SINTEF

OC2020 F-096 - Åpen

Rapport

Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet

Forfatter(e)
Per Håkon Meland
Karin Bernsmed
Ørnulf Jan Rødseth
Dag Atle Nesheim

SINTEF Ocean AS
Maritim transport
2021-01-08

SINTEF Ocean AS
Postadresse:
Postboks 124 Blindern
0314 Oslo
Sentralbord: 46415000

Foretaksregister:
NO 937 357 370 MVA

Rapport

Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet

EMNEORD:
Cybersikkerhet
Trusselvurdering
Maritim

VERSJON	DATO
1.1	2021-01-08

FORFATTER(E)
Per Håkon Meland
Karin Bernsmed
Ørnulf Jan Rødseth
Dag Atle Nesheim

OPPDRAGSGIVER(E)	OPPDRAGSGIVERS REF.
Kystverket	32602495

PROSJEKTNR	ANTALL SIDER OG VEDLEGG:
302005756	29+0

SAMMENDRAG

Overskrift sammendrag

Rapporten tar for seg en gjennomgang av cybersikkerhet-relaterte hendelser innen maritim og offshore sektor de siste ti årene og presenterer deretter en rangering av relevante cybertrusler for maritim næring.

Rapportens kontekst og omfang ("scope") baseres på en overordnet systembeskrivelse av den maritime sektor og en beskrivelse av skipet og dets systemer. Dette med tanke på å definere relevante aktører, systemer og dermed potensielle angrepspunkter. Gjennomgangen av hendelser er internasjonal, all den tid norske, maritime interesser må sees i en internasjonal kontekst.

UTARBEIDET AV	SIGNATUR
Per Håkon Meland	GODKJENT ELEKTRONISK
KONTROLLERT AV	SIGNATUR
Egil Wille	GODKJENT ELEKTRONISK
GODKJENT AV	SIGNATUR
Trond Johnsen	GODKJENT ELEKTRONISK

RAPPORTNR	ISBN	GRADERING	GRADERING DENNE SIDE
OC2020 F-096	N/A	Åpen	Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
0.1	2020-08-20	Rapport klar for intern QA
1.0	2020-08-26	Rapport klar for levering til kunde
1.1	2021-01-08	Rapport nedgradert fra "fortrolig" til "åpen"

Innholdsfortegnelse

Forkortelser og ordforklaringer

Forkortelse	Forklaring
AIS	Automatic Identification System, skipsinformasjon og navigasjonsdata sendt over digital VHF.
Angrepsvektor	Metoden en angriper velger for å utføre et angrep på en datamaskin, et nettverk eller et system.
AtoN	Aids to Navigation, seilingsmerker som fra tid til annen bruker digital VHF, vanligvis AIS, til å sende ut informasjon.
CCTV	Closed Circuit Television, videoovervåkning.
DSC	Digital Selective Calling, digital signalering over VHF, også del av GMDSS.
ECDIS	Electronic Chart Display and Information System, elektronisk kartplotter.
GMDSS	Global Maritime Distress and Safety System, sett av protokoller, utsyr og internasjonale tjenester som skal sikre at informasjon om nødsituasjoner kommer frem til rette vedkommende.
GNSS	Global Navigation Satellite System, inkluderer GPS, GLONASS, Galileo og andre systemer.
HF	High Frequency, kortbølge på radio.
IP	Internet Protocol, vanligste protokollsettet i industrielle og åpne datanettverk.
Jamming	Forstyrrelser, blokkering eller fastlåsing av for eksempel radiosignaler.
Malware	En generell betegnelse på ondsinnet programvare.
MF	Medium Frequency, mellombølgen på radio.
MRS	Mandatory Ship Reporting, innrapportering av skip i forbindelse med passering gjennom for eksempel VTS-områder eller ved spesielle hendelser.
MSI	Maritime Safety Information, sikkerhetsmeldinger som blir kringkastet over GMDSS tjenestene NAVTEX og Safetynet.
MSW	Maritime Single Window, i Norge er dette SafeSeaNet Norway som opereres av Kystverket.
NAVTEX	Smalbåndet digital meldingstjeneste over MF eller HF.
OpenIOC	Et åpent rammeverk for deling av trusselinformasjon i et maskinlesbart format. IOC= Indicators of Compromise.
PA	Public Announcement, sikkerhetsrelatert og annen informasjon til passasjerer og mannskap på skipene.
Ransomware/løsepengevirus	En type ondsinnet programvare som gjør filer eller system utilgjengelige, som oftest gjennom kryptering. Angriper ber om løsepenger for å gjøre dekrypteringsnøkkel tilgjengelig.
SATCOM	Kommunikasjon via satellitt.
Social engineering	(Norsk: Sosial manipulering) betyr angrepsteknikker hvor man lurer menneskelige brukere istedenfor tekniske systemer. Gjennomføres ofte ved hjelp av falske eposter eller telefonsamtaler, samt en klype sjarm.
Spear-phishing/phishing	Spear-phishing går ut på å sende tilsynelatende autentiske eposter til spesifikke personer man har gjort en undersøkelse på i forkant. Phishing er enklere varianter hvor mottakere kan være mer tilfeldige.
Spoofing	Går ut på å forkle falsk kommunikasjon som noe ekte.
RCC	Remote Control Center, overvåkning av skip fra land.
SSAS	Ship Security Alert System, system for varsling av for eksempel kapring av skipet.

Forkortelse	Forklaring
Tailgating	En uautorisert person får tilgang ved å følge etter noen med autorisasjon.
VDES	Fremtidig VHF Data Exchange System, inkluderer AIS og VDE, høyere båndbredde digital kommunikasjon.
VHF	Very High Frequency, normalt skip til skip og skip til land kommunikasjonssystem, både med tale og digital dataoverføring (DSC og AIS).
VoIP	Voice over IP, IP protokoller for taleoverføring.
VTS	Vessel Traffic Services, en form for maritim trafikkovervåkning og rådgiving.

1 Innledning

Denne rapporten er leveranse fra prosjektet "Trusselvurdering i forbindelse med strategi for maritim digital sikkerhet", eid av Sjøfartsdirektoratet og gjennomført av SINTEF Ocean og SINTEF Digital. Leveransen faller inn under Sjøfartsdirektorats arbeid med Strategi for Maritim Digital Sikkerhet.

Rapporten tar for seg en gjennomgang av cybersikkerhet-relaterte hendelser innen maritim og offshore sektor de siste ti årene og presenterer deretter en rangering av relevante cybertrusler for maritim næring.

Rapportens kontekst og omfang ("scope") baseres på en overordnet systembeskrivelse av den maritime sektor og en beskrivelse av skipet og dets systemer. Dette med tanke på å definere relevante aktører, systemer og dermed potensielle angrepspunkter. Gjennomgangen av hendelser er internasjonal, all den tid norske, maritime interesser må sees i en internasjonal kontekst.

Cybersikkerhet defineres av Koordineringsgruppen[1] for IKT-risikobildet som "Cybersikkerhet omfatter tiltak for beskyttelse mot reelle og potensielle trusler som kanaliseres via IKT-infrastruktur. Cybersikkerhet er en underkategori til IKT-sikkerhet." I denne sammenhengen benytter vi ISO/IEC 27005 [1] sin definisjon av trussel, som er "en potensiell årsak til en hendelse, som kan resultere i skade på system og organisasjon."

IKT-sikkerhet favner et mer generelt og bredere spekter av farer og trusler, inkludert naturkatastrofer, uhell og fysisk ødeleggelse. I denne rapporten utelukkes denne type farer og trusler. Rapporten skiller dermed ikke på "security" og "safety", utover det faktum at vi fokuserer på ondsinnede/villede handlinger, ikke menneskelig svikt og systemsvikt.

[1] Politiets sikkerhetstjeneste, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet, 2010

2 Systembeskrivelse

Maritim virksomhet har en del spesielle egenskaper som kan gjøre trussel-profilen forskjellig fra mer tradisjonelle landsystemer:

1. Det er et lite system, med omtrent 95 000 skip i UNCTADs database[2]. Av dette er ca. 50 000 skip over 1000 tonn. Dette betyr at det er begrensede ressurser til mer systematiske analyser og forbedringsprosesser innen bransjen, også angående cybersikkerhet.
2. Det er et meget kostnadssensitivt marked på grunn av sterk internasjonal konkurranse om fraktoppdrag. Dette gir en stor andel operatører og skip som ikke prioriterer cybersikkerhet høyt nok.
3. Skipene vil vanligvis seile imellom 25 og 35 år og oppgraderinger gjøres gradvis/trinnvis slik at utstyr om bord ikke skiftes ut samtidig. Det betyr også at det er svært blandet datautstyr om bord i skipene, både for mer administrative funksjoner og for styringssystemene. Dette er en fordel fordi det kan være vanskelig å forutsi hva slags datamaskin et angrep skal rettes mot, men der er også en ulempe fordi det er vanskelig å drifte systemene og å sørge for oppdaterte operativsystemer og sikkerhetsmekanismer.
4. Skipene er også internasjonalt regulert som delvis gir ulemper ved at det ofte blir minimumskrav som gjelder, men som også gir fordeler ved at sikkerhetsaspektet er prioritert og tilstedeværende.

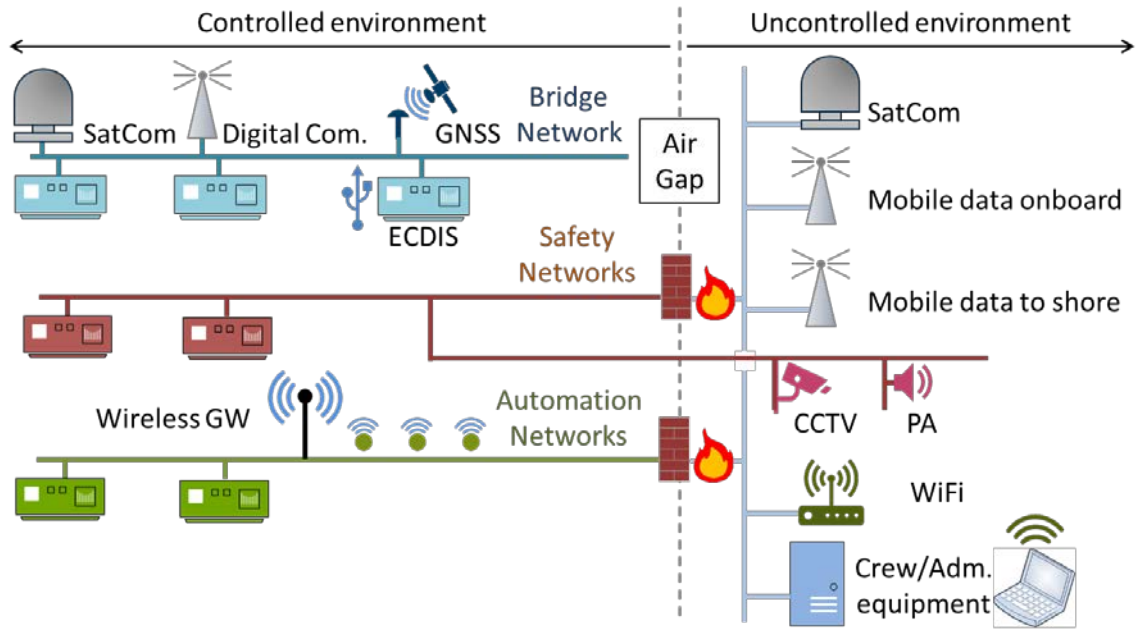
Dette avsnittet vil presentere to generaliserte kontekstdiagram som kan brukes som referanse for denne analysen. Ett diagram vil vise en oversikt over datasystemene om bord i skip og det andre vil gi en tilsvarende oversikt over de viktigste kommunikasjonssystemene (og aktørene) som er involvert i skipsfart. Disse vil blant annet vise hvor eventuelle sikkerhetsproblem kan oppstå.

2.1 Generell oversikt over skipssystemet

Figur 1 viser en generell skisse av et moderne datasystem om bord i skip. Det reelle systemet på et skip vil kunne være forskjellig fra dette på mange måter:

- Mange skip har ikke IP-baserte datanettverk i sub-systemene til venstre, men bruker for eksempel serielinjer eller feltbuss-løsninger for kommunikasjon mellom enhetene. Noen skip har ikke datanettverk om bord i det hele tatt.
- Spesialskip, for eksempel for rørlegging eller kranoperasjoner kan ha egne nettverk for styring av dynamisk posisjonering og annet spesialutstyr på skipet.

[2] UNCTAD, 2019, United Nations Conference on Trade and Development, Review of Maritime Transport, 2019.



Figur 1 – Generelt datasystem ombord i skip

Datasystemene om bord er delt opp i kontrollerte nettverk som er relatert til styring av skipssystemer og ukontrollerte nettverk som kan være for administrative gjøremål eller for mannskap. Administrative nettverk vil ofte ha beskyttelse fra mannskapsnettverk, noe som ikke er tegnet inn her.

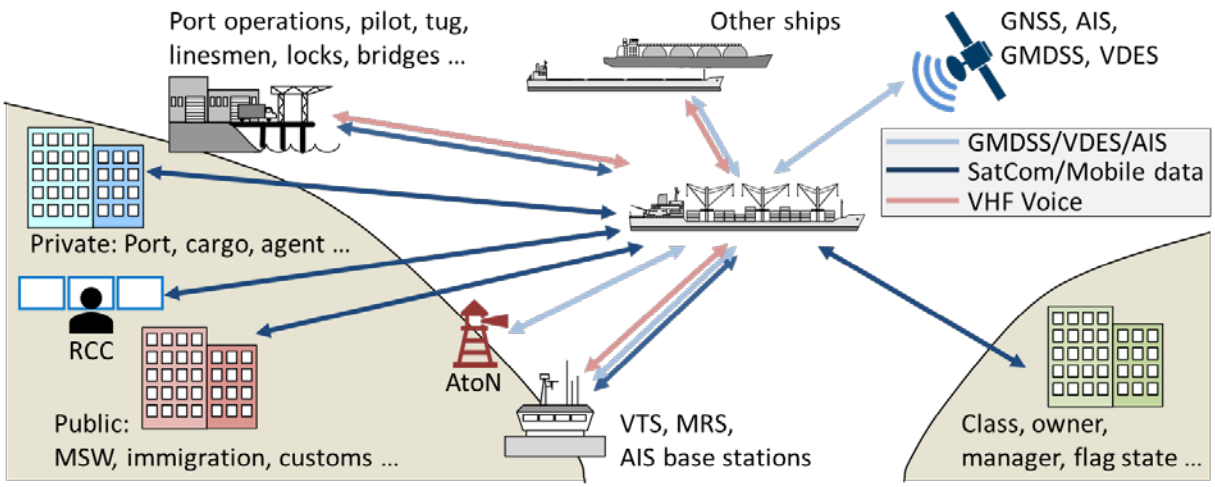
De kontrollerte nettverkene vil være installert slik at de ikke kan fysisk nås av utenforstående, uten at fysiske barrierer brytes (låste dører, inne i kabinett etc.). Ett unntak kan være noen sikkerhetsnettverk som for eksempel kan bruke datanettverk og VoIP for å overføre PA-meldinger eller IP-baserte protokoller for CCTV. Da vil den fysiske barrieren for å få tilgang til nettet være lavere enn for de helt lukkede nettverkene.

Kontrollerte nettverk kan være helt fysisk adskilt fra de generelle nettverkene om bord ("Air Gap") eller de kan være koblet til dem gjennom en form for brannmur.

På de ukontrollerte nettverkene vil det i dag være koblinger mot satellitt eller mobilt bredbånd for å kunne koble seg til internett i land. Det begynner også å bli vanlig å installere WiFi eller mobilt datanett om bord som kan brukes av mannskapets egne mobiltelefoner eller PCer.

2.2 Generell oversikt over maritimt kommunikasjonssystem

Hvis man tar utgangspunkt i skipet, så gir **Figur 2** en oversikt over de vanligste kommunikasjonskanalene. Her er mørk blå forskjellige typer digital eller stemme-kommunikasjon over satellitt eller mobile data- og stemmenettverk. Lys blå er digital smalbånd-kommunikasjon over VHF eller andre maritime radiokanaler, for eksempel GMDSS, NAVTEX eller VDES. Dette inkluderer også GNSS samt mottak av differensielle korreksjonssignaler til GNSS som for eksempel kan sendes på MF. I dag brukes det også satellitter for å lytte til AIS-signaler fra skip og det eksperimenteres med å sende MSI-type informasjon fra de samme satellittene. Lys rød er stemmekommunikasjon over VHF. I forbindelse med introduksjon av e-navigasjon kan man forvente at en del av denne kommunikasjonen blir digitalisert og overført til VDES.



Figur 2 – Generelle kommunikasjonskanaler til og fra skipet

RCC (Remote Control Center) har vært diskutert i forbindelse med autonome skip, men brukes også i overvåkning av mer konvensjonelle skip, blant annet i cruise-industrien og for overvåkning av teknisk utstyr om bord. Kommunikasjon med AtoN (Aids to Navigation) er vanligvis visuell, men det er i økende grad også bruk av digital VHF i dette området, for eksempel for å markere vrak, fiskebruk, merder og andre midlertidige seilingshindringer med AIS-signaler. Dette brukes også noen ganger til å sende lokale værdata, for eksempel strøm, tidevann og vind.

2.3 Oversikt over relevante angrepspunkter

Tabellene under vil gi en oversikt over noen viktige angrepspunkter mot maritime systemer. Tabellene er ikke komplette og er inkludert som forslag. De bør oppdateres etter behov. Vi har bare inkludert punkter som kan utgjøre en sikkerhetsrisiko.

Tabell 1. Skipsrelatert, herunder også offshore-installasjoner

Referanse	Beskrivelse
S1	Operasjonssystemer om bord (bro, maskin, etc.)
S2	Administrative systemer om bord
S3	Satellitt eller mobil datakommunikasjon
S4	VHF-kommunikasjon for operativt bruk, inkludert AIS
S5	GMDSS-kommunikasjon til eller fra skip
S6	GNSS- eller andre navigasjonssignaler
S0	Annet

Tabell 2. Offentlig infrastruktur på land relatert til skip

Referanse	Beskrivelse
L1	VHF-stasjoner (Stemme, DSC, AIS basestasjoner) og tilhørende nettverk
L2	VTS og nettverk som knytter VTS til andre datasystemer
L3	GMDSS infrastruktur (unntatt VHF)
L4	Annen informasjon til skip (anbefalte ruter, notices to mariners etc.)
L5	MSW og tilhørende kommunikasjon til myndigheter og havner
L6	Navigasjonshjelpemidler (AtoN) med digital transmisjon
L0	Annet

Tabell 3. Myndighetssystemer

Referanse	Beskrivelse
M1	Sertifikater og annen myndighets-informasjon om skip eller mannskap
M2	Klasserelatert informasjon om skip
M3	Klarering av skipsanløp (toll, immigrasjon, helse, veterinær …)
M4	Datasystemer relatert til skipsanløp og operasjoner
M5	Datasystemer relatert til informasjon om passasjerer og last på skip og i terminaler (toll, immigrasjon, ISPS, klarering inn/ut)
M0	Annet

Tabell 4. Havn og terminal

Referanse	Beskrivelse
H1	Kommunikasjon mellom skip og havnetjenester
H2	Kommunikasjon internt i havn
H3	Datasystemer relatert til skipsanløp og operasjoner
H4	Datasystemer relatert til informasjon om passasjerer og last på skip og i terminaler (toll, immigrasjon, ISPS, klarering inn/ut)
H0	Annet

Tabell 5. Private aktører

Referanse	Beskrivelse
P1	Reder, manager eller chartrer
P2	Verft, utstyrsleverandører og annen teknologi
P3	Tjenesteleverandører
P0	Annet

3 Tidligere arbeid

Vi har tatt for oss tidligere arbeid relatert til vurdering av maritime trusler og sårbarheter for å få en historisk oversikt og se om det har vært noen spesiell utvikling over tid.

Går vi tilbake til 2006, ga sikkerhetsselskapet RAND [2] ut en tidlig bok om moderne maritim terrorisme, men denne omhandler i veldig liten grad angrep/aksjoner relatert til cyber-domenet. Dette har vært en trend i mye av den påfølgende litteraturen også, med fokus på "tradisjonell" maritim piratvirksomhet og studier av terroristorganisasjoner som har angrepet skip, eksempelvis al-Qaeda, Lashkar-e-Taiba, LTTE (Sri Lanka) og Al Shabaab (Somalia) [3].

Går vi til 2011 utga ENISA[3] rapporten "Analysis of Cyber Security Aspects in the Maritime Sector" [4], hvor den maritime sektoren blir trukket fram som kritisk infrastruktur og det ble identifisert et sett med utfordringer som setter cybersikkerheten på prøve:

a) Liten bevissthet og fokus på maritim cybersikkerhet i næringen.
b) Komplekst IKT-miljø.
c) Fragmentert organisering og styre (governance).
d) Manglende inkludering i maritime reguleringer og lover.
e) Ingen helhetlig tilnærming til maritime cyber-risikoer.
f) Manglende økonomiske insentiver for å implementere cybersikkerhet.

[3] The European Union Agency for Cybersecurity (ENISA), https://www.enisa.europa.eu/

I EU-prosjektet MUNIN [5] ble det i 2015 laget en risikomatrise for både security og safety, hvor de høyest rangerte truslene var knyttet til jamming, spoofing og hacking av AIS, GPS og kommunikasjonssystemene om bord.

Samme år (2015) kom Lysneutvalget med en egen rapport [6] på digitale sårbarheter i maritim sektor, hvor topp 10 ble definert til å være:

a) Manglende oppmerksomhet og opplæring hos de ansatte og underleverandører på sjø og land.
b) Navigasjonssignaler fra satellitt er normalt ikke beskyttet mot modifikasjon.
c) System for identifikasjon av fartøy er normalt ikke beskyttet mot modifikasjon.
d) Fjernoppkobling mot kritiske systemer for vedlikehold.
e) Et stort antall aktører utveksler mye informasjon på usikret e-post om skip, last og passasjerer.
f) Separasjon av datanett om bord og i havner.
g) Bruk av mobile lagringsenheter.
h) Bookingsystemer og administrasjonssystemer for passasjerer, last og havneanlegg er sårbare.
i) Manglende fysisk sikring av datarom, kablingsskap, m.m. på skip.
j) Begrenset autentisering av brukere mot systemer for offentlig innrapportering. System for autentisering av utenlandske borgere mangler.

Jones et al. [7] fra University of Plymouth har i mange år jobbet med maritim cybersikkerhet, og publiserte i 2016 en artikkel som innehold en taksonomi over maritime trusler, kort oppsummert:

a) Systemsårbarheter for havn og skip, for eksempel kompromittering av ECDIS eller AIS.
b) Digital kapring (hijacking), hvor skip styres inn i andre mål eller blir utilgjengelige etter løsepengevirus (ransomware).
c) Utdatert programvare om bord på skip med mange kjente sårbarheter.
d) Kostnader og profitt, som peker på at det er relativt billig å angripe skip, samt at det er gode muligheter for avkastning ettersom 90% av verdens handel blir transportert med skip.

I det norske CySiMS-prosjektet ble det i 2017 skrevet en egen rapport som vurderte risiko spesifikt rundt maritim digital kommunikasjon [8]. Tabell 6 er gjengitt fra denne rapporten som viser hvilke trusler som ble vurdert for ulike tjenester som benyttet seg av digital kommunikasjon.

Tabell 6. Trusler spesifikke for digital kommunikasjon.

General threat	Unwanted event
Jamming of terrestrial link	Loss of one or more messages
Jamming of satellite link	Loss of one or more messages
Short DoS attack towards shore-based system	Limited or no communication capacity for a short period of time (1-2 hours)
Long DoS attack towards shore-based system	Limited or no communication capacity for a long period of time (1-2 days, or more)
Wiretapping of terrestrial link	Confidential data overheard by an unauthorised actor
Wiretapping of satellite link	Confidential data overheard by an unauthorised actor
Repudiation of transmitted message	Data is received, but the sender denies having sent the data
Repudiation of received message	Data is sent, but the receiver denies having received the data
Broadcasting of false messages on an open channel	False data received by one or more actors listening to the broadcast channel
Transmission of an unauthenticated message to a single actor	False data received by the ship or the shore
Retransmission of a previously transmitted message	False data received by the ship or the shore

Det britiske *Department of Transport* publiserte i 2017 en egen IET standard "Code of Practice: Cyber Security for Ships" [9] som identifiserer seks hovedkategorier med motivasjoner for trusler:

a) Cyber misbruk (misuse), som inkluderer enkel vandalisering og systemforstyrrelser av ikke-eksperter og misfornøyde innsidere.
b) Aktivistgrupper (hacktivism), som ønsker publisitet rundt sin sak eller for å legge press på organisasjoner.
c) Spionasje, uautorisert tilgang til sensitiv informasjon (IPR, kommersielle data, strategier og personlige data).
d) Organisert kriminalitet, i hovedsak økonomisk vinningskriminalitet. Dette kan relateres til tyveri av gods, smugling av narkotika, menneskehandel og skatteunndragelse.
e) Terrorisme, som benytter skip til å skape frykt for fysisk ødeleggelse eller økonomiske forstyrrelser.
f) Krig (warfare), konflikter mellom stater kan føre til skade på infrastruktur eller operasjonsnekt.

I 2018 publiserte BIMCO et sett med retningslinjer for cybersikkerhet om bord på skip [10]. Denne rapporten gir praktiske anbefalinger på håndtering av cybersikkerhet i land- og skipsbaserte systemer. I tillegg inkluderer rapporten støtte for identifisering og analyse av sårbarheter og trusler, risikovurdering og håndtering av hendelser. Spesielt relevant for vår analyse er listen med typiske sårbarheter på skipene:

- Umoderne og ustøttede operativsystemer
- Utdaterte eller manglende antivirus programvare og mangler på beskyttelse fra skadevare
- Utilstrekkelige sikkerhetskonfigurasjoner og tiltak, inkludert virkningsløs nettverksbeskyttelse og utstrakt bruk av standard brukernavn og passord for admin-kontoer.
- Skipsnettverk som mangler grensebeskyttelse og segmentering
- Sikkerhets-(safety) kritisk utstyr som er permanent koblet til landbaserte systemer
- Utilstrekkelig tilgangskontroll for tredjeparter, inkludert entreprenører og tjenestetilbydere

Rapporten inneholder i tillegg en oversikt over systemer, utstyr og teknologier som bør beskyttes.

Vinnem og Utne [11] fra NTNU så i 2018 på trusler mot autonome skip og hva man kan lære fra faktiske hendelser innen andre industrier (petroleum, biler, energi). Forfatterne peker først og fremst på faren med et hacket autonomt skip og den skaden det kan gjøre ved at man bevisst krasjer det inn i oljeinstallasjoner, infrastruktur langs kysten eller cruiseskip og oljetankere.

ENISA kom på tampen av 2019 med en ny rapport [12] som omhandlet cybersikkerhet for havner. Det mest interessante herfra er beskrivelsene av verdier (assets) som skal beskyttes, en trusseltaksonomi, utfordringer for cybersikkerhet og et sett med kritiske angrepsscenarioer. Trusseltaksonomien her skiller mellom konsekvensene:

a) Operasjonsavbrudd
b) Menneskelig skade, død, kidnapping
c) Tyveri av sensitive eller kritiske data
d) Tyveri av last
e) Smugling (narkotika, våpen, ulovlig gods og mennesker)
f) Finansielle tap
g) Svindel eller tyveri av penger
h) Skade eller ødeleggelse på havnesystemer/infrastruktur
i) Ødelagt renommé, tap av konkurransedyktighet
j) Miljøkatastrofe

og selve truslene (selv om det er noe overlapp med konsekvenser):

a) Avlytting, hindring og kapring av datakommunikasjon, som inneholder *interception of emissions, interception of sensitive information, man in the middle/session hijacking, network reconnaissance, network traffic manipulation.*
b) Forbrytersk aktivitet, som inneholder *Denial of Service (DOS), malware, brute force, phishing, identity theft, social engineering, targeted attacks, abuse and theft of data, manipulation of information, geolocalisation signals spoofing/jamming.*
c) Katastrofe, med elementene *environmental disasters, natural disasters.*
d) Driftstans, som *inneholder main supply outage, network outage, absence of personnel, loss of support.*
e) Utilsikted skade, som inneholder *use of unrealiable source, erroneous administration of IT/OT systems, resulting from penetration testing, data deletion, 3rd party security failure, information leakage.*
f) Fysiske angrep, som inneholder *fraud, sabotage, vandalism, theft, unauthorised access, terrorism, hacktivism, coercion, extortion or corruption, piracy/illegal crime/Mafia.*
g) Feil og maskinsvikt knyttet til *systems, devices, navigation and communication systems, main supply systems, failure or distruption of service providers.*

I år (2020) ble det utgitt en artikkel av Caprolu et al. [13] som omhandler utfordringer med "vessel cyber security" og som peker på følgende:

a) Manglende "GNSS Spoofing Detection".
b) Måter å begrense elektronisk krigføring på, først og fremst knyttet til jamming av GNSS og SATCOM.
c) Manglende sikkerhetsstandardisering for SATCOM.
d) Manglende "AIS Spoofing Detection".
e) Manglende sikkerhetsvurdering av brosystemer.
f) Malware-angrep er effektive når det er dårlig fysisk separasjon mellom systemer.
g) Manglende integrasjon av safety-systemer.
h) Bruk av utdatert og proprietær sikkerhet i kommunikasjonssystemer.

Boken *Global Challenges in Maritime Security - An Introduction* [14] fra 2020 inneholder et eget kapittel dedikert til cybersikkerhet og trekker fram følgende systemer, tjenester og felt som er spesielt utsatte som under en cyberhendelse:

- Tap av forretningskritisk informasjon.
- Finansielle tap.
- IT- og OT-systemers konfidensialitet, integritet og tilgjengelighet.
- Sikkerhet ("safety") for liv og navigasjon til sjøs, som igjen kan gi miljøskader.

I sin årlige nasjonale trusselvurdering [15] peker Politiets sikkerhetstjeneste (PST) ut statlig etterretningsvirksomhet som en av de største truslene mot Norge i 2020, og trekker fram virksomheter innen maritime teknologi som et særlig utsatt mål. Spionasjen vil rette seg mot underleverandører så vel som mot hovedleverandører av tjenester og produkter

Rapporten "RISIKO 2020" [16] fra Nasjonal Sikkerhetsmyndighet (NSM) som ble utgitt våren 2020 gir en oppdatert oversikt over risikobildet i Norge. Rapporten beskriver sårbarheter i virksomheter og på nasjonalt plan, hvordan trusselaktører kan utnytte dem og hvilken risiko dette medfører. Sammen med rapporten "Helhetlig digitalt risikobilde" fra 2019 [17] gir denne rapporten et godt grunnlag for å vurdere hvilke typer av trusler som vil bli relevante for Norge og norske interesser i årene fremover. I sum så finner disse to rapportene at hovedtrenden er den samme i år som for tidligere år: den digitale risiko øker. Det er flere verdier som må passes på, det finnes fortsatt betydelige digitale sårbarheter i det norske samfunnet og hos norske virksomheter og vi blir stadig utsatt for angrep fra profesjonelle og målrettede trusselaktører. Under vil vi trekke frem noen faktorer fra disse to rapportene som vi finner spesielt relevante for den maritime sektoren i Norge:

- Den store betydningen av satellittbaserte tjenester, deriblant posisjonsbestemmelse, navigasjon og tidsbestemmelse (PNT), for luftfart, sjøfart og navigasjon på land. *Forstyrrelser eller bortfall av PNT-tjenester* er identifisert som en stor risiko, hvor tilsiktet "jamming" og andre former for forstyrrelse av satellittsignaler sies å benyttes aktivt for militære formål. NSM poengterer at alle brukere av satellittbaserte tjenester bør vurdere behovet for reserveløsninger, inkludert rutiner og alternative prosedyrer og de påpeker spesielt at sektormyndigheter og deres overordnede departementer har et særlig ansvar.
- *Løsepengevirus* er også tatt opp spesielt og NSM skriver at de de siste årene har sett en økning av løsepengevirus rettet mot bedrifter og virksomheter som har større betalingsevne enn enkeltpersoner.

NSM ser i tillegg et jevnt trykk av det de refererer til som *digitale etterretningsoperasjoner*, mot norske virksomheter hvor fremmende stater søker etter høyteknologi og forretningshemmeligheter. I rapporten er den maritime sektoren pekt ut som et av flere utsatte mål i Norge. Videre peker rapporten ut *digitale verdikjeder* og *tjenesteutsetning i skyen* som mulige risikofaktorer og fremhever at trusselaktører kan utnytte virksomheter og produkter ett sted i verdikjeden for å få tilgang til informasjon og funksjonalitet andre steder i verdikjeden. Rapporten advarer i tillegg spesielt mot å bli låst til én leverandør ved tjenesteutsetting. *Droner som verktøy* er pekt ut som en mulig risiko; dog er fokus i rapporten på innsamling informasjon fra luftbårne sensorer. Bruk av droner som våpen er i tillegg nevnt som en trussel i noen deler av verden. Rapporten påpeker at til tross for at norske virksomheter generelt er blitt flinkere på IKT-sikkerhet de siste årene, så er *den menneskelige faktoren* fortsatt en betydelig risiko. Epost er fortsatt en meget effektiv angrepsvektor og sosial manipulasjon og "tailgating" fungerer alfor ofte: "*Det er bare et spørsmål om tid*".

4 Oversikt over kjente hendelser

For å innhente informasjon om hendelser har vi lett etter vitenskapelige publikasjoner, offentlige og kommersielle rapporter, avisartikler og annen form for "grå litteratur" med søkeord knyttet til "cyber attack", "cyber risk", "cyber threat", "cyber security" og "maritime" i populære søkemotorer. Videre har vi brukt en "snowballing"-teknikk der vi går gjennom kildenes kilder for å fange opp artikler som ikke dukker opp i første omgang.

Vi har prøvd å benytte oss av flere uavhengige kilder for hver av hendelsene der det har vært mulig, og ettergått de opprinnelige kildene i rapporter som lister opp flere hendelser, for eksempel i Kapalidis [18], Jones et al. [7], KNect365 [19], Singh [20], CyberKeel [21]. Omfanget er begrenset basert på følgende kriterier:

- Tidsomfanget er begrenset til de siste 10 årene, dvs. mellom 2010 og 2020.
- Vi har bare tatt for oss vellykkede angrep, ikke angrepsforsøk.
- Vi har sett bort fra demonstrerte "white hat" angrep (for eksempel av studenter, sikkerhetsfirma og forskere, typisk GNSS-manipulasjon [22], AIS-spoofing, ECDIS-manipulasjon og modifisering av satellittkommunikasjon [21]).
- Vi har sett bort fra mindre enkelthendelser (ordinær "angrepsstøy"), men har prøvd å fange opp trender og endringer.
- Hovedfokus er på den type hendelser som er relevante for norske interesser.

Vi har også fått utlevert anonymiserte hendelsesdata fra *Den Norske Krigsforsikring for Skib* (DNK). Dette er data som ikke tidligere har vært omtalt i åpne kilder.

Resultatet av innhentingen kan sees i tabellen under, hvor hver hendelse har fått tildelt en identifikator, årstall, identifisert angrepspunkt, beskrivelse og dokumenterte tiltak som er blitt implementert som følge av hendelsen.

Tabell 7. Kronologisk oversikt over publiserte cyberhendelser

Id	År	Angreps-punkt	Beskrivelse	Tiltak i etterkant
A1	2010	S1	En Sørkoreansk oljeplattform på vei til Sør-Amerika blir infisert med skadevare (malware). Systemet som kontrollerer blowout blir rammet, og operasjonell drift stanses i 19 dager. Slike stopp estimeres til å bety et tap på $700,000 US for hver dag. Kilde: Houston Chronicle [23], CyberKeel [21].	Ingen spesielle tiltak nevnt i forbindelse med denne hendelsen, men en kilde nevner problemet med manglende cybersikkerhet-krav for safety-systemer.
A2	2010 - 2011	P1	Et gresk shipping-selskap sitt hovedkvarter blir hacket via WiFi-nettet. I de følgende to årene blir informasjon om skip og ruter brukt av de kriminelle til å gjennomføre fysiske piratangrep i Adenbukta. Kilde Kapalidis [18].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.

Id	År	Angreps-punkt	Beskrivelse	Tiltak i etterkant
A3	2011 - 2013	H4	Ved Antwerpen havn ble lastesporingssystemet infisert for å smugle containere med narkotika og våpen (skjult som bananer fra Sør-Amerika). Dette pågikk i to år før det ble oppdaget. Også i 2018 ble samme havn utsatt for samme type angrep. Kilder: Walker og Spencer [24], Lysneutvalget [6], Kapalidis [18], KNect365 [19].	Første tiltak var å installere en brannmur for å beskytte havna sine IT-systemer, men angriperne gjorde senere et fysisk innbrudd og installerte en trådløs bro slik at de kunne angripe systemet igjen.
A4	2011 - 2013	P2	Et angrep døpt "Icefog" av Kaspersky [25] rammet Japanske og Koreanske forretninger blant annet knyttet til skipsverft og maritime operasjoner. Dette var et målrettet angrep knyttet til industrispionasje, og benyttet teknikker som spear-phishing og utnyttelse av kjente sårbarheter. Kilde: Kaspersky [25].	For dette spesifikke angrepet ble det gjort tilgjengelig maskinlesbare angrepsindikatorer for OpenIOC-rammeverket.
A5	2011	P1	I et cyberangrep mot det statseide shipping-selskapet IRISL (Islamic Republic of Iran Shipping lines) ble all data knyttet til tariffer, last- og forsendelsesdata ødelagt, og lastedata stjålet. Det interne kommunikasjonsnettet ble også ødelagt. Hendelsen førte store økonomiske tap og tap av last. Kilder: Reuters [26], CyberKeel [21].	Etter flere cyberangrep mot kritisk infrastruktur i Iran har landet investert tungt i cyberforsvar [27]. Veldig få maritime cyberhendelser har blitt annonsert etter 2012 [20].
A6	2012	S3	Iran melder om angrep på deres kommunikasjonsnett på offshore-installasjoner i den persiske gulf. Kilde: Singh [20]	
A7	2012	H4	Fraktsystemet brukt av for toll- og grensekontroll i Australia ble infisert slik at angriperne kunne sjekke om deres containere var flagget som mistenkelige. I disse tilfellene ble smuglergodset aldri hentet. Kilde: CyberKeel [21].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.
A8	2012	M1	Kinesiske hackere blir anklaget for å ha stått bak et målrettet angrepet mot den Danske Søfartsstyrelsen (Danish Maritime Authority). Det ble stjålet dokumenter og informasjon om nettverksstrukturen for videre angrep. Infeksjonen kom fra en epost med et PDF-vedlegg. Kilde: Shippingwatch [28], CyberKeel [21].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.

Id	År	Angreps-punkt	Beskrivelse	Tiltak i etterkant
A9	2013	S1	Arbeidere på en borerigg i den Meksikanske gulfen kobler ved et uhell infiserte PCer og USB-utstyr til det lokale nettverket på riggen. Skadevaren forstyrrer signalene mellom posisjonssystemene og propellene. Hendelsen fører til en nedstenging av boreoperasjonen, Kilder: Athens Group [29], US Coast Guard [30], KNect365 [19].	Ingen spesielle tiltak nevnt i forbindelse med denne hendelsen, men den er blitt nevnt som et eksempel på mangel på sikkerhetskultur i bransjen. I 2015 ble US Coast Guard Cyber Strategy publisert [31].
A10	2014	P1	Eposter med kontonummer for overføring av penger mellom et anonymt rederi og drivstoffleverandør, samt mellom rederi og skipsverft, blir endret. Store pengesummer kommer på avveie. Kilde: CyberKeel [21].	Rapporten anbefaler prosesser for verifikasjon av opplysninger epost (for eksempel over telefon) eller prøveoverføring med mindre beløp.
A11	2012 - 2014	S4	En rapport fra Windward [32] viser at mellom 2012 og 2014 er 1% av alle IMO-nummer i AIS-signalene på verdensbasis manipulerte/falske. I tillegg skrur mer enn 25% av fartøyene av AIS i minst 10% av tiden ("going dark"). Slike teknikker benyttes gjerne i forbindelse med smugling, terrorisme, menneskehandel, illegalt fiske og i militære konflikter.	Per i dag kan man ikke stole på AIS-data alene. Skip og posisjoner må verifiseres med radar eller satellittbilder. Problemet med manipulering av AIS-data er økende.
A12	2016	S6	I Sør-Korea må 280 skip returnere til havn etter problemer med navigasjonssystemene. Nord-Korea har fått skylden for hendelsen, men dette er ikke bevist. Kilde: Kapalidis [18].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.
A13	2014 - 2017	S4	En analyse av historiske AIS-data fra Kystverket mellom 2014-2017 viser at sivile russiske fartøy gjennomfører gjentatte stopp langs norskekysten som ikke er naturlige for deres primære oppgave. Disse uregelmessighetene sammenfaller ofte i tid og rom med NATO-operasjoner, kurs eller øvelser, og det er grunn til å mistenke elektronisk spionasje/avlytting. Tilsvarende aktiviteter er observert i Sør-Kina-havet og Svartehavet. Kilde: Schnelle [33], Wallace og Mesko [34].	Som Schnelle foreslår i [33] er det mulig å benytte nettverksanalyse på AIS-data for å avdekke mistenkelig aktivitet i norske maritime interesseområder.

Id	År	Angreps-punkt	Beskrivelse	Tiltak i etterkant
A14	2017	P3	Det britiske skipsmeglerselskapet Clarksons blir hacket og angriperne krever løsepenger for data som er blitt stjålet. Noe sensitiv informasjon ble stjålet og aksjekursen på selskapet sank 5% rett i etterkant (andre kilder opplyser lavere tall). Kilder: KNect365 [19], Middle East Logistics [35], Bleeping Computer [36], Kapalidis [18].	Clarkson valgte å ikke betale løsepenger og gikk isteden ut med en offentlig advarsel til sine kunder.
A15	2017	P1	Verdens største shipping-selskap Maersk blir tilfeldig rammet av løsepengeviruset NotPetya som følge av en oppdatering for økonomisystemet MeDoc (brukes i Ukraina for skatterapportering). Viruset utnyttet en sårbarhet i Microsoft Windows og baserte seg på et lekket angrepsverktøy (EternalBlue) utviklet av US NSA. Hendelsen regnes som historiens mest ødeleggende cyberangrep og gikk ut over nær en femtedel av verdens shipping-operasjoner, inkludert 76 havner. Maersk har uttalt at de tapte nær $300 millioner i form av redusert inntekt som følge av hendelsen. Over 4000 servere, 45000 PCer og 2500 applikasjoner måtte reinstalleres. Kilder: WIRED [37], Maritime Executive [38], Singh [20] , Bleeping Computer [39], Kapalidis [18].	Maersk oppgir at de har iverksatt "different and further protective measures" etter angrepet [40]. Det var tilgjengelig patch mot sårbarheten i forkant av angrepet. Dette var en øyeåpner for aktører i den maritime bransjen verden over [19], og Maersk har fått ros for å ha vært så åpne om hendelsen. Andre aktører i bransjen ser ut å ha lært fra dette angrepet (se COSCO hendelsen i 2018).
A16	2017	S6	Minst 20 skip utenfor Novorossiysk i Svartehavet rapporterte om at deres posisjon er 32 km feil i navigasjonssystemene. Dette skyldes sannsynligvis GNSS-spoofing. Kilde: Kapalidis [18].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.
A17	2018	S6	Et skip blir utsatt for GPS-spoofing i Svartehavet (samme område som hendelse A16). Skipet befinner seg til sjøs, mens geolokasjonssystemet hevder det er på land. Dette skjer 4 ganger i løpet av 3 dager med varighet opp til 30 minutter. Kilde: DNK [41].	Skipseier er medlem i DNK og har blitt informert om preventive og reaktive tiltak for å sikre seg mot slike hendelser.

Id	År	Angreps-punkt	Beskrivelse	Tiltak i etterkant
A18	2018	P3	Kinesiske hackere får skylden for å ha stjålet informasjon fra leverandører til den amerikanske marinen. Også 27 amerikanske universiteter antas å ha blitt angrepet for å stjele forskningsdata knyttet til maritim teknologi. Kilde: Wall Street Journal [42] [43]	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.
A19	2018	H4	Barcelona havn rapporterer om et cyberangrep som viser seg å være en infeksjon av løsepengeviruset Ryuk. Dette gikk ikke ut over skipstrafikken, men de interne IT-systemene. Kilder: Safety4Sea [44], ZDNet [45].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.
A20	2018	H4	San Diego havn rapporterer om alvorlige forstyrrelser på sine IT-systemer. Også her er det snakk om løsepengeviruset Ryuk, og konsekvensene blir begrenset funksjonalitet ved havna. Hendelsen fant sted bare fem dager etter tilsvarende i Barcelona, og det er uklart om de er relaterte på noe vis. Kilder: Safety4Sea [44], ZDNet [45].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.
A21	2018	P2	Iranske hackere får skylden for å ha stjålet skipsdesign og ansattes personlige informasjon fra det australske verftet Austal. Austal leverer militære skip til både eget land og USA. Den stjålne informasjonen var uklassifisert og ble senere funnet til salgs på det mørke nettet. Hackerne prøvde også å kreve penger for informasjonen fra verftet. Kilde: Safety at Sea [46].	Kilden oppgir bare at flere sikkerhetsmekanismer er kommet på plass etter hendelsen.
A22	2017 - 2018	P1	Nigerianske svindlere med kallenavnet "Gold Galleon" har angivelig lurt til seg flere hundre tusen dollar ved å få tak i epostkontoer hos shippingselskaper og endre betalingsdetaljer. Angrepene har først og fremst vært rettet mot japanske og koreanske selskaper, men også Norge nevnes. Kilder: Safety at Sea [46], Secureworks [47]	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.

Id	År	Angreps-punkt	Beskrivelse	Tiltak i etterkant
A23	2018	P1	COSCO Shipping Lines sine kommunikasjonslinjer i USA ble angrepet. Dette er et av verdens største shipping-selskaper, og epost og telefonlinjer var ute av drift i fem dager. Interne eposter viser til at det var løsepengevirus som forårsaket skaden. Kilde: Dualog [48], Bleeping Computer [39] .	Det oppgis at COSCO hadde lært fra Maersk-hendelsen i 2017 og at dette reduserte konsekvensen av hendelsen. De ansatte tok i bruk private Yahoo-epost for å holde kontakt med kundene.
A24	2019	S1	Et stort skip på vei til New York får en malware-infeksjon i kontrollsystemet ombord som førte til redusert funksjonalitet. Kilde: Dark Reading [49].	Som en følge av denne hendelsen ble det gitt føderale råd til kommersielle skip om segmentering av nettverk ombord, individuelle passord og roller, beskyttelse og regelmessig oppdatering av systemene.
A25	2018 - 2019	S6	GPS-jamming er registrert i Troms og Finnmark (ved flere anledninger gjennom 2018-2019). Forstyrrelsene har til en viss grad påvirket skipstrafikk, men har heldigvis ikke fått alvorlige konsekvenser. Kilde: NSM [16].	Forsvaret/FFI testet i 2020 et varslingssystem for GPS-jamming, men per juni er det fremdeles ikke operativt. Eksisterende varslingssystemer langs den russiske grensen klarer ikke alltid å oppfatte jamming. Kilde: NRK [50].
A26	2019	H3	En ikke-navngitt amerikansk havn blir infisert av løsepengeviruset Ryuk. Infeksjonen kom som en lenke i en phishing-epost, og gjorde at overvåkningskameraer, adgangskontrollsystemer og overvåkningssystemer for kritiske prosesser ble satt ut av drift. Kilde: ZDNet [45].	Den amerikanske kystvakten publiserte informasjon om hendelsen for å advare andre maritime fasiliteter.
A27		P3	Den maritime tjenestetilbyderen James Fisher & Sons i England blir rammet av løsepengevirus og må stenge sine systemer. I etterkant av hendelsen falt aksjekursen til selskapet med 7%. Kilde: Cybersecurity Insiders [51].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.
A28	2019	S1	Et amerikansk maritimt anlegg for kompresjon av naturgass blir rammet av et løsepengevirus (sannsynligvis Ryuk) og må stenge ned i to dager. Angrepet kom via phishing-epost, og gikk ut over både IT- og OT-systemer. Kilder: Carrier Management [52], Dragos [53].	Department of Homeland Security (DHS) har sammen med Infrastructure Security Agency arbeidet med et cybersikkerhetsinitiativ for rørledninger.

Id	År	Angreps-punkt	Beskrivelse	Tiltak i etterkant
A29	2019	S2	Et tankskip ved Naantali havn i Finland får administrasjonsserveren infisert av et ukjent løsepengevirus. Også disken med backup blir overskrevet. Sannsynlige angrepsvektorer blir beskrevet som enten over Remote Desktop Protokollen, en USB-enhet eller epost-vedlegg. Samme skip blir rammet på nytt samme år fire måneder senere ved samme havn. Kilde: DNK [41].	Skipseier er medlem i DNK og har blitt informert om preventive og reaktive tiltak for å sikre seg mot slike hendelser.
A30	2019	S2	To skip med samme eier blir infisert av løsepengeviruset Hermes 2.1. Infeksjonen kom sannsynligvis over epost som en makro i et Word-dokument, og flere arbeidsstasjoner i den administrative delen ble rammet. Kilde: DNK [41].	Skipseier er medlem i DNK og har blitt informert om preventive og reaktive tiltak for å sikre seg mot slike hendelser.
A31	2020	S2	Et fartøy forankret ved Tynemouth, UK, får skipsserveren og PC-klienter infisert av løsepengeviruset Ryuk. To spesialister fra IT-tjenesteleverandør ble sendt om bord, og fant ut at all data var kryptert og tapt. Systemene måtte gjenoppbygges fra nytt. Kilde: DNK [41].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant. Skipet hadde allerede forsikring med dekning for cyberhendelser.
A32	2020	S2	Tre skip med Amerikansk flagg får administrative systemer infisert av løsepengeviruset Sodinokibi. Dette viruset truer også med å lekke informasjon ("ransomtheft") i tillegg til at dataene blir kryptert. Kilde: DNK [41].	Skipseier er medlem i DNK og har blitt informert om preventive og reaktive tiltak for å sikre seg mot slike hendelser.
A33	2020	P1	Shippingselskapet MSC blir rammet av løsepengevirus og hovedkvarteret i Genève blir satt ut av drift i fem dager. Kilder: Maritime Executive [38], HKMK [54].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.
A34	2020	H3	Israel får skylden for å ha hacket den Iranske havnen Shahid Rajaee, slik at all transport og vareflyt stopper opp og det blir forsinkelser i lang tid. Angrepet skal angivelig ha vært en hevnaksjon etter angrep på et vanndistribusjonssystem i Israel. Kilder: Washington Post [55], HKMK [54].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.

Id	År	Angreps-punkt	Beskrivelse	Tiltak i etterkant
A35	2019 - 2020	P1	Cruise-operatøren Carnival Corporation & plc har blitt rammet to ganger på to år av løsepengevirus, og personlig informasjon og kredittkortopplysninger for passasjerer og ansatte har sannsynligvis kommet på avveie. Det er foreløpig ikke publisert detaljer om type virus og angrepsvektor, men selskapet ser for seg at det kan komme erstatningskrav fra dem som er rammet. Kilde: Maritime Executive [56].	Hendelsene ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.

5 Prioritering av viktigste/alvorligste trusler for maritim næring

Basert på kjente hendelser og tidligere arbeid har vi utarbeidet en "Topp 10"-liste for cybertrusler for maritim næring slik vist i Tabell 8. Selve rangeringen er basert på hendelsesfrekvens, alvorlighet og vurderinger fra tidligere arbeid, og representerer derfor dagens og gårsdagens situasjonsbilde. Øverst på listen finner vi de mest alvorlige.

Vi har valgt å definere truslene på et overordnet nivå, mens vi i tilhørende beskrivelse sier mer om hva som er typiske angrepsvektorer og mål. Enkelte hendelser har blitt knyttet til flere typer trusler. Dette er gjerne naturlig da angrep ofte består av flere faser av forskjellig art og kan ramme flere aktører.

Tabell 8. "Topp 10"-cybertrusler for maritim næring

Prioritering	Navn	Beskrivelse	Vurderingsgrunnlag
1	Angrep på IT/administrative systemer i havner	Havner har vært blant de mest utsatte målene og har hatt et rykte på seg om å være dårlig beskyttet mot cyberangrep. Driftsstans har svært store kostnader og dette gjør havner attraktive for utpressere. Videre kan informasjonstyveri og manipulasjon knyttes til smugling av ulovlig gods. Fra hendelsene ser vi at den vanligste angrepsvektoren er løsepengevirus, som oftest i form av epostvedlegg eller lenker. Som i andre sektorer er det en økende trend for "ransomtheft"-virus, som kombinerer både driftsstans og informasjonstyveri. Ellers ser vi flere hendelsesbeskrivelser som bare omtaler havner som "hacket", og i konfliktområder kan dette tyde på større operasjoner hvor statlige aktører står bak.	Hendelser: A3, A7, A15, A19, A20, A26, A34 Kilder: Jones et al. [7], ENISA [12], NSM [16]
2	Angrep på IT-system hos shipping-selskap	Shipping-selskaper har et tilsvarende trusselbilde som havner, og er utsatt for driftsstans, tyveri av informasjon og forsøk på økonomisk svindel. I hendelsene er det hacking, løsepengevirus og sosial manipulasjon som typisk inngår i angrepsvektorene.	Hendelser: A2, A5, A10, A15, A22, A23, A33, A35. Kilder: NSM [16], Otto [14].
3	Spionasje mot maritime operasjoner	I denne gruppen finner vi hendelser som kjennetegnes av omfattende og målrettede angrep for å gjennomføre spionasje, avlytting og overvåkning av maritime operasjoner. Som angrepsvektorer nevnes typisk spear-phishing eller mer generell hacking.	Hendelser: A4, A7, A8, A13, A18, A21 Kilder: ENISA [12], PST [15], IET [9], Otto [14].

Prioritering	Navn	Beskrivelse	Vurderingsgrunnlag
4	Angrep på IT-systemer hos underleverandører, verft, landanlegg, tjenesteleverandører og forskning.	Denne typen hendelser er mer preget av tyveri av forretningskritisk informasjon, i tillegg til mer tilfeldig utpressing. Fra hendelsene ser vi at sosial manipulasjon, hacking og løsepengevirus er gjengangere i angrepsvektorene.	Hendelser: A14, A18, A21, A27, A28 Kilder: NSM [16]
5	Angrep på IT-/administrative systemer på skip	IT-systemer på skip har også vært mye utsatt for løsepengevirus, men her er det nok mer snakk om tilfeldige angrep. Det er gjerne epostvedlegg og lenker som er angrepsvektor, og skipsservere og klienter har blitt satt ut av spill. Etterforskning av episodene har vært begrenset da data blir slettet.	Hendelser: A29, A30, A31, A32 Kilder: NSM [16], Caprolu et al. [13]
6	Angrep på GNSS	Denne typen trussel er i all hovedsak knyttet til blokkering (jamming) eller manipulering/integritetsbrudd (spoofing) av GPS/GNSS-signaler som skip benytter under navigasjon. Det er typisk statlige aktører som mistenkes i disse hendelsene, og konsekvensene har vært mer forstyrrende enn av kritisk art. Det er grunn til å frykte denne trusselen i geopolitiske konfliktområder.	Hendelser: A12, A16, A17, A25 Kilder: MUNIN [5], CySiMS [8], Vinnem og Utne [11], Caprolu et al. [13], NSM [16]
7	Angrep på OT-systemer på skip/offshore	OT-systemer om bord på skip og offshore-installasjoner er som regel separert fra andre systemer og har derfor vært mindre utsatt. Likevel finnes det eksempler på slike hendelser og konsekvensene har også vært kritiske. Angrepene har typisk kommet inn som malware på USB-enheter eller PC-er som er koblet på feil nett. Utsatte OT-systemer er blant annet ECDIS (ved oppdatering av kartdata) og kontrollsystemer.	Hendelser: A1, A9, A24, A28 Kilder: Jones et al. [7], Vinnem og Utne [11], Caprolu et al. [13], Otto [14].
8	Angrep på kommunikasjonssystem	Det har vært noen få angrep på kommunikasjonssystemene på landbaserte operasjoner og offshore-installasjoner. Skip har ikke vært mye utsatt, men med mange ulike og nødvendige kommunikasjonssystemer om bord, er de fremdeles i faresonen. Angrepene har først og fremst satt kommunikasjonen ut av spill (tap av tilgjengelighet) gjennom generell hacking og løsepengevirus.	Hendelser: A5, A6, A23 Kilder: MUNIN [5], CySiMS [8], Caprolu et al. [13], NSM [16]

Prioritering	Navn	Beskrivelse	Vurderingsgrunnlag
9	Økonomisk svindel	Slike trusler kjennetegnes ved dedikerte angrep, hvor falske eposter eller hackede brukerkontoer benyttes som angrepsvektor for å initiere eller manipulere økonomiske transaksjoner. Angrepene er høyst målrettede og gjøres ved å endre kontoinformasjon eller sende falske fakturaer.	Hendelser: A10, A22 Kilder: IET [9], ENISA [12], Otto [14]
10	Misbruk av AIS og posisjonsdata	Det er registrert flere enkelthendelser hvor et skips AIS-system har blitt manipulert eller deaktivert. Slike teknikker benyttes gjerne i forbindelse med smugling, terrorisme, menneskehandel, illegalt fiske og i militære konflikter. Dette kan også føre til kollisjoner eller at andre skip blir tvunget til å legge om kursen.	Hendelser: A11 (flere) Kilder: Windward [32], Caprolu et al. [13]

Dagens trusselbilde er dessverre ikke fasit på hva som vil være situasjonen i nær og overskuelig framtid. Som i andre næringer som gjennomgår høy grad av digitalisering og teknologisk utvikling, øker eksponeringen mot cyberangrep. Samtidig gjør digitale verdikjeder at man blir mer utsatt for konsekvensene av angrep mot andre. Covid-19 pandemien har for eksempel vist oss at hendelser ett sted i verden, som i utgangspunktet ikke har noen kobling til "cyber" eller maritime interesser, raskt kan få enorme ringvirkninger som vil påvirke alle deler av samfunnet vårt. Både ENISA [57] og INTERPOL [58] har pekt ut endringer i det digitale trusselbildet som følge av pandemien og da spesielt sårbarheter som er oppstått ved økt bruk av hjemmekontor. I maritim sektor anslås det at antall cyberangrepsforsøk har økt med 400% fra februar til juni i 2020 [59]. Eksempler er blant annet sosial manipulasjon gjennom ondsinnet epost, hvor emnefelt inneholder tekst som “Maersk New Shipping schedule details due to COVID-19-Shipment notification” og "COVID-19 SUSPECTED CREW /VESSEL" [60]. Det er et kjent fenomen at personer under stress tenderer til å glemme den sikkerhetshygienen man har under normale forhold. I tillegg har det blitt vanskeligere for vedlikeholdspersonell å fysisk kunne reise dit skipene ligger. Dette har ført til at sperrer for fjerntilgang har blitt åpnet opp slik at de har kunnet gjøre nødvendige oppgraderinger og dermed gjort systemene mer utsatte for angrep.

6 Referanser

[1] *Information technology — Security techniques — Information security risk management*, ISO/IEC, 2018. [Online]. Available: https://www.iso.org/standard/75281.html

[2] M. D. Greenberg, P. Chalk, H. H. Willis, I. Khilko, and D. S. Ortiz, *Maritime terrorism: Risk and liability*. Rand Corporation, 2006.

[3] A. C. Winner, P. Schneider, and A. T. Weldemichael, "Maritime terrorism and piracy in the Indian Ocean Region," ed: Taylor & Francis, 2012.

[4] D. Cimpean, J. Meire, V. Bouckaert, S. Vande Casteele, A. Pelle, and L. Hellebooge, "Analysis of cyber security aspects in the maritime sector," 2011.

[5] L. Kretschmann, Ø. J. Rødseth, Å. Tjora, B. S. Fuller, H. Noble, and J. Horahan, "D9.2. Qualitative assessment," Maritime Unmanned Navigation through Intelligence in Networks (MUNIN), 2015-09-30 2015.

[6] P. B. Kristoffersen, T. Hartvigsen, P. Myrvang, and A. Torjusen, "Digitale Sårbarheter Maritim Sektor," in "Lysneutvalget," DNV-GL, 2015-0569, Rev. 1, 2O15-1O-21 2015.

[7] K. D. Jones, K. Tam, and M. Papadaki, "Threats and impacts in maritime cyber security," *Engineering & Technology Reference* 2016.

[8] D. A. Nesheim, Ø. J. Rødseth, K. Bernsmed, C. Frøystad, and P. H. Meland, "D1.1 Risk Model and Analysis," CySiMS, 2017-04-07 2017.

[9] *Code of Practice: Cyber Security for Ships*, IET Standard H. Boyes and R. Isbell, Department for Transport (UK), 2017.

[10] BIMCO, "THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, version 3," BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, WORLD SHIPPING COUNCIL, 2018. [Online]. Available: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

[11] J. E. Vinnem and I. B. Utne, "Risk from cyberattacks on autonomous ships," *Safety and Reliability-Safe Societies in a Changing World*, 2018.

[12] A. Drougkas, A. Sarri, P. Kyranoudi, and A. Zisi, "Port cybersecurity-good practices for cybersecurity in the maritime sector, November 2019," ed, 2020.

[13] M. Caprolu, R. Di Pietro, S. Raponi, S. Sciancalepore, and P. Tedeschi, "Vessels Cybersecurity: Issues, Challenges, and the Road Ahead," *arXiv preprint arXiv:2003.01991*, 2020.

[14] L. Otto, *Global Challenges in Maritime Security - An Introduction*. Springer, 2020.

[15] PST, "Nasjonal trusselvurdering 2020," PST, 4 Feb 2020. [Online]. Available: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

[16] NSM, "RISIKO 2020," 2020. [Online]. Available: https://nsm.no/aktuelt/risiko-2020

[17] NSM, "Helhetlig digitalt risikobilde 2019," 2019. [Online]. Available: https://nsm.no/getfile.php/133669-1592830841/Demo/Dokumenter/Rapporter/2019---nsm-helhetlig-digitalt-risikobilde.pdf

[18] P. Kapalidis, "Cybersecurity at Sea," in *Global Challenges in Maritime Security*, L. Otto Ed.: Springer, 2020.

[19] KNect365, "Shipping 2030 - Collaboration in the Shipping Industry: Innovation and Technology," KNect365, 2018.

[20] H. Singh, "Cybe f Oslo, 2019.

[21] CyberKeel, "Ma . Available: https://maritimec

[22] UTNews, "UT A Sea," in *UT News*, ed, 2013.

[23] Z. Shauk, "Malw Houston Chronicle*,* ed, 2013.

[24] J. Walker and J. Spencer, Marine Claims Conference. Cyber Marine: Risks & Loss Scenarios. Available: http://www.marineclaimsconference.com/imcc-docs/docs/Cyber%20workshop.pdf.
[25] GReAT. "The Icefog APT: A Tale of Cloak and Three Daggers." Kaspersky. https://securelist.com/the-icefog-apt-a-tale-of-cloak-and-three-daggers/57331/ (accessed 10 Aug, 2020).
[26] Y. Torbati and J. Saul. "Iran's top cargo shipping line says sanctions damage mounting." https://www.reuters.com/article/us-iran-sanctions-shipping/irans-top-cargo-shipping-line-says-sanctions-damage-mounting-idUSBRE89L10X20121022 (accessed 10 Aug, 2020).
[27] B. Gertz. "Iran Rapidly Building Cyber Warfare Capabilities." https://freebeacon.com/national-security/iran-rapidly-building-cyber-warfare-capabilities/ (accessed 10 Aug, 2020).
[28] T. Kristiansen, "DR: Kina hackede sig ind i Søfartsstyrelsen," ed. Shippingwatch, 2014.
[29] AthensGroup. "Cybersecurity - There is no silver bullet." https://athensgroup.com/cybersecurity-there-is-no-silver-bullet/ (accessed 11 Aug, 2020).
[30] J. Knox. "Coast Guard Commandant on Cyber in the maritime domain." https://mariners.coastguard.dodlive.mil/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain/ (accessed 11 Aug, 2020).
[31] H. A. Schwartz and C. Diamond. "The U.S. Coast Guard Cyber Strategy." https://www.csis.org/events/us-coast-guard-cyber-strategy (accessed 11 Aug, 2020).
[32] Windward, "AIS Data on the High Seas: An Analysis of the Magnitude and Implications of Growing Data Manipulation at Sea," 2014. [Online]. Available: https://www.arbitrage-maritime.org/fr/Gazette/G36complement/Windward.pdf
[33] S. Schnelle, "Kartlegging av maritime hybride trusler - Kan bruk av stordata og sosial nettverksanalyse bidra til økt maritim situasjonsbevissthet?," Forsvarets Høgskole, 2018. [Online]. Available: https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2583966/2018%20Masteroppgave%20Schnelle%20Stian.pdf?sequence=1
[34] T. Wallace and F. Mesko, *The Odessa Network: Mapping Facilitators of Russian and Ukrainian Arms Transfers*. C4ADS, 2013.
[35] ASCStaff. "Cyberattack on Clarkson's shipbroker reaffirms industry's vulnerability." https://www.logisticsmiddleeast.com/article-13696-cyberattack-on-clarkson%E2%80%99s-shipbroker-reaffirms-industry%E2%80%99s-vulnerability (accessed 11 Aug, 2020).
[36] C. Cimpanu. "Shipping Firm Avoids Customer Data Dump in Last Year's Hack & Ransom Incident." https://www.bleepingcomputer.com/news/security/shipping-firm-avoids-customer-data-dump-in-last-years-hack-and-ransom-incident/ (accessed 11 Aug, 2020).
[37] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," in *WIRED*, ed, 2018.
[38] MaritimeExecutive. "Naval Dome: Cyberattacks on OT Systems on the Rise." https://www.maritime-executive.com/article/naval-dome-cyberattacks-on-ot-systems-on-the-rise (accessed 10 Aug, 2020).
[39] C. Cimpanu, "Ransomware Infection Cripples Shipping Giant COSCO's American Network," vol. 2020, ed. Bleeping Computer, 2018.
[40] J. Novet, "Shipping company Maersk says June cyberattack could cost it up to $300 million," in *CNBC*, ed, 2017.
[41] L. B. Vold, "Hendelser registrert mot DNK forsikrede fartøy," ed, 2020.
[42] G. Lubold and D. Volz, "Chinese Hackers Breach U.S. Navy Contractors," in *The Wall Street Journal*, ed, 2018.
[43] D. Volz, "Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets," in *The Wall Street Journal*, ed, 2019.
[44] SAFETY4SEA. "2018 Highlights: Major cyber attacks reported in maritime industry." https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/ (accessed 10 Aug, 2020).

[45] C. Cimpanu, "US Coast Guard discloses Ryuk ransomware infection at maritime facility," in *ZDNet*, ed, 2019.
[46] Z. Reynolds. "Australian defence shipbuilder Austral victim of Iranian cyber attack." https://safetyatsea.net/news/news-safety/2018/australian-defence-shipbuilder-austral-victim-of-iranian-cyber-attack/ (accessed 19 Nov, 2020).
[47] Secureworks. "GOLD GALLEON: How a Nigerian Cyber Crew Plunders the Shipping Industry." https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry (accessed 11 Aug, 2020).
[48] W. Hannemann, "Key takeaways from 3 recent cyber attacks in shipping," vol. 2020, ed. Dualog, 2019.
[49] R. Lemos. "Coast Guard Warns Shipping Firms of Maritime Cyberattacks." https://www.darkreading.com/vulnerabilities---threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks/d/d-id/1335198 (accessed 10 Aug, 2020).
[50] C. Kråkenes, "Norwegian Armed Forces creating GPS jamming alert system," in *NRK*, ed, 2020.
[51] N. Goud. "Cyber Attack on James Fisher and Sons." https://www.cybersecurity-insiders.com/cyber-attack-on-james-fisher-and-sons/ (accessed 14 Aug, 2020).
[52] C. Buurma and A. Sebenius, "Ransomware Shuts U.S. Natural Gas Compressor Facility for Two Days," in *Carrier Management*, ed, 2020.
[53] Dragos. "Assessment of Ransomware Event at U.S. Pipeline Operator." https://www.dragos.com/blog/industry-news/assessment-of-ransomware-event-at-u-s-pipeline-operator/ (accessed 14 Aug, 2020).
[54] M. Grinter. "Maritime cyber-attacks up 900% in three years." http://www.hongkongmaritimehub.com/maritime-cyber-attacks-up-900-in-three-years/ (accessed 10 Aug, 2020).
[55] J. Warrick and E. Nakashima, "Officials: Israel linked to a disruptive cyberattack on Iranian port facility," in *Washington Post*, ed, 2020.
[56] MaritimeExecutive, "Carnival Corporation Reports Ransomware Attack Accessed Data," in *Maritime Executirve*, ed, 2020.
[57] ENISA. "COVID19." https://www.enisa.europa.eu/topics/wfh-covid19 (accessed 17 Aug, 2020).
[58] INTERPOL, "Cybercrime: COVIC-19 IMPACT," INTERPOL, 2020. [Online]. Available: https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf
[59] M. Grinter. "Shipping subjected to 400% increase in attempted hacks." http://www.hongkongmaritimehub.com/shipping-subjected-to-400-increase-in-attempted-hacks/ (accessed 18 Aug, 2020).
[60] DryadGlobal. "Vessel Impersonation Report." https://dryadglobal.com/maritime-cyber-security-threats-2-2/ (accessed 10 Aug, 2020).