, dokumenter mm.	X			X		X	X	X	X	X
Rutiner for å håndtere minnepinner	X			X		X	**X**	X		
Sikkerhet i utviklingsmiljø						X	X	**X**		
Sikre tuneller (VPN) for fjernarbeid	X			**X**		X	X	X		
Sikring av operatørgrensesnitt						X	X	X		
Tilgangsstyring basert på tidsbegrensede arbeidsordre	X			X		X	X	X	X	
Tydeliggjøre ansvar i ansettelseskontrakt / kontrakt med underleverandører, konsulenter mm.	X			**X**	X	X	X	X	X	
Vaske e-post	X			X			X	X		
Vaske webtrafikk	X			X			X	X		

Faktaboks 22: Barrierer for å hindre at en uønsket hendelse skjer

Barriere for å hindre en hendelse	Oppmerksomhet	Navigasjon (GPS)	Identifikasjon (AIS)	Fjernarbeid	Usikret e-post	Separasjon av nett	Mobil lagring	Bookingsystemer	Fysisk sikring	Brukerautentisering
Alternative system / Manuelle prosedyrer		**X**	**X**	X				X		
Anti-spionprogramvare (Legger ondsinnet programvare i karantene og sender alarm)	X			X	X	X	X	X		X
Antivirus programvare (Legger ondsinnet programvare i karantene og sender alarm)	X			X	X	X	X	X		X
Beredskapsplan	X			X	X	X	X	X	X	X
Digital etterforskning (Samle spor)	X			X	X	X	X	X		X
Loggovervåkning	X	X	X	X	X	X	X	X	X	X
Nettverksovervåking	X	X	X	X	X	X	X	X		X
Rutiner for å koble fra enheter og nett	X			X	X	X	X	X		X
System for å oppdage inntrenging (Intrusion detection system)	X			X	X	X	X	**X**		X
Tilbakelegging av sikkerhetskopi (Rent system)	X	X	X	X	X	X	X	X		X
Tilkobling til CERT	X			X	X	X	X	X		X

Faktaboks 23: Barrierer for å redusere konsekvensen av en hendelse

6 REFERANSER

/1/ Risiko 2015, Nasjonal Sikkerhetsmyndighet:
http://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2015-web.pdf

/2/ NOU 2000:24, Et sårbart samfunn — Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet:
https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf

/3/ Fokus 2015 er Etterretningstjenesten ugraderte vurdering av områder som anses som særlig relevante for norsk sikkerhet og nasjonale interesser:

http://forsvaret.no/fakta/undersokelser-og-rapporter/fokus

/4/ Evaluering av den statlige oljevernaksjonen etter grunnstøtingen av MV Full City 31. juli 20099:

http://evalueringsportalen.no/evaluering/evaluering-av-den-statlige-oljevernaksjonen-etter-grunnstotingen-av-mv-full-city-31.-juli-2009

/5/ The Fiscal Times/Reuters: Cost of Union Dock Strike in CA: $1B a Day:
http://www.thefiscaltimes.com/Articles/2012/12/03/Cost-of-Union-Dock-Strike-in-CA-1B-a-Day

/6/ UT news: UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea:

http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea

/7/ The General Lighthouse Authorities of the United Kingdom and Ireland: GPS Jamming and the Impact on Maritime Navigation:

http://www.navnin.nl/NIN/Downloads/GLAs%20-%20GPS%20Jamming%20and%20the%20Impact%20on%20Maritime%20Navigation.pdf

/8/ GPS Spoofing and Jamming: A global concern for all vessels. By Ms. Brittany M. Thompson. I Proceedings of the Marine Safety & Security Council, the Coast Guard Journal of Safety at Sea, Vol. 71, Number 4, Winter 2014-2015.

http://www.uscg.mil/proceedings/archive/2014/Vol71_No4_Wint2014.pdf

/9/ National Transportation Safety Board Washington, Marine Accident Report: Grounding Of The Panamanian Passenger Ship Royal Majesty On Rose And Crown Shoal Near Nantucket, Massachusetts June 10, 1995

http://www.ntsb.gov/investigations/AccidentReports/Reports/mar9701.pdf

/10/ CyberKeel : Maritime Cyber-Risks, Virtual pirates at large on the cyber seas.

http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf

/11/ Fokus på risiko 2015

http://www.sjofartsdir.no/Global/Ulykker-og-sikkerhet/Ulykker og sikkerhet_dokumenter/Fokus p%c3%a5 risiko 2015_WEB revidert.pdf

/12/ Trend Micro: A Security Evaluation of AIS

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf

/13/ Techworld: Hackers planted remote devices to smuggle drugs through Antwerp port, Europol reveals:

http://www.techworld.com/news/security/hackers-planted-remote-devices-smuggle-drugs-through-antwerp-port-europol-reveals-3474018/

/14/ NCC Group: Preparing for Cyber Battleships – Electronic Chart Display and Information System Security:

https://www.nccgroup.trust/media/481230/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf

/15/ US Navy: Command Investigation into the Grounding of USS Guardian (MCM 5) on Tubbataha Reef, Republic Of The Philippines that Occurred on 17 January 2013:

http://www.cpf.navy.mil/foia/reading-room/2013/06/uss-guardian-grounding.pdf

/16/ Evaluering av den statlige oljevernaksjonen etter grunnstøtingen av MV Full City 31. juli 20099:

http://evalueringsportalen.no/evaluering/evaluering-av-den-statlige-oljevernaksjonen-etter-grunnstotingen-av-mv-full-city-31.-juli-2009

/17/ Norsk Standard NS 5832:2014 «Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse» http://www.standard.no/nyheter/nyhetsarkiv/bygg-anlegg-og-eiendom/2014/risikostandarder-mot-uonskede-handlinger/?gclid=CjwKEAjwp_uqBRClvrrXmsbPog4SJACK4gIPQW_YQhpaWgDOWk7BUp6WYoiWgvXJ75Gpyio25jfUrxoCFgfw_wcB

/18/ United States Government Accountability Office: Air Traffic Control. FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen

http://www.gao.gov/assets/670/669627.pdf

/19/ Wired: Feds Warn Airlines to Look Out for Passengers Hacking Jets

http://www.wired.com/2015/04/fbi-tsa-warn-airlines-tampering-onboard-wifi/

/20/ Exxon Valdez Oil Spill Trustee Council

http://www.evostc.state.ak.us/

/21/ Stavanger Aftenblad: 25 år siden Exxon Valdez. (24. mars 2014)

http://www.aftenbladet.no/energi/25-ar-siden-Exxon-Valdez-3383107.html

/22/ NCC Group: Preparing for Cyber Battleships – Electronic Chart Display and Information System Security:

https://www.nccgroup.trust/media/481230/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf

/23/ US Navy: Command Investigation into the Grounding of USS Guardian (MCM 5) on Tubbataha Reef, Republic Of The Philippines that Occurred on 17 January 2013:

http://www.cpf.navy.mil/foia/reading-room/2013/06/uss-guardian-grounding.pdf

/24/ Forskrift 29. mai 2013 nr. 539 om sikring av havner

https://lovdata.no/dokument/SF/forskrift/2013-05-29-539

/25/ NOU 1991:1A "Scandinavian Star"-ulykken, 7 april 1990. Hovedrapport, Oslo, 1991

https://www.regjeringen.no/globalassets/rpub/nou/19911991/001/pdfs/nou199119910001000dddpdfs.pdf

/26/ The threat of GPS jamming- the risk to an information utility» February 2014 Jeff Coffed/Exelis

/27/ Forskrift om sikring av havner.

https://lovdata.no/dokument/SF/forskrift/2013-05-29-539

/28/ Ulykker skjer ikke – de forårsakes; En studie på hva som kjennetegner er «sikkert rederi» Dr.Ing. Torkel Soma/DNV Maritime Solutions

/29/ Wikipedia : Costa Concordia disaster (14.05.2015)

http://en.wikipedia.org/wiki/Costa_Concordia_disaster

/30/ ENISA: Analysis Of Cyber Security Aspects In The Maritime Sector

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport

/31/ IMO Statistical Resources, Casualties
http://www.imo.org/KnowledgeCentre/ShipsAndShippingFactsAndFigures/Statisticalresources/Casualties/Pages/default.aspx

/32/ DV GL: Digitale Sårbareter Olje og Gass

/33/ *Vulnerability assessment of the transportation infrastructure relying on the global positioning system; John A. Volpe National Transportation Systems Center, 2001*

/34/ *Straight talk on anti-spoofing; Securing the future of PNT; Kyle Wesson, Daniel Shepard, Todd Humphreys, GPS World*

/35/ *Recommendation ITU-R M.1371-4*

/36/ NSM: Hvordan forebygge, oppdage og håndtere dataangrep:
http://nsm.stat.no/globalassets/dokumenter/temahefter/apt_2014_web.pdf

About DNV GL

Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organizations to advance the safety and sustainability of their business. We provide classification and technical assurance along with software and independent expert advisory services to the maritime, oil and gas, and energy industries. We also provide certification services to customers across a wide range of industries. Operating in more than 100 countries, our 16,000 professionals are dedicated to helping our customers make the world safer, smarter and greener.