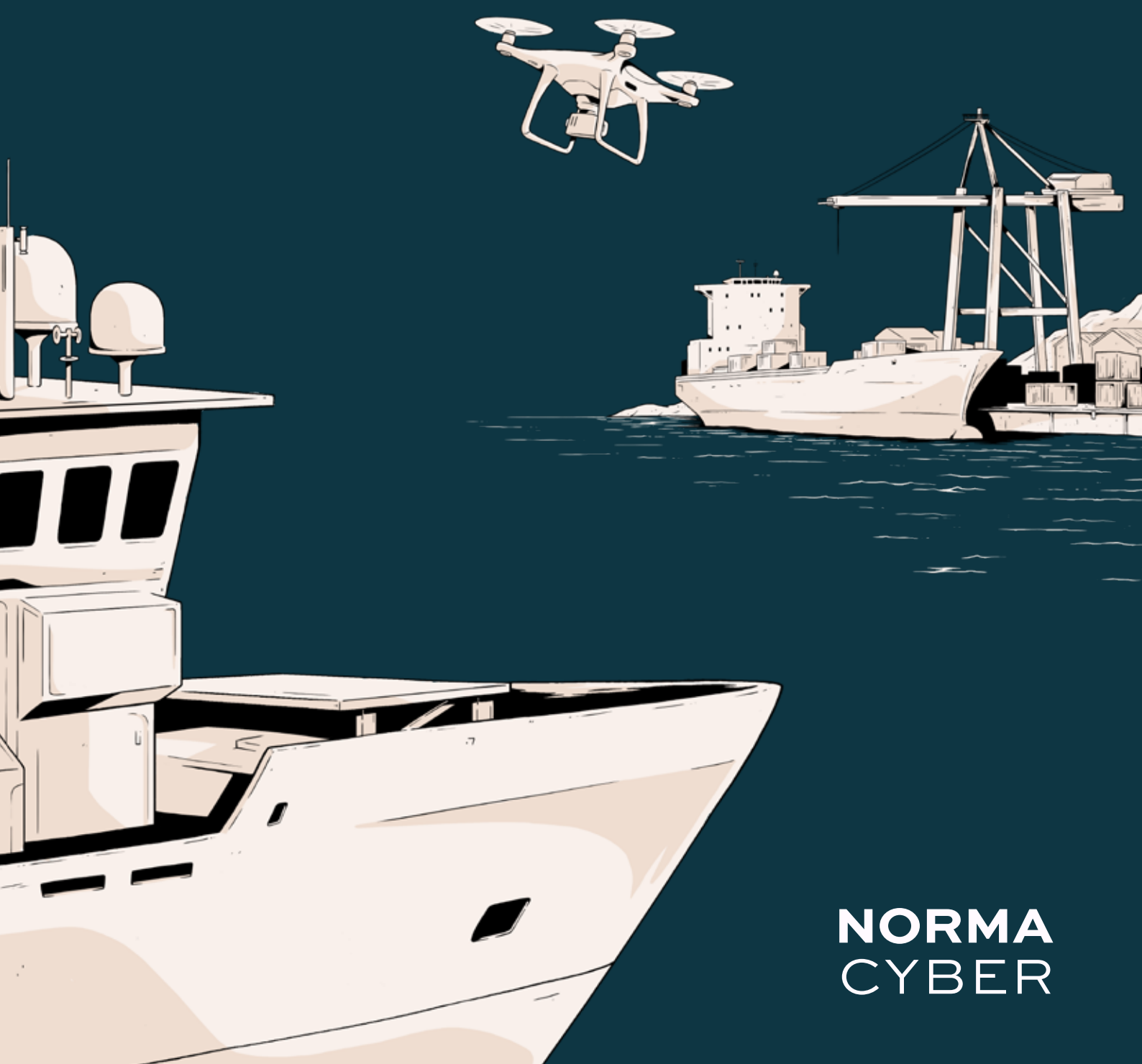
The Nordic Maritime Cyber Resilience Centre

Årlig trussel-vurdering 2026

normacyber.no



NORMA CYBER

Nordic Maritime Cyber Resilience Centre, NORMA Cyber, er ledende innen operativ cybersikkerhet i den nordiske maritime næringen. Senteret har vært i drift siden 2021 og ble etablert som et felles samarbeid mellom Den Norske Krigsforsikring for Skib (DNK) og Norges Rederiforbund (NR). Senteret fokuserte opprinnelig på den norske maritime næringen, men ekspanderte til å favne hele den nordiske næringen våren 2024.

NORMA Cyber opererer som en non-profit, og medlemmene er virksomheter innen den maritime sektoren i Norden. Senteret tilbyr også affilierte- og leverandørmedlemskap til internasjonale virksomheter og maritime leverandører.

NORMA Cyber har for øyeblikket over 170 medlemmer som representerer mer enn 3 000 skip og offshore-enheter.

Senteret leverer en sentralisert cybersikkerhetsfunksjon så medlemmene kan samle ressursene, og være mer effektive og motstandsdyktige enn om selskapene skulle etablere lignende ressurser hver for seg. NORMA Cyber bruker derfor betydelig tid og ressurser på å utvikle nye løsninger som drar nytte av ny teknologi og sikrer effektiv og kostnadseffektiv cybersikkerhet for våre medlemmer.

Tjenestene inkluderer trusseletterretning, en tjeneste for tidsriktig informasjonsdeling blant medlemmer, hendelses- og krisehåndtering samt flere lignende tjenester.

Siden 2024 har NORMA Cyber vært den operative enheten for sektorvis responsmiljø (SRM) i den norske maritime sektoren, ledet av Kystverket.

Våre eksperter jobber tett sammen med sikkerhets- og beredskapsavdelingene i DNK og NR. I Oslo har våre tre organisasjoner etablert Norwegian Shipping Security and Resilience Centre. Dette er et felles senter for å støtte våre medlemmer når komplekse operasjoner inntreffer, hvor både fysiske og digitale trusler er involvert.

Kontaktdetaljer:
contact@normacyber.no
Telefon: **22 22 00 50**

Nødnummer: **+47 90 98 97 37**

Innholdsfortegnelse

Kjære leser,
Velkommen til den nyeste utgaven av NORMA Cybers årlige trusselvurdering.

Maritime næring opererer i et stadig mer usikkert globalt landskap. Økte spenninger mellom stormakter og pågående regionale konflikter har blitt normalen. Næringens avhengighet av komplekse forsyningskjeder øker eksponeringen mot disse geopolitiske utviklingene.

Digitaliseringen i den maritime næringen fortsetter å skyte fart. Fullt tilkoblede fartøy er nå standard, med økt integrasjon mellom havner, terminaler og logistikksystemer. Operasjonell teknologi knyttes tettere til IT og eksterne nettverk. Dette gir effektivisering, men introduserer også nye sårbarheter og øker den potensielle konsekvensen av cyberhendelser.

I perioder med økt usikkerhet bekrefter våre medlemmer at NORMA Cybers rolle som et ideelt, medlemsfokusert senter med tett myndighetssamarbeid, er viktigere enn noen gang. Dette gjenspeiles i et rekordhøyt antall nye medlemmer det siste året.

Det er også positivt å se økt bevissthet og engasjement for cybersikkerhet på toppledernivå. Nye klassekrav og utviklingen av regelverk som EUs NIS2-direktiv, bidrar til dette. Samtidig kan disse endringene være krevende å navigere for maritime aktører.

NORMA Cyber samarbeider tett med medlemmer, myndigheter og partnere for å legge til rette for rettidig informasjonsdeling og kontinuerlig overvåking av cybertrusselbildet. Gjennom dette arbeidet har vi opparbeidet en unik tilgang til data som gjør oss i stand til å identifisere de mest betydningsfulle trendene som påvirker den maritime sektoren. Denne rapporten presenterer våre viktigste funn og vurderinger av det nåværende og fremvoksende cybertrusselbildet.

Vi håper denne trusselvurderingen gir verdifull innsikt for beslutningstakere og styrker situasjonsforståelsen. Selv om digitale trusler ikke kan elimineres fullstendig, er vi dedikerte til å støtte våre medlemmer i arbeidet med å redusere risiko og opprettholde trygge og effektive operasjoner.

Vi håper også at vurderingen bidrar til videre diskusjon, dialog og informasjonsdeling. Sammen kan vi fortsette å styrke den digitale motstandskraften i den maritime sektoren i året som kommer.

God lesning.

Lars Benjamin Vold
Daglig leder

Nordic Maritime Cyber Resilience Centre

Daglig leder Lars Benjamin Vold
Nordic Maritime Cyber Resilience Centre

Sammendrag

Maritim sektor står fortsatt sentralt i både global handel og geopolitisk spenning. I dette landskapet er cyberspionasje den mest betydelige strategiske bekymringen. Det er en høy trussel om cyberspionasjeoperasjoner mot maritim sektor i 2026, ettersom stater prioriterer etterretningsinnhenting for å støtte militær beredskap og økonomisk sikkerhet. Stater som Russland, Kina og Iran vil meget sannsynlig fortsette å rette seg mot maritime virksomheter for å innhente etterretning om sanksjonshåndheving, militær mobilitet, energistrømmer og operasjoner i Arktis. De kombinerer ofte cyberinntrenging med fysisk overvåking for å bygge situasjonsforståelse og etablere digital tilgang for mulig fremtidig påvirkning.

Maritime virksomheter i Norden vil også sannsynlig bli trukket inn i informasjonsoperasjoner knyttet til geopolitisk spenning. Hacktivister og statstilknyttede aktører forsterker narrativer gjennom påstander om cyberaktivitet og kombinerer ofte propaganda med forstyrrende angrep fremfor å søke dyp teknisk effekt. Forstyrrende operasjoner vil i hovedsak drives av politisk motiverte hacktivistkollektiver, der DDoS-angrep fortsatt vil dominere.

Angrep mot operasjonell teknologi øker i omfang og bidrar til et stadig mer komplekst trusselbilde. Den generelle trusselen mot operasjonell teknologi er lav, men internetteksponerte enheter står overfor en moderat trussel for manipulering. Samtidig blir GNSS-forstyrrelser mer sofistikerte, påvirker i økende grad flere satellittkonstellasjoner og medfører reelle navigasjons- og kommersielle konsekvenser. Trusselen om destruktive cyber operasjoner mot maritim sektor er lav for det meste av den kommersielle flåten. Selv om statlige aktører som Russland og Kina har kapasitet til å gjennomføre destruktive angrep, foretrekker de per i dag hybride tilnærminger som kombinerer cyberspionasje med fysisk sabotasje for å unngå direkte attribusjon.

Trusselen fra økonomisk motiverte kriminelle mot nordisk maritim sektor er høy. Identitetsbasert tilgang og phishing vil sannsynlig være de dominerende metodene for å kompromittere virksomheter, og angripere rammer i stor grad vilkårlig. Maritime virksomheter vil sannsynlig fortsatt møte trusler fra løsepengevirus, datatyveri og skadevare etter hvert som det kriminelle økosystemet fortsetter å industrialiseres.

Nøkkeltall fra 2025

77

bekreftede kompromitterte kontoer og enheter er rapportert til maritime virksomheter av NORMA Cyber

60

ganger har NORMA Cyber registrert at ransomwaregrupper har navngitt maritime organisasjoner

8

påståtte angrep mot OT i maritim sektor utført av hacktivistgrupper

350+

hendelser ble håndtert av SOC på vegne av SOC medlemmene

Sammanfattning

Geopolitisk bakteppe

Det globale sikkerhetsbildet fremstår både stabilt og uforutsigbart. De sikkerhetspolitiske fremtidsutsiktene er alvorlige, den geopolitiske situasjonen er spent, og nye konflikter oppstår samtidig som andre går inn i nye faser. I sentrum av dette landskapet finner man i økende grad maritim sektor. Det maritime domenet har blitt en sentral arena for geopolitisk rivalisering knyttet til handel, transport og energiforsyning.

Maritime aktører påvirkes både direkte og indirekte. Direkte gjennom fysiske og digitale angrep i sine operasjonsområder, og indirekte ved at sektoren har blitt et stadig mer attraktivt mål for spionasje, kartlegging og innsideaktivitet. Dette stiller høyere krav til sektorens egen evne til å beskytte verdier, situasjonsforståelse og håndtering av risiko.

Samspillet og rivaliseringen mellom USA, Kina og Russland er i kontinuerlig endring og har direkte innvirkning på verdensøkonomien. Dette kompliserer risikobildet for maritime aktører. Samtidig vurderer norske sikkerhetsmyndigheter trusselen fra Russland, Kina og Iran mot både offentlige og private norske virksomheter som vedvarende høy. Denne vurderingen gjenspeiles i trusselbildet rettet mot maritim sektor.

Skillet mellom væpnet konflikt på land eller til sjøs og angrep mot global maritim handel blir stadig mer utydelig. Det har vært gjentatte fysiske og digitale angrep mot sivil skipsfart. Parallelt har andelen av den globale flåten som opererer i skyggeflåten økt betydelig. Dette visker ut grensen mellom legitim og illegitim skipsfart og forsterker at sivile fartøy i økende grad betraktes som legitime mål. Samtidig øker oppmerksomheten mot kritisk maritim infrastruktur på land, til sjøs og på havbunnen, særlig i nordiske områder.

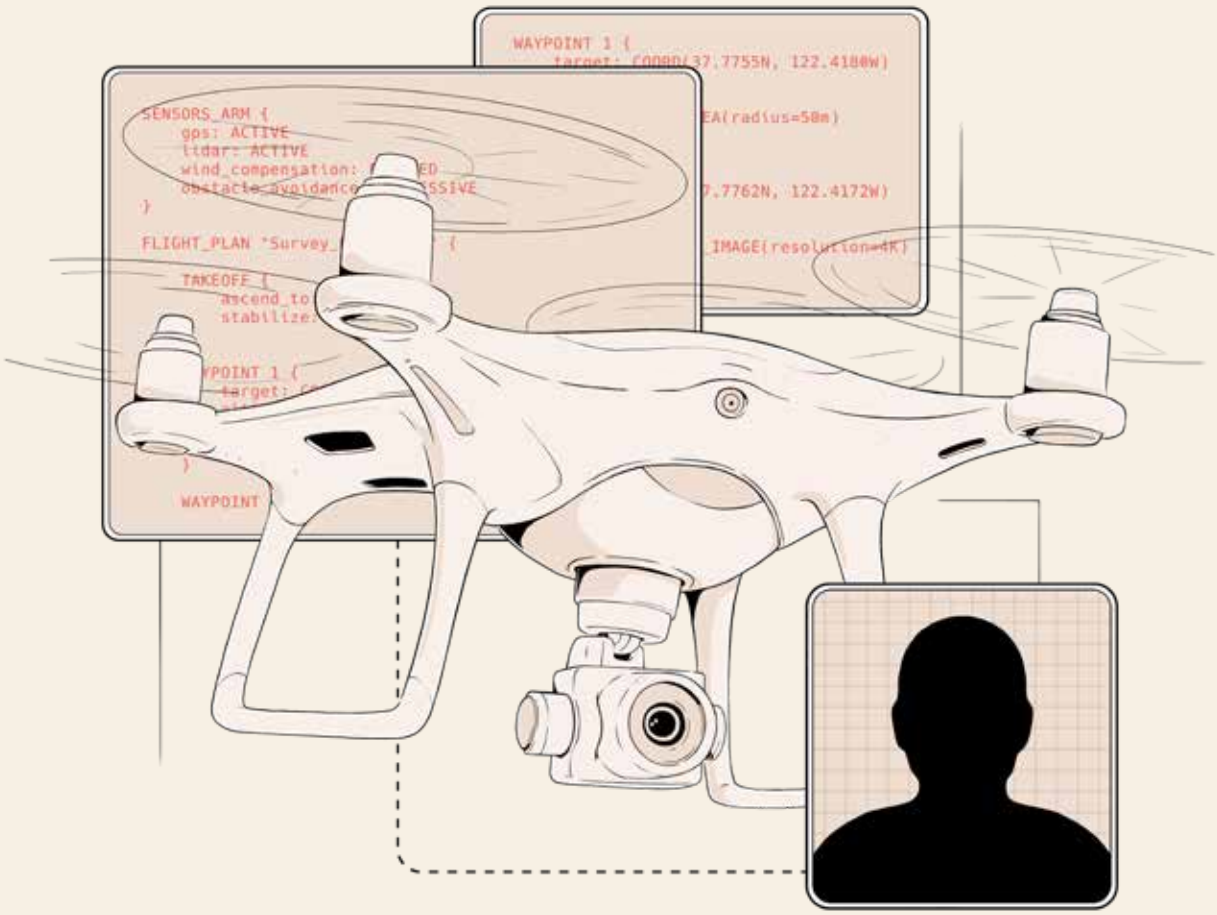
Bruken av droner fra eller mot fartøy øker også og inngår i et bredere sett av hybride virkemidler. Utviklingen viser at hybride midler ikke lenger er unntaket, men har blitt en standard del av verktøykassen til både statlige og ikke-statlige aktører i konfliktmiljøer.

Våpenhvilen mellom Israel og Hamas forblir skjør. I Rødehavet er det registrert færre angrep mot skipsfart ved inngangen til 2026, men houthiene sier fortsatt at tonnasje med israelsk tilknytning er legitime mål.

Russlands krig mot Ukraina går inn i sitt fjerde år, uten tegn til grunnleggende endringer til tross for gjentatte forsøk på å forhandle frem en fredsløsning. Spenningene i Svartehavet forblir vedvarende høye. Selv om det har vært få kinetiske angrep mot skipsfart utover bruken av sjøminer, er GNSS-interferensen omfattende. Dette bidrar til at skipstrafikken i området fortsatt ligger betydelig under normale nivåer.

Sør-Kinahavet har lenge vært et geopolitisk brennpunkt. Den digitale dimensjonen er en integrert del av rivaliseringen mellom stormakter og regionale aktører. Cyberoperasjoner rettet mot den maritime sektoren kan brukes som pressmiddel i territorielle konflikter og inngå i en bredere kamp om innflytelse i regionen, der cyberkapasiteter muliggjør påvirkning uten å utløse direkte militær konfrontasjon.

> Maritim sektor har blitt en hovedarena for geopolitisk konkurranse om handel, transport og energitilgang



I Østersjøen har cyberrelaterte navigasjonsforstyrrelser blitt en vedvarende utfordring. Rapportert GNSS-interferens har til tider ført til at fartøy har mistet eller mottatt feil posisjonsdata. Hendelsene skjer i en region preget av økte sikkerhetsspenninger, der rapporter om sabotasje mot kritisk infrastruktur, transitt av skyggeflåtefartøy og bruk av hybride virkemidler bidrar til et komplekst trusselbilde. Digital interferens mot maritime systemer må derfor ses som en integrert del av et bredere trussellandskap i Nord-Europa.

Disse utviklingstrekkene har ført til at europeiske myndigheter har innført tiltak for å styrke sikkerheten i maritime områder og senke terskelen for inspeksjon av fartøy. Samtidig er det ofte vanskelig å fastslå intensjonen bak hendelser eller mistenkelige bevegelser. Dette kan føre til økt mistanke mot fartøy som driver legitim handel, hyppigere inspeksjoner og tilbakeholdelser, og samlet sett bidra til en uthuling av de internasjonale reglene og normene som global skipsfart er avhengig av – regler som over lang tid har kommet både næringen og verdensøkonomien til gode.

Presset mot internasjonale regler og normer begrenser seg ikke til skipsfarten. Den økende uforutsigbarheten i det globale miljøet drives også av økende utfordringer mot den regelbaserte internasjonale orden. Multilaterale institusjoner mister innflytelse og legitimitet, mens parallelle allianser og avtaler i økende grad etableres utenfor etablerte rammeverk. For en global og grensekryssende næring som skipsfarten representerer dette et særlig krevende operasjonsmiljø.

Spionasje

Maritime virksomheter står overfor en høy trussel om cyberspionasje i 2026 ettersom stater prioriterer etterretningsinnhenting for å støtte militær beredskap, økonomisk sikkerhet og geopolitisk påvirkningskraft. Sjøtransport, havner og energilogistikk er grunnleggende for nasjonal sikkerhet og global handel, noe som gjør virksomheter som forvalter sensitiv operasjonell informasjon til attraktive etterretningsmål.

Russlands krigsdrevne etterretningsbehov, Kinas strategiske maritime posisjonering, økende energisamarbeid i Arktis og vedvarende spenninger i Midtøsten vil meget sannsynlig opprettholde langsiktige innhentingskampanjer.

Sammenfallet mellom cyberinntrenging, fysisk overvåking, sanksjonsomgåelse og utvikling av arktisk energi øker etterretningsverdien av maritime nettverk. Maritime virksomheter involvert i arktiske operasjoner, LNG-transport, NATO-relatert logistikk og energistrømmer i Midtøsten vil forbli særlig attraktive etterretningsmål.

Russland: Krig, sanksjoner og energiomlegging

Spionasjetrusselen fra Russland mot maritime virksomheter er høy, særlig i Europa og i nordområdene. Russlands krig mot Ukraina vil meget sannsynlig fortsatt drive etterretningsbehov i 2026. Russland-tilknyttede trusselaktører vil sannsynlig søke innsikt i militær mobilitet, sanksjonshåndheving, energieksport og varestrømmer som kan undergrave russiske strategiske mål.

Maritime virksomheter som støtter NATO-logistikk, energiinfrastruktur, arktiske operasjoner eller aktiviteter som involverer maritim teknologi med dobbelt anvendelsesområde, er sannsynlige etterretningsmål. Russland-tilknyttede aktører vil også sannsynlig innhente etterretning om avanserte maritime kapasiteter, inkludert sensorer, navigasjonssystemer, robotikk, autonomi og undervannsteknologi. Russland-tilknyttede trusselaktører vil også meget sannsynlig gjennomføre cyberoperasjoner for å legge til rette for fremtidig sabotasje, forstyrrende eller destruktive operasjoner.

Slik aktivitet vil sannsynlig omfatte kartlegging av sårbarheter i kritisk undervannsinfrastruktur, havner og terminaler, samt forhåndsetablering av tilgang til infrastrukturen.

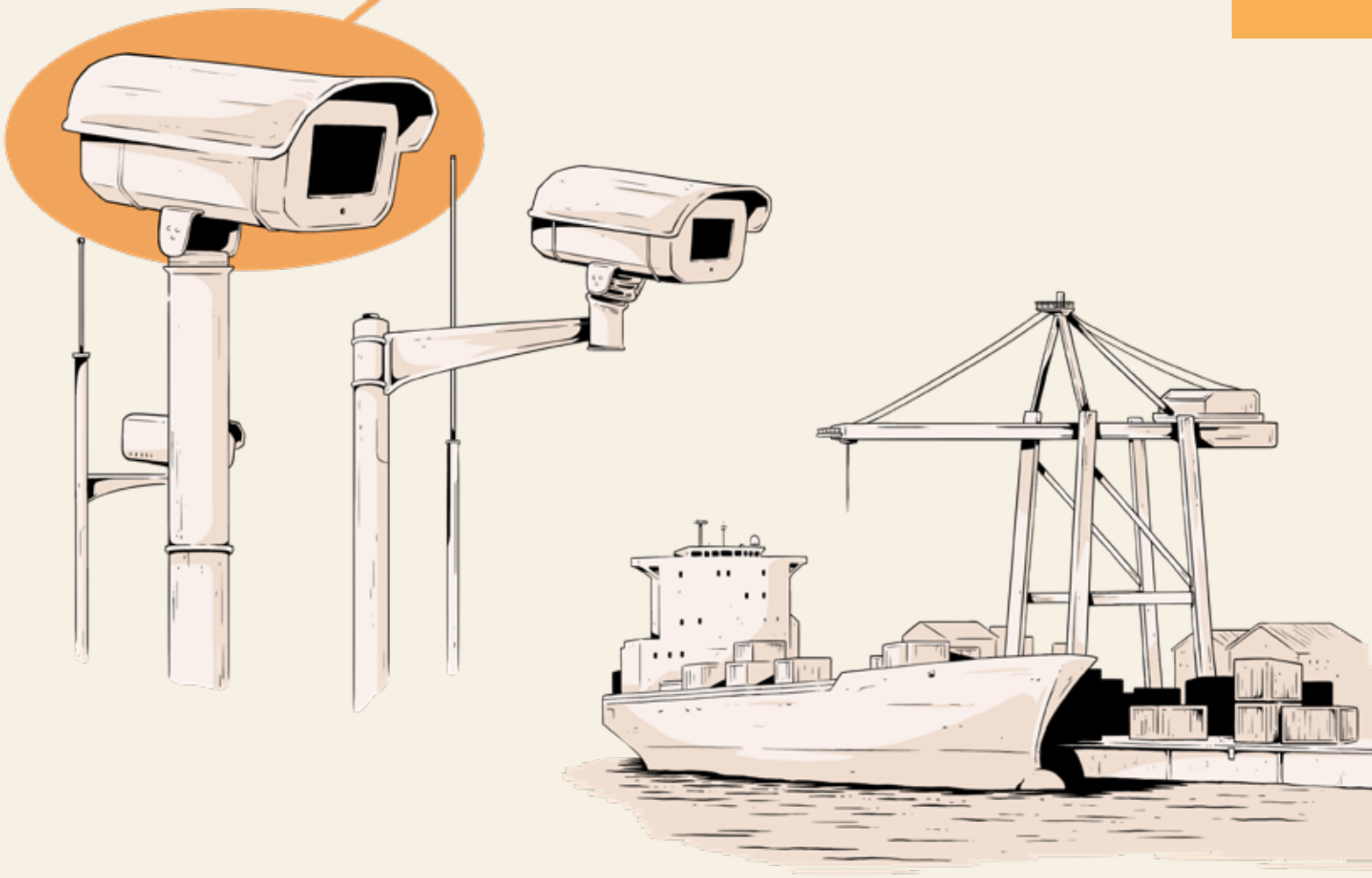
Kina: Strategisk maritim og arktisk posisjonering

Trusselaktører tilknyttet Kina vil sannsynlig fortsette langsiktig etterretningsinnhenting i tråd med Beijings geopolitiske prioriteringer i Indo-Stillehavsregionen, Europa og Arktis. Den primære etterretningstrusselen fra Kina-tilknyttede grupper ligger i cyberdomenet.

Sør-Kinahavet forblir en sentral arena for Kina-tilknyttet cyberspionasje. Trusselaktører vil sannsynlig integrere cyberoperasjoner med fysisk overvåking for å opprettholde situasjonsforståelse i omstridte farvann. Disse operasjonene vil sannsynlig ha et todelt formål: å innhente umiddelbar politisk og militær etterretning, samtidig som de etablerer tilgang i kritisk infrastruktur for mulig fremtidig påvirkning. Kina-tilknyttede trusselaktører vil meget sannsynlig fortsette å bruke USB-enheter som initial angrepsvektor, med kapasitet til å krysse luftgap i maritime systemer. Regimetilknyttede aktører fortsetter å rette seg mot skipsfartsnæringen ved å bruke infiserte USB-enheter for å oppnå første tilgang. I midten av 2025 introduserte Kina-tilknyttede aktører geografisk avgrensning i skadevaren, slik at den kun kjører på maskiner innenfor et spesifikt målland. Dette tillegget er sannsynlig ment å begrense infeksjoner og redusere støy som kan svekke aktørenes operasjonelle sikkerhet.

Iran: Skjæringspunktet mellom maritim sektor og energi

Spionasjetrusselen fra Iran mot nordiske maritime virksomheter er moderat. Maritime virksomheter som opererer i Midtøsten eller har tilknytning til Israel eller USA, står imidlertid overfor en høy trussel.



Iran-tilknyttede aktører vil sannsynlig fortsette systematisk rekognosering og innsamling av legitimasjon rettet mot rederier, bemanningsselskaper, havneoperatører og energilogistikkaktører. Etterretningens prioriteringer vil meget sannsynlig omfatte maritime logistikknettverk som støtter energieksport og trafikk gjennom strategiske flaskehalser som Hormuzstredet og Suezkanalen.

En datalekkasje i 2025, tilskrevet en trusselaktør knyttet til Irans revolusjonsgarde, beskrev vedvarende forsøk på å kompromittere bemannings- og charteravdelinger i Europa og Midtøsten. Lekkasjonen vurderes som autentisk og indikerer systematisk kartlegging av globale maritime og energirelaterte nettverk. Iran vil sannsynlig bruke cyberspionasje for å styrke kriseberedskap og muliggjøre potensiell forstyrrelse i perioder med regional eskalering.

Overvåking av transportknutepunkter

Statlige trusselaktører vil meget sannsynlig fortsette å kombinere cyberinntrenging med fysisk overvåking for å styrke maritim situasjonsforståelse. Transportknutepunkter, inkludert havner, LNG-terminaler, grensesnitt mellom jernbane og sjøtransport samt tilstøtende logistikkknutepunkter, er etterretningsmål med høy verdi på grunn av deres rolle i militær mobilitet, sanksjonshåndheving og energieksport.

Russland-tilknyttede trusselaktører har vist evne til å kompromittere internett-tilkoblede kameraer og andre kant-enheter plassert nær transportinfrastruktur. Slik tilgang kan muliggjøre vedvarende overvåking av fartøysankomster, lastehåndtering og bevegelsesmønstre. Denne typen innhenting vil sannsynlig støtte både sanntids etterretningsbehov og beredskapsplanlegging. Iran vil sannsynlig bruke cyberspionasje for å innhente informasjon om maritime logistikknettverk og infrastruktur som støtter energieksport, for å styrke strategisk situasjonsforståelse og muliggjøre potensiell forstyrrelse under regionale kriser. Iran vil sannsynlig bruke cyberoperasjoner til å samle informasjon om fartøy og bevegelser, særlig i strategiske flaskehalser som Suezkanalen og Hormuzstredet, for direkte å støtte fremtidige militære operasjoner.

Samtidig vil Kina-tilknyttede aktører sannsynlig fortsette å utnytte relénettverk for å gjennomføre storskala innhenting av maritim informasjon i åpne kilder. Rapportering viser bruk av slike nettverk for anonymt å hente data fra amatørbaserte maritime sporingssystemer og programvaredefinerte radioer. Ved å aggregere offentlige data fra tusenvis av noder kan aktørene bygge et detaljert bilde av marine bevegelser og logistikkjeder. Statlige trusselaktører vil sannsynlig fortsette å rette seg mot et bredt spekter av enheter og plattformer innenfor sine strategiske interesseområder, enten for å utlede etterretning eller etablere vedvarende tilgang som støtte for nettverksoperasjoner.

India-tilknyttede trusselaktører vil sannsynlig fortsette å rette seg mot havner og maritime virksomheter i Indiahavsregionen ved bruk av maritimt tematisert phishing og innsamling av legitimasjon. Operasjonene fokuserer primært på regional situasjonsforståelse og forsvarsrelatert etterretning.

Spenninger på Koreahalvøya vil meget sannsynlig fortsette å drive Nord-Korea-tilknyttet etterretningsinnhenting.

Nordkoreanske aktører vil sannsynlig rette seg mot maritim transport og logistikkaktører for å innhente sanksjonsrelevant økonomisk etterretning og innsikt med potensiell militær verdi.

Agentenes tidsalder

Metodene innen cyberspionasje vil sannsynlig fortsette å utvikle seg i 2026 etter hvert som automatiserte cyberoperasjoner drevet av KI og agentbaserte systemer tas i bruk. Statlige aktører beveger seg utover enkle automatiseringsskript og begynner å deployere KI-støttede verktøy som kan utføre komplekse inntrengingsoppgaver med mindre menneskelig oppfølging.

Generelt indikerer rapportering en økning i statlig aktivitet som utnytter KI. Denne aktiviteten er ikke begrenset til forberedelser av cyberoperasjoner, men støtter i økende grad også agentbaserte operasjoner. Fra 2025 har man sett en utvikling fra bruk av KI til å generere kommandoer for kartlegging og dataeksfiltrering, til kampanjer som mer autonomt kan gjennomføre rekognosering, lateral bevegelse og dataeksfiltrering, med et menneske i loopen. Innføringen av agentisk KI i etterretningsarbeidsflyter vil meget sannsynlig gjøre kampanjer i 2026 større, raskere og mer komplekse.

Russland-tilknyttet trusselaktør retter seg mot IP-kameraer

Russland-tilknyttet cyberspionasje mot europeisk maritim og transportinfrastruktur økte i 2025. Fancy Bear gjennomførte storskala utnyttelse av internett-tilkoblede IP-kameraer i nærheten av havner, grenseoverganger, jernbaneknutepunkter og logistikkknutepunkter. Kampanjen inngår sannsynlig i en bredere etterretningsinnsats som støtter russiske militære mål knyttet til Ukraina. Aktørene utnyttet usikrede IP-kameraer for å innhente visuell etterretning om bevegelser og aktivitet ved kritisk infrastruktur i sanntid.

Fancy Bear brukte automatiserte verktøy, standard- eller svake passord og proxy-infrastruktur lokalisert nær målene for å redusere oppdagelse og muliggjøre vedvarende og skjult innhenting av bilder og metadata. Aktiviteten viser en dreining mot tettere integrasjon mellom cybertilgang og fysisk etterretning. Den understreker en vedvarende spionasjetrussel mot maritime virksomheter, der selv perifere digitale systemer kan utnyttes til å generere operasjonelt verdifull innsikt.

Iran-tilknyttet trusselaktør retter seg mot maritim sektor

I september 2025 ble et stort antall interne dokumenter fra den Iran-tilknyttede trusselaktøren Charming Kitten lekket på GitHub. Analyse av dokumentene bekrefter at maritime virksomheter bevisst målrettes som del av en strategisk etterretningsinnhenting rettet mot globale forsyningskjeder, energistrømmer og sanksjonsovervåking. Trusselaktøren viser inngående forståelse for maritime operasjoner og prioriterer systematisk tilgang til avdelinger med ansvar for befraktning, flåtestyring, bemanning, tekniske operasjoner og havneaktiviteter.

Operasjonene utnytter primært internetteksponerte tjenester, inkludert Microsoft Exchange og VPN-løsninger, for å hente ut e-postarkiver, legitimasjon og interne distribusjonslister. Dette muliggjør langsiktig kartlegging av organisasjoner og videre målretting. Det finnes ingen indikasjoner på nært forestående forstyrrende hensikt, men omfanget og vedvarende tilgangen som er oppnådd, senker terskelen betydelig for fremtidige pressmidler, forstyrrende eller hybride operasjoner dersom Iran-tilknyttede aktører skulle handle i tråd med endrede strategiske prioriteringer.

De lekkede dokumentene inneholder detaljer om nær 700 virksomheter som er målrettet, og minst 30 bekreftede kompromitteringer: 14 ofre innen energi (olje og gass), 8 innen logistikk og forsyningskjede og 8 innen maritim skipsfart.


SET confidence_score = 0.0001
FUNCTION
RETURN
LOOP FOREV
ELSE:
FOR EA
cache(
emit(o
<context:init>
<state id=
<vector na
<loop condition="entropy!=0 && truth<=approx">
normal
RETURN

KI og agenter

Det er meget sannsynlig at trusselaktører vil ta i bruk kunstig intelligens (KI) for å forbedre egne operasjoner. Tempoet og omfanget av bruken avhenger i stor grad av aktørene og deres mål, og gjenspeiler den samme variasjonen i adaptasjon som vi ser hos legitime virksomheter. Det er sannsynlig at KI vil være både et mål og et verktøy for trusselaktører i 2026.

KI som verktøy

Trusselaktører vil med stor sikkerhet bruke KI til å forbedre kvaliteten og spredningen av phishingkampanjer. KI har vist seg å øke både troverdigheten til, og rekkevidden av, kampanjene. KI brukes også i stor grad til å lage deepfakes – medier som fremstår som ekte, som bilder, video og lyd. Med rask modellutvikling og økt tilgjengelighet blir det stadig vanskeligere å skille ekte fra falskt. Deepfakes kan brukes i phishingkampanjer, falske møter og informasjonsoperasjoner rettet mot maritim sektor. Bruken av syntetiske medier undergraver tilliten i det digitale rom. Maritim sektor er global av natur, med mye fjernarbeid, og bør være særlig bevisst denne utviklingen.

Det er meget sannsynlig at trusselaktører vil bruke KI til kompetanseheving og utviklingsstøtte. For etablerte aktører kan dette innebære bruk av KI til å utvikle avansert skadevare som tilpasser seg miljøet den kjøres i og kan omgå forsvarsmekanismer. En annen mulighet er KI-drevne kampanjer som simultant kan teste inngangspunkter på tvers av en global flåte i et tempo som ikke er mulig om det gjøres manuelt. Slike kampanjer identifiserer svakheter raskere enn menneskelige analytikere kan reagere.

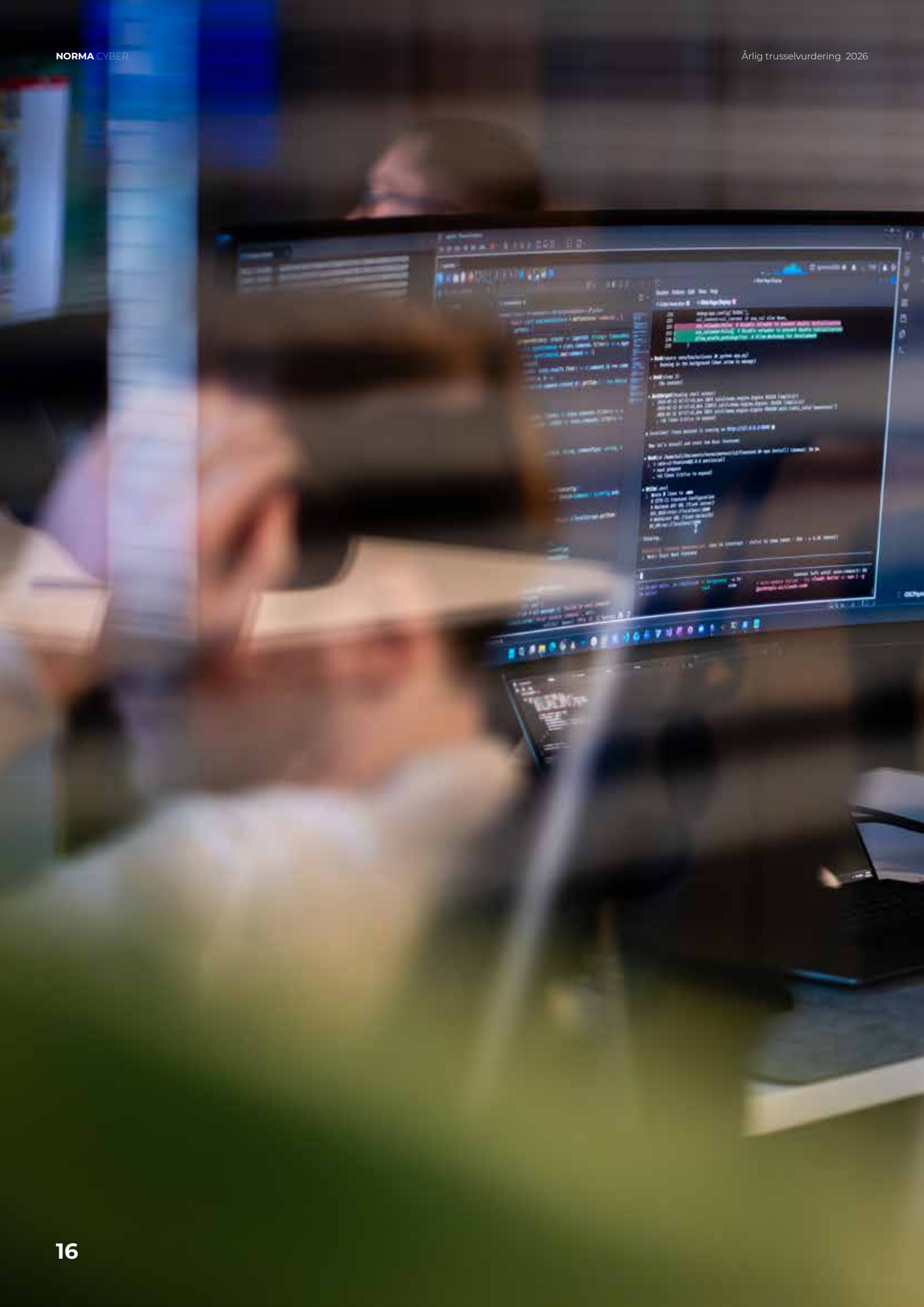
KI muliggjør utvikling av skadevare for mindre erfarne individer og grupper. I tillegg kan den veilede i hvordan de kan få tilgang til bedrifter, lateral bevegelse i nettverk og deployering av skadevare og verktøy. Dette vil sannsynlig gjøre det mulig for et bredere spekter av trusselaktører å påvirke bransjer og teknologi de tidligere manglet forutsetninger for. Dette senker terskelen for avanserte angrep.

KI som mål

Bruken av KI i virksomheter medfører risiko for datalekkasjer og utnyttelse av selve KI-løsningene. Etter hvert som KI blir mer utbredt er det sannsynlig at ansatte vil bruke slike verktøy. Bruk av uregulerte og ikke-godkjente KI-verktøy, som gratis modeller, nettleserutvidelser og andre gratisprogrammer, innebærer høy risiko for informasjonslekkasje. Trusselaktører og utviklere som ønsker økt inntjening vil sannsynlig bygge inn funksjonalitet for dataeksfiltrering i slike verktøy. Dette kan føre til at informasjon som deles med, eller vises mens applikasjonen er aktiv på systemet, kan overføres uten at brukeren er klar over det.

Økningen i såkalt vibe coding – der brukere beskriver hva de vil lage og KI skriver koden – åpner også nye angrepsflater. Uten tilstrekkelig kodegjennomgang kan KI introdusere sårbarheter som kreative angripere kan utnytte.

Agentiske KI-løsninger er et sannsynlig mål for trusselaktører. Agentisk KI er KI-systemer som opererer delvis autonomt for å nå et mål. I en virksomhetsarkitektur betyr dette ofte at agenter har egne identiteter med brede rettigheter for å løse oppgaver. Slike identiteter er attraktive mål for angripere som ønsker å utføre handlinger i systemene. Når agentisk KI erstatter eller integreres i interne prosesser kan det føre til redusert menneskelig forståelse og innsikt i systemenes virkemåte. En slik utvikling vil sannsynlig svekke evnen til å avdekke ondsinnede aktører som manipulerer agentene.



Informasjonsoperasjoner

Det er meget sannsynlig at nordiske maritime virksomheter vil bli utsatt for angrep som del av informasjonsoperasjoner som fremmer anti-vestlige, anti-NATO- og anti-EU-narrativer. Formålet er å påvirke og forsterke eksisterende holdninger. Både stater og uavhengige trusselaktører gjennomfører informasjonsoperasjoner for å forme offentlig oppfatning og fremme strategiske mål. Det digitale rom, og særlig sosiale medier, egner seg godt til dette.

Krig og geopolitikk

Det er sannsynlig at geopolitiske spenninger vil utløse reaksjoner fra aktører som ønsker å utøve innflytelse. Det er sannsynlig at de fleste informasjonsoperasjoner rettet mot nordiske maritime virksomheter vil komme fra hacktivistgrupper og kombinere budskap med direkte angrep. Det er lite sannsynlig at primærmålet med operasjonene er å endre holdninger internt i maritime virksomheter. Angrepene vil sannsynlig heller brukes til å forsterke angriperens verdensbilde. Dette kan innebære å bruke angrep som sosialt bevis på egne (ofte overdrevne) ferdigheter og overlegenhet, å rettferdiggjøre handlingene på bakgrunn av politikk, og å repetere et forenklet narrativ. Slik søker aktørene sannsynlig å styrke støtten til egne synspunkter og å øke tilliten til egen nasjons kapasitet.

Russland benytter aktivt ulike former for cyberstøttede informasjonsoperasjoner som del av en bredere strategi. Det er sannsynlig at prorussiske trusselaktører opererer i hele spekteret av statlig tilknytning. Fremtredende grupper fungerer sannsynlig som stedfortredere for staten, og budskapene deres blir sannsynlig forsterket av aktører som oppriktig tror på narrativet som fremmes.

Trusselaktører som opererer åpent på sosiale medier vil meget sannsynlig kombinere informasjonsoperasjoner med forstyrrende angrep som tjenestenektangrep (DDoS) og innbruddsforsøk.

Arktis

Det er meget sannsynlig at offentlige diskusjoner om Arktis vil være fremtredende i 2026. Dersom situasjonen eskalerer og maktbalansen forskyves, vil maritime virksomheter som opererer i regionen sannsynlig bli brukt og misbrukt i ulike mediesaker. Form og vinkling vil avhenge av hvem som publiserer og hvilket narrativ de ønsker å forsterke. Virksomheter innen fiskeri, energi og militære operasjoner står overfor den høyeste trusselen.

Miljø

Med økende splittelse mellom vestlige land i spørsmål som klimaendringer, er det sannsynlig at miljøbevegelser og deres støttespillere vil uttrykke seg digitalt, særlig i sosiale medier. Når det gjelder forstyrrende virkemidler, har klimaaktivister historisk hatt størst suksess med fysiske demonstrasjoner for å skape oppmerksomhet, og dette vil sannsynlig forbli hovedmetoden. Samtidig kan virksomheter som deltar i fossil energivirksomhet med land som oppfattes som klimafiendtlige, møte sosial eller omdømmemessig motreaksjon fra miljøengasjerte aktører.

Forstyrrende angrep

Nordiske maritime virksomheter står overfor en moderat trussel fra politisk motiverte forstyrrende angrep mot sin infrastruktur. Hensikten med slike angrep er å påvirke systemer negativt og legge press på virksomheter gjennom utilgjengelige systemer. Slike angrep vil meget sannsynlig medføre økonomiske tap dersom de rettes mot tjenester og enheter som brukes i operativ drift.

Hacktivistkollektiver motivert av politiske eller religiøse overbevisninger er de fremste driverne bak forstyrrende angrep. Deres primære metode er Distributed Denial-of-Service (DDoS), som brukes for å gjøre nettressurser utilgjengelige ved å overbelaste nettverkstrafikken og skape midlertidig nedetid. Det er sannsynlig at enkelte profilerte grupper har involvering. Ved å bruke hacktivister som mellomledd kan stater opprettholde plausibel benektelse og redusere direkte attribusjon, noe som gjør det mulig å gjennomføre ulovlig aktivitet samtidig som de formelt forholder seg til internasjonale avtaler.

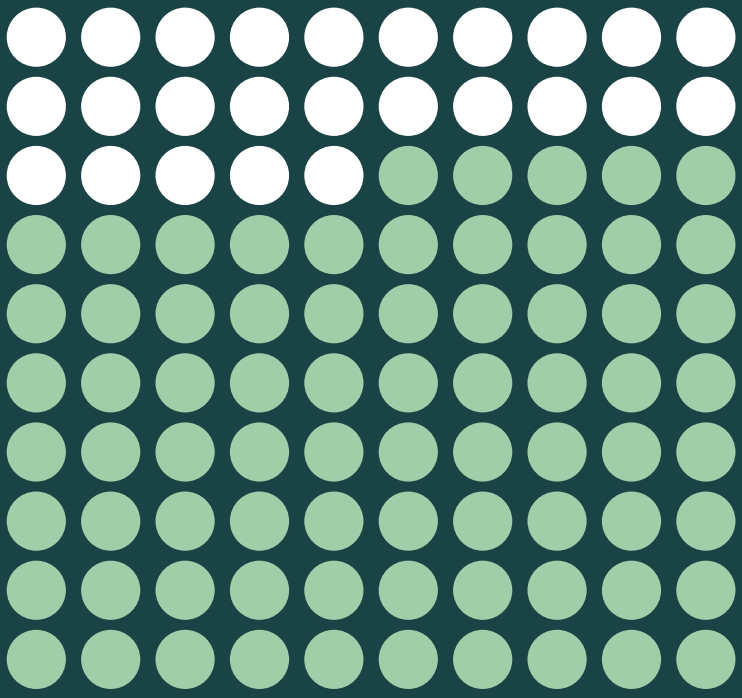
Forstyrrende cyberoperasjoner vil sannsynlig medføre økonomiske tap dersom de rettes mot systemer og tjenester i operativ bruk, uavhengig av angriperens motivasjon. De økonomiske konsekvensene oppstår typisk som følge av driftsstans, tjenesteforsinkelser og håndtering av hendelser. Havner og passasjertransport har dominert oversikter over maritime DDoS-ofre i 2025, og dette vil sannsynlig fortsette.

Det forventes at det bredere hacktivistmiljøet fortsatt vil foretrekke angrepsmetoder med lav kompleksitet. DDoS-angrep vil sannsynlig forbli den dominerende taktikken, ettersom det muliggjør forstyrrelser uten at angriperne må bryte seg inn i systemene. Fremtredende hacktivistgrupper vil sannsynlig fortsette å utvikle verktøy og utvide sine kapasiteter.

I 2025 fortsatte utviklingen med at hacktivister forsøker å angripe operasjonell teknologi (OT) globalt, en trend som sannsynlig vil fortsette i 2026. Dette skyldes sannsynlig hvor enkelt noen slike angrep kan gjennomføres og hvor effektive de er for å bygge et image som en forstyrrende og kapabel aktør i offentligheten. Den generelle trusselen mot operativ OT i nordisk maritim sektor fra hacktivistmiljøer er lav. Feilkonfigurerte, svakt sikrede eller internetteksponerte enheter står imidlertid overfor en moderat trussel for manipulering og utnyttelse som skrytemateriale. Hensikten bak angrepene er sammensatt og varierer mellom aktører. De fleste hacktivister i dette domenet er politisk motiverte og bruker OT-angrep for å oppnå oppmerksomhet og bygge omdømme. Angrep mot OT-systemer, særlig de med fysisk og/eller økonomisk konsekvens, vil meget sannsynlig tiltrekke seg medieoppmerksomhet og dermed gi eksponeringen de søker. Dette utelukker ikke at enkelte også kan ønske å forårsake fysisk skade. Hacktivister vil meget sannsynlig feilvurdere og overvurdere egen påvirkning på fysiske systemer, noe som fører til et generelt misforhold mellom påståtte resultater og verifiserbare konsekvenser. Hacktivistgrupper med høyt operasjonstempo finner og får sannsynlig tilgang til OT-systemer ved å skanne etter internetteksponerte Virtual Network Computing (VNC)-instanser. VNC er en teknologi som gjør det mulig å vise og styre en datamaskin eksternt over nettverk. Dersom en oppdaget VNC-instans er passordbeskyttet, vil de sannsynlig forsøke brute force-angrep ved bruk av passordlister.

75,82%

av DDoS angrep utført av NoName057(16) var mot havner



NoName057(16)

Den hacktivistgruppen som leder an i målrettingen av maritime virksomheter i Norden, er NoName057(16). Den pro-russiske hacktivistgruppen har vært aktiv mot NATO-allierte land siden kort tid etter starten på krigen mellom Russland og Ukraina. Kjerneledelsen i NoName057(16) er meget sannsynlig tilknyttet statlige aktører, noe som former gruppens struktur og operasjoner.

Den sentrale gruppen velger ut mål, og støttespillere oppfordres til å delta i angrep gjennom DDoSia, deres egenutviklede verktøy. NORMA Cyber registrerte 182 DDoS-angrep mot maritime virksomheter utført av enkeltpersoner som brukte DDoSia. Av disse var 138 rettet mot havner og havnerelaterte virksomheter.

GNSS-forstyrrelser

Trusselen fra GNSS-forstyrrelser vil forbli høy i geopolitisk sensitive områder det kommende året. Nordiske rederier som opererer i slike områder vil meget sannsynlig oppleve GNSS-forstyrrelser.

De mest observerte metodene er jamming og spoofing. Jamming fører til tap av posisjon eller tid, mens spoofing gir feil posisjon. Langvarig tap av posisjon eller tid vil sannsynlig ha kaskadeeffekt på andre systemer ombord. Forstyrrelser har også ført til grunnstøtinger og stans i terminal- og havneoperasjoner. Hovedhensikten er sannsynlig defensiv, der forstyrrelsesteknikker brukes for å etablere GPS-nektede soner rundt kritiske militære installasjoner for å beskytte mot drone- og missilangrep. Samtidig fungerer det som et strategisk signal i hybrid krigføring, ved å demonstrere kapasitet og hevde innflytelse over omstridte maritime områder uten direkte militær konfrontasjon. GPS- eller AIS-spoofing brukes også av sivile fartøy involvert i sanksjonerte eller ulovlige aktiviteter for å unngå sporing. Forstyrrelser forventes å vedvare i geopolitisk sensitive områder som nordområdene (Barentshavet), den østlige delen av Østersjøen, vestlige og nordlige deler av Svartehavet, det østlige Middelhavet, Rødehavet og Suezkanalen, Persiabukta/Arabiske gulf og Hormuzstredet.

En tydelig utvikling er at forstyrrelsene blir mer sofistikerte, ved at flere GNSS-konstellasjoner rammes og ved bruk av hybride mønstre som kombinerer spoofing og jamming. Dette øker trusselen mot maritime operasjoner. GNSS leverer kritiske posisjons-, navigasjons- og tidstjenester, men er iboende sårbart på grunn av svake satellittsignaler, manglende autentisering og begrensninger i sivile mottakere. Mot slutten av 2025 viste rapporter en overgang til hybride mønstre, der spoofede GPS L1-signaler ble kombinert med samtidig jamming av GLONASS-, Galileo- og BeiDou-konstellasjoner. Denne fler-konstellasjonsmålrettingen gjør det vanskelig for fartøy å bytte til reservesystemer.

I 2025 rapporterte NORMA Cybers medlemmer om GNSS-forstyrrelser i Norskehavet, Barentshavet, Østersjøen, Rødehavet, Persiabukta/Arabiske gulf og Omanbukta. Forstyrrelser påvirket også terminal- og havneoperasjoner ved Jubail Inner Anchorage og King Abdullah Port i Saudi-Arabia, Gdańsk havn i Polen og LNG-terminalen i Bahrain.

Forstyrrelser i nordlige havområder

Den østlige delen av Østersjøen utenfor Kaliningrad vil meget sannsynlig forbli preget av omfattende GNSS-forstyrrelser. Området har gjennomgått en betydelig utvikling, fra vedvarende, men lokal jamming til en mer sofistikert hybrid kampanje kjennetegnet av kraftig økning i hendelser, geografisk utvidelse og økt teknisk kompleksitet. I fjor strakte forstyrrelsene seg vestover inn i Sør-Sverige, og et nærmest vedvarende belte av forstyrrelser ble etablert fra Finskebukta til Gdańskbukta, med betydelig påvirkning på innseilingene til Kaliningrad, Klaipėda og Gdańsk. Antallet hendelser økte kraftig i 2025. Innen september rapporterte svenske myndigheter at GNSS-forstyrrelser hadde økt fra 55 hendelser i 2023 til 733 i 2025, med aktivitet sporet til russisk territorium. En studie i juli triangulerte signalene til Baltiysk (Kaliningrad) og områder rundt St. Petersburg, og bekreftet at kraftig utstyr bevisst ble rettet mot internasjonalt farvann. Russland bruker elektronisk krigføring for å signalisere handlekraft i strategiske områder og påvirke maritime rom. Det er sannsynlig at GNSS-forstyrrelsene i Østersjøen vil forbli høye i 2026.

Forstyrrelser i Barentshavet

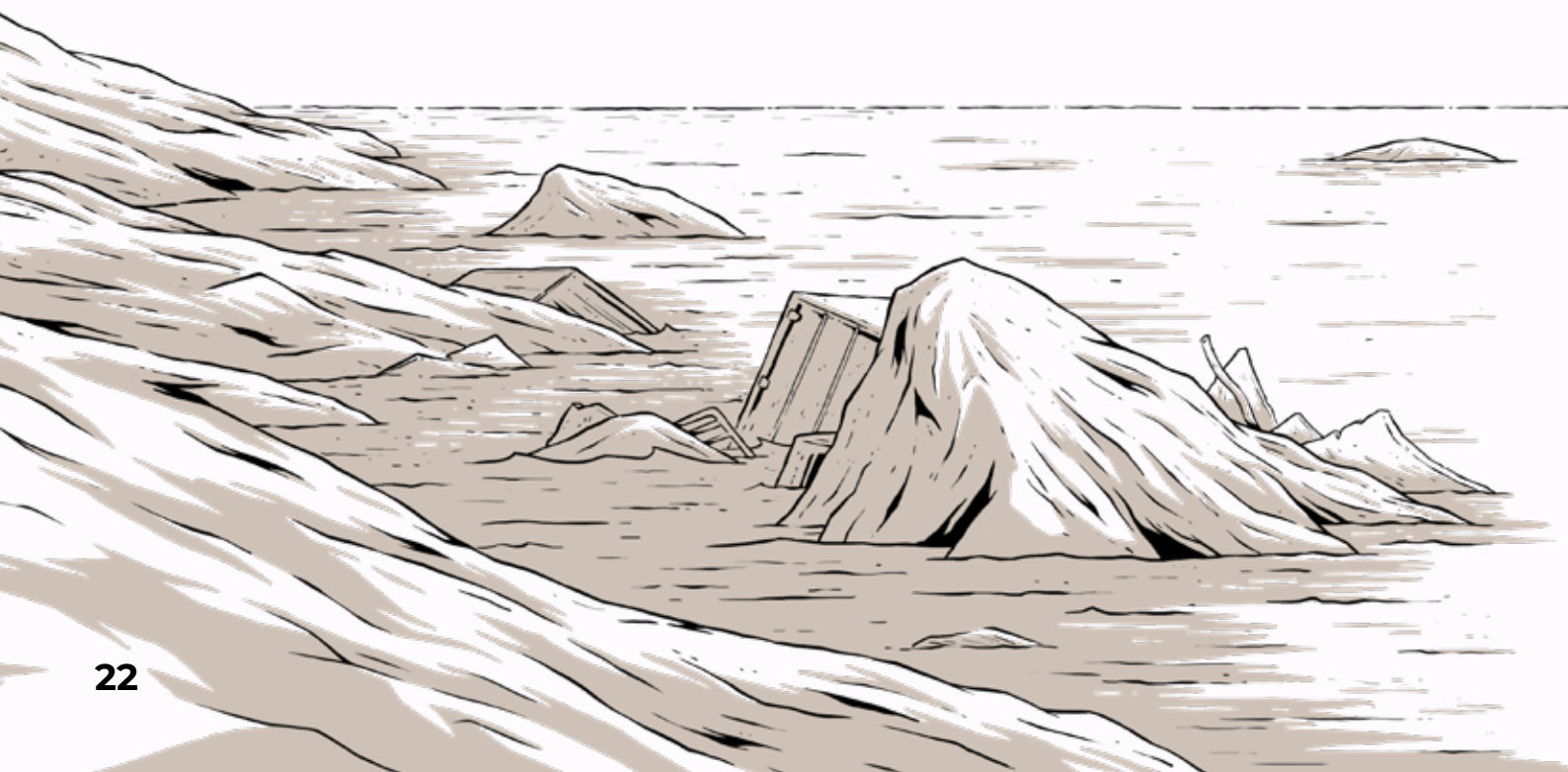
Det er sannsynlig at GNSS-forstyrrelsene i nordområdene vil forbli høye i 2026. I 2025 utviklet forstyrrelsene i Øst-Finnmark og Barentshavet seg fra høydebasert jamming til mer sofistikert lavtflygende spoofing som også påvirker operasjoner på bakkenivå. NORMA Cybers medlemmer har rapportert GNSS-forstyrrelser i Barentshavet.

Russland bruker GNSS-forstyrrelser som et strategisk beskyttelsestiltak for å skjerme høyverdige militære og politiske ressurser mot moderne trusler som droner og presisjonsstyrte våpen. I slutten av november 2025 deployerte Russland betydelige militære kapasiteter til Kolahalvøya, da 16 Tu-22M3 langtrekkende bombefly ble flyttet til Olenya flybase. Den økte tilstedeværelsen av bombeflygruppen øker sannsynligheten for intensivert GNSS-forstyrrelse i Barentsregionen.

Forstyrrelser i Rødehavet og Persiabukta / Arabiske gulf

Trusselen fra GNSS-forstyrrelser i Rødehavet og Persiabukta / Arabiske gulf vil være moderat det kommende året. I 2025 utviklet GNSS-forstyrrelsene i Rødehavet seg fra lokal jamming i sør til omfattende interferens som nådde helt til Suezkanalen. Den operative påvirkningen ble tydelig 10. mai, da containerskipet MSC ANTONIA gikk på grunn utenfor Jeddah i Saudi-Arabia. Hendelsen ble vurdert som sannsynlig forårsaket av omfattende GPS- eller AIS-spoofing i området.

I Persiabukta / Arabiske gulf skjedde en markant eskalering i juni etter Israels angrep på iranske atomanlegg. Åpne kilder rapporterte om utbredt spoofing som påvirket opptil 200 kommersielle fly daglig, mens maritim rapportering dokumenterte falske posisjonssignaler og kraftig jamming i Hormuzstredet. Til tross for våpenhvile økte interferensen igjen i tredje og fjerde kvartal. 30. september ble det rapportert en betydelig topp ved Jubail Inner Anchorage i Saudi-Arabia, der havnemyndighetene midlertidig stanset all fartøysbevegelse på grunn av upålitelig GNSS. Dette påvirket også LNG-terminalen i Bahrain.



Operative konsekvenser av GNSS-forstyrrelser

Grunnstøtingen av MSC ANTONIA

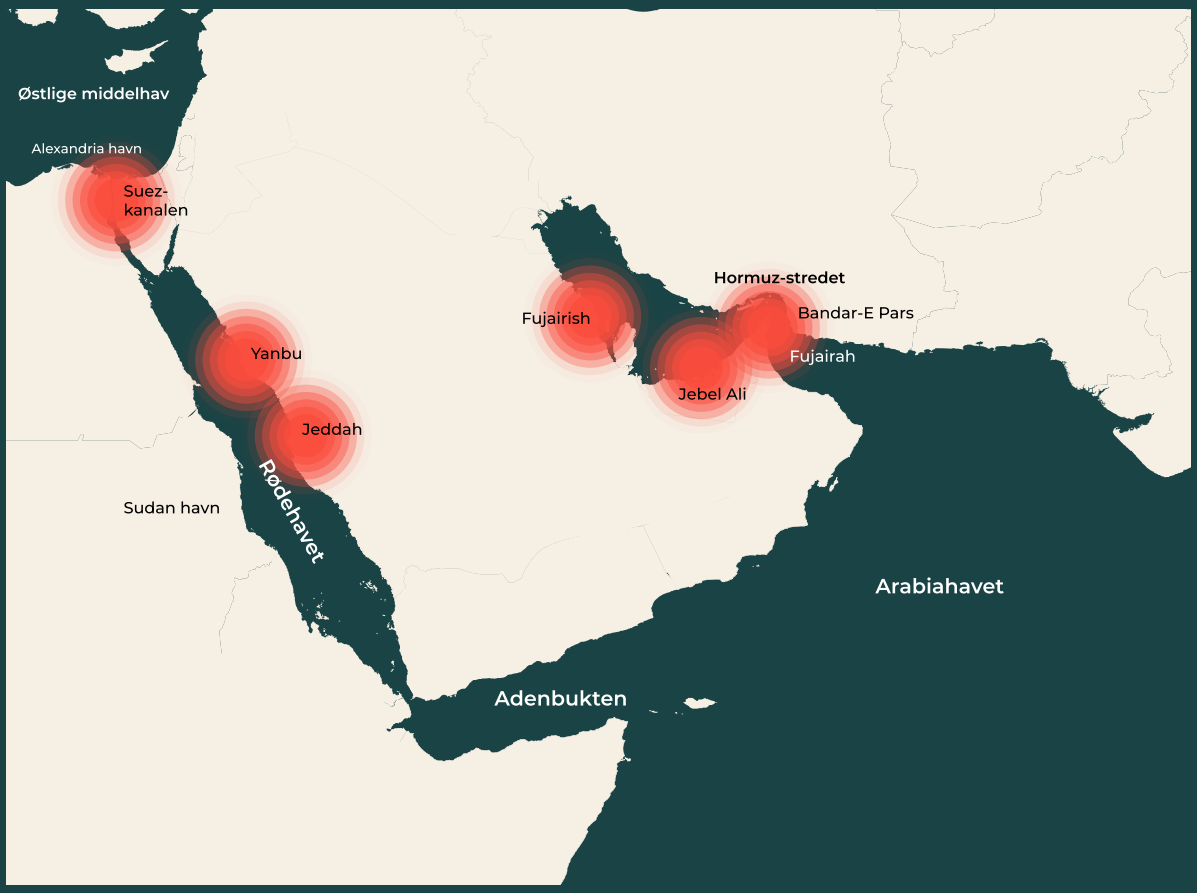
10. mai 2025 gikk det Liberia-flaggete containerskipet MSC ANTONIA (IMO 9398216) på grunn utenfor Jeddah i Saudi-Arabia. Fartøyet var sannsynlig utsatt for omfattende GPS- eller AIS-spoofing i operasjonsområdet. Hendelsen fant sted i en periode med dokumentert navigasjonsustabilitet i Rødehavet, der MarineTraffic viste en rekke fartøy med spoofede posisjoner i området. Området var utstyrt med etablerte navigasjonshjelpemidler.

Grunnstøtingen av MEGHNA PRINCESS

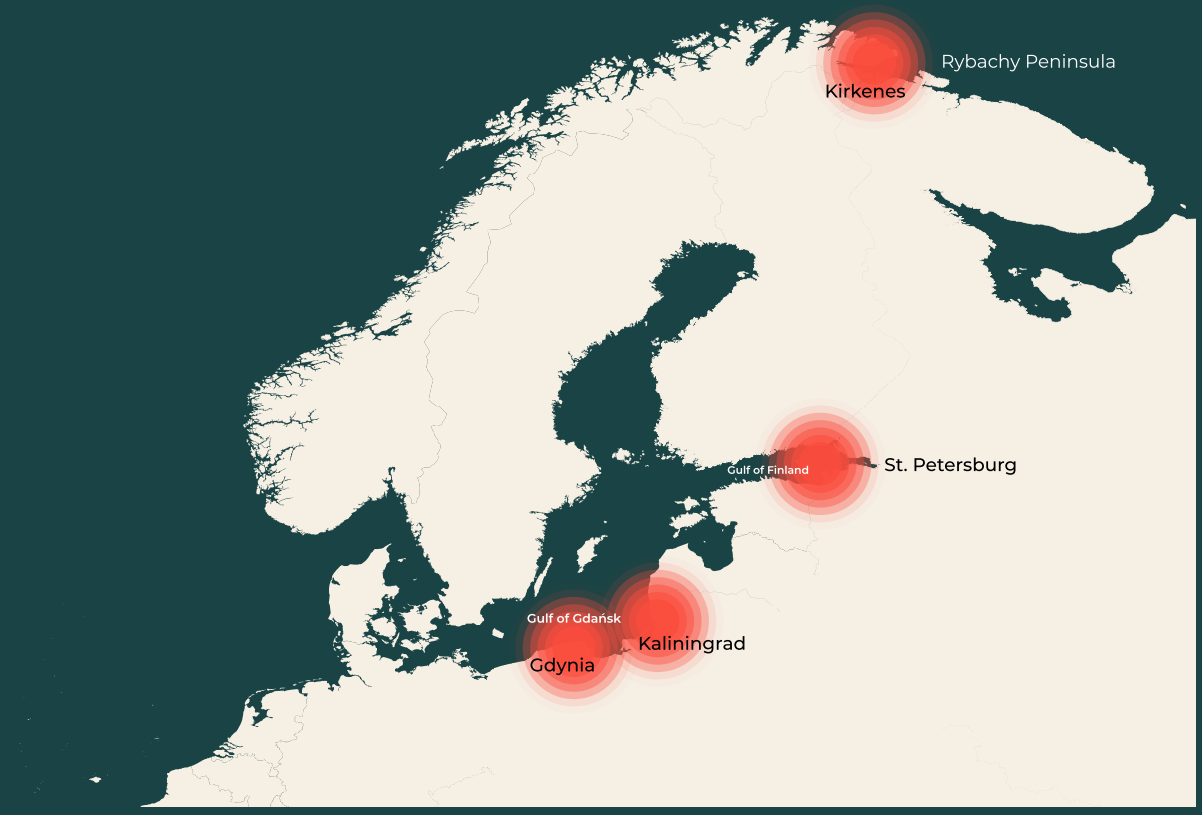
29. desember 2024 gikk det Bangladesh-eide bulkskipet MEGHNA PRINCESS (IMO 9805776) på grunn nær den russiske havnen Ust-Luga i Finskebukta. Fartøyet befant seg utenfor hovedleden da det traff grunnen, som var merket med fire kardinalmerker. Medieomtale hevdet at fartøyet kom ut av kurs som følge av GPS-jamming og traff en undersjøisk grunne på 4,8 meters dyp. Data fra GPSJam bekreftet høye nivåer av forstyrrelser i området 28. desember.

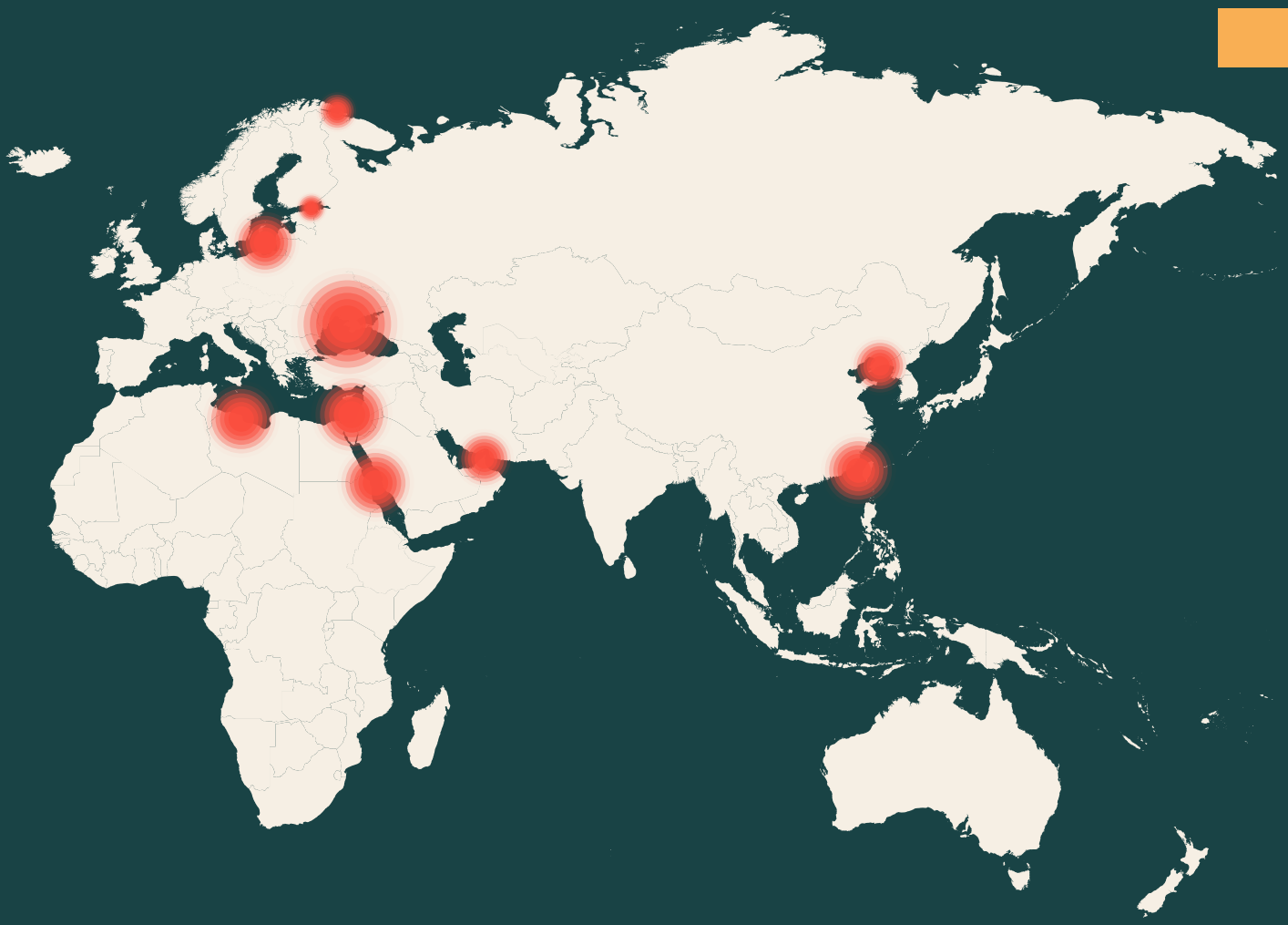
Trussel fra GNSS-forstyrrelser

Hotspots i Rødehavet og Persiabukta i 2025



Hotspots i Barentshavet og Østersjøen i 2025





Områder med høy trussel

Svartehavet

Høy trussel for GNSS forstyrrelser i nordvestlig del av Svartehavet, og rundt Krimhalvøya, Sevastopol, Novorossiysk og Sochi

Barentshavet og Østersjøen

Høy trussel for GNSS forstyrrelser rundt Kirkenes og Rybachy Peninsula, i østlig del av Østersjøen, fra Gdanskbukta til Finskebukta, inkludert Kaliningrad og St. Petersburg.

Østlige Middelhav

Høy trussel for GNSS forstyrrelser i østlige middelhav, innseilingen til Suez og utenfor Tripoli.

Viktige Maritime flaskehalser

Høy trussel for GNSS forstyrrelser i Suezkanalen, midtre deler av Rødehavet og i Hormuz-stredet.

Signifikante hendelser

Fra jamming til hybride trusler

Rapporter viser et skifte mot hybridtaktikk, der jamming av flere satellittkonstellasjoner kombineres med GPS-spoofing.

Massiv AIS-spoofing hendelse

Tusenvis av falske skip dukket opp i Østersjøen når en landstasjon i Finland sendte falske AIS data inn til fartøysovervåkningstjenester.

Destruktive operasjoner

Det foreligger en lav trussel om bevisste destruktive operasjoner mot den bredere nordiske maritime sektoren. Destruktive cyberangrep har som formål å forstyrre eller ødelegge fysiske eller digitale systemer. For virksomheter som støtter NATO-logistikk, energiinfrastruktur eller Ukraina, vurderes trusselen som moderat. Den økte trusselen mot disse segmentene skyldes sammensmeltingen av cyberoperasjoner og hybride virkemidler, som fysisk sabotasje, som direkte truer sikkerhet og operativ kontinuitet.

Russland-tilknyttede trusselaktører utgjør den mest troverdige og alvorlige destruktive trusselen mot maritim sektor. Disse aktørene integrerer i økende grad cyberkapasiteter med fysisk sabotasje. Selv om Russland har evne til å gjennomføre destruktive cyberoperasjoner, er det mer sannsynlig at de benytter mellomledd eller hybride metoder for å unngå direkte attribusjon og eskalering med NATO. Den primære manifestasjonen av den russiske trusselen i maritimt domene er derfor hybrid fremfor rent cyberbasert.

Trusselaktører knyttet til Russlands militære etterretningstjeneste, GRU, representerer den mest betydelige destruktive trusselen mot maritim infrastruktur. Disse aktørene bruker en kombinasjon av tilpasset hyllevarebasert skadevare og spesialutviklede destruktive verktøy, og benytter villedningstaktikker, som å kamuflere destruktiv skadevare som løsepengevirus, for å villede attribusjonsforsøk.

Russland-tilknyttede aktører vil sannsynlig rette seg mot OT-nettverk for å etablere langsiktig tilgang med tanke på mulig fremtidig forstyrrelse. GRU-tilknyttede aktører har gjennomført kampanjer for å oppnå skjult tilgang til OT-miljøer innen energi, transport og offentlig sektor. Selv om direkte fysisk ødeleggelse av maritim OT er krevende, har Russland demonstrert evne til å gjennomføre datavaskingskampanjer mot logistikk- og energivirksomheter i Ukraina.

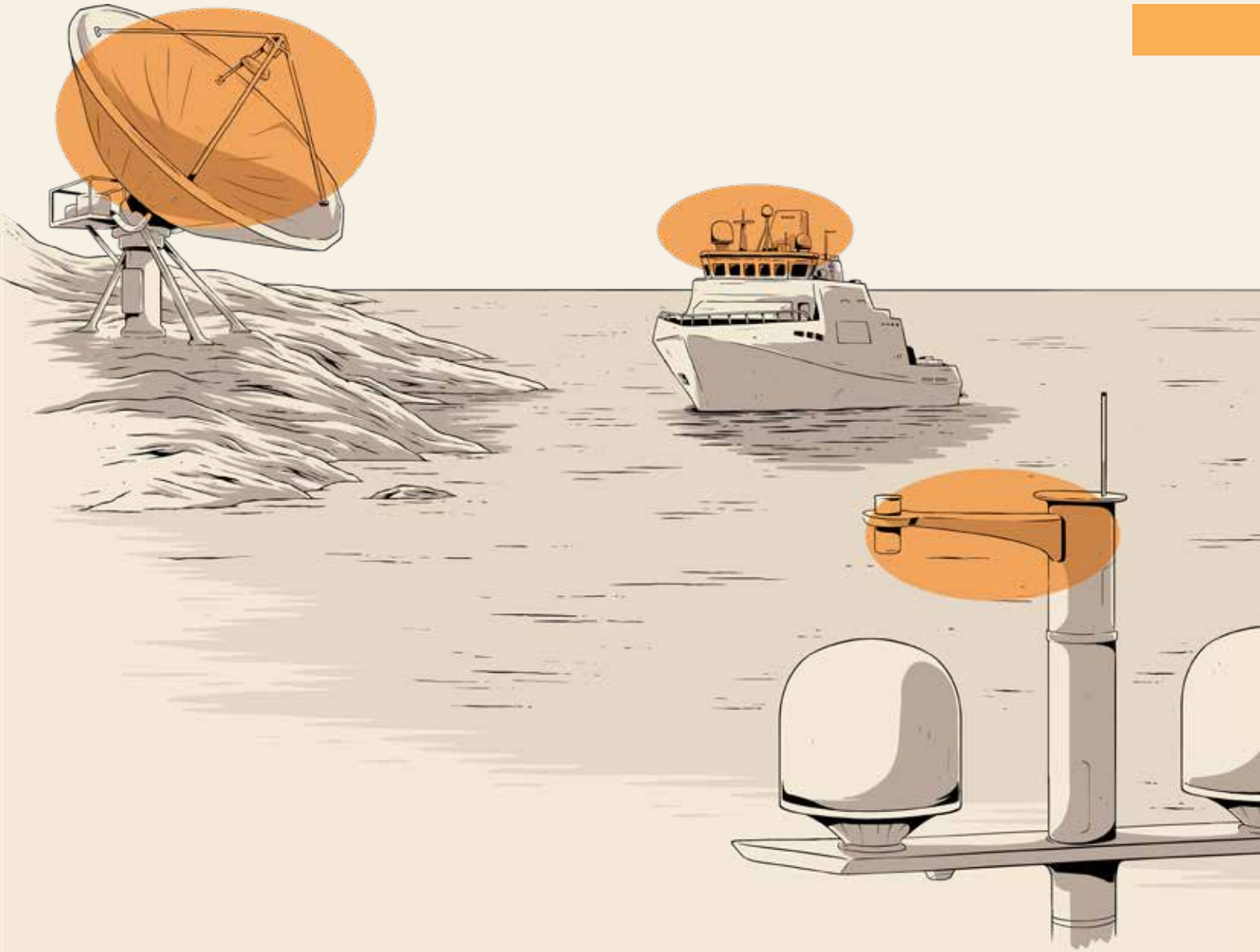
For å unngå politisk eskalering benytter Russland sannsynlig mellomledd, som hacktivistgrupper, til å gjennomføre forstyrrende og destruktive operasjoner. Denne strategien reduserer direkte statlig kontroll, men senker terskelen for sabotasje mot vestlige mål. Slike mellomledd forsøker kontinuerlig å manipulere eksponert infrastruktur, noe som gjør det mulig for russiske myndigheter å opprettholde plausibel benektelse samtidig som de skaper vedvarende press mot stater som ikke deler russiske narrativer.

Til tross for intensjonen vil destruktiv effekt gjennom hacktivistmellomledd sannsynlig oftere være utilsiktet enn bevisst

Den destruktive cybertrusselen fra Iran-tilknyttede aktører mot nordiske maritime virksomheter er lav. Virksomheter med direkte tilknytning til Israel eller USA, eller som opererer i Midtøsten, står imidlertid overfor en moderat trussel som følge av risiko for å bli rammet indirekte i regionale konflikter. Iran har vist en tydelig dreining mot «cyberstøttet kinetisk målutvelgelse», der digital rekognosering kombineres med fysiske angrep. Rapportering indikerer at Iran-tilknyttede aktører har kompromittert fartøysporingssystemer, som AIS-plattformer og CCTV-strømmer, for å følge skip i sanntid og direkte støtte missilangrep i Midtøsten.

Den umiddelbare sannsynligheten for et destruktivt kinesisk cyberangrep er lav, men grunnlaget legges for å kunne forstyrre maritime logistikkjeder dersom geopolitisk spenning eskalerer. Kina-tilknyttet aktivitet retter seg primært mot forhåndsposisjonering i kritisk infrastruktur for å avskrekke ekstern militær støtte til Taiwan. Dette inkluderer målretting mot havner og forsyningsinfrastruktur samt utnyttelse av kant-enheter for å opprettholde langsiktig, skjult tilgang og mulig destruktiv kapasitet. Gitt den kritiske betydningen av transportnettverk, havner og skipsfartsinfrastruktur, er disse sannsynlig innenfor målområdet.

Oppsummert er trusselen om destruktive cyberoperasjoner lav for det meste av den kommersielle flåten, men moderat for virksomheter knyttet til strategiske interesser. Statlige aktører foretrekker per i dag hybride tilnærminger, der cyberspionasje kombineres med fysisk sabotasje, fremfor direkte destruktive cyberangrep.



Nedstenging av SATCOM på sanksjonerte iranske fartøy

Operasjonen rettet seg mot Islamic Republic of Iran Shipping Lines (IRISL) og National Iranian Tanker Company (NITC). Fartøyene var underlagt sanksjoner fra USA og EU og mistenkt for å være involvert i ulovlig transport av missilkomponenter med dobbelt anvendelsesområde fra Kina til Iran. Operasjonen ble sannsynlig gjennomført ved å kompromittere en iransk landbasert IT- og satellittkommunikasjonsleverandør, fremfor direkte internettbaserte angrep mot enkeltfartøy.

Angriperne utnyttet backend-infrastrukturen som støttet flåtens VSAT-tjenester. Ved bruk av kompromittert legitimasjon og VPN-tunneler beveget de seg lateralt fra det landbaserte nettverket til utstyr ombord via interne IP-områder. Angrepet fokuserte på iDirect VSAT-modemer. Angriperne kjørte kommandoer via et interaktivt skall for å terminere den sentrale iDirect-modemprosessen og slo dermed umiddelbart ut satellittkommunikasjonen.

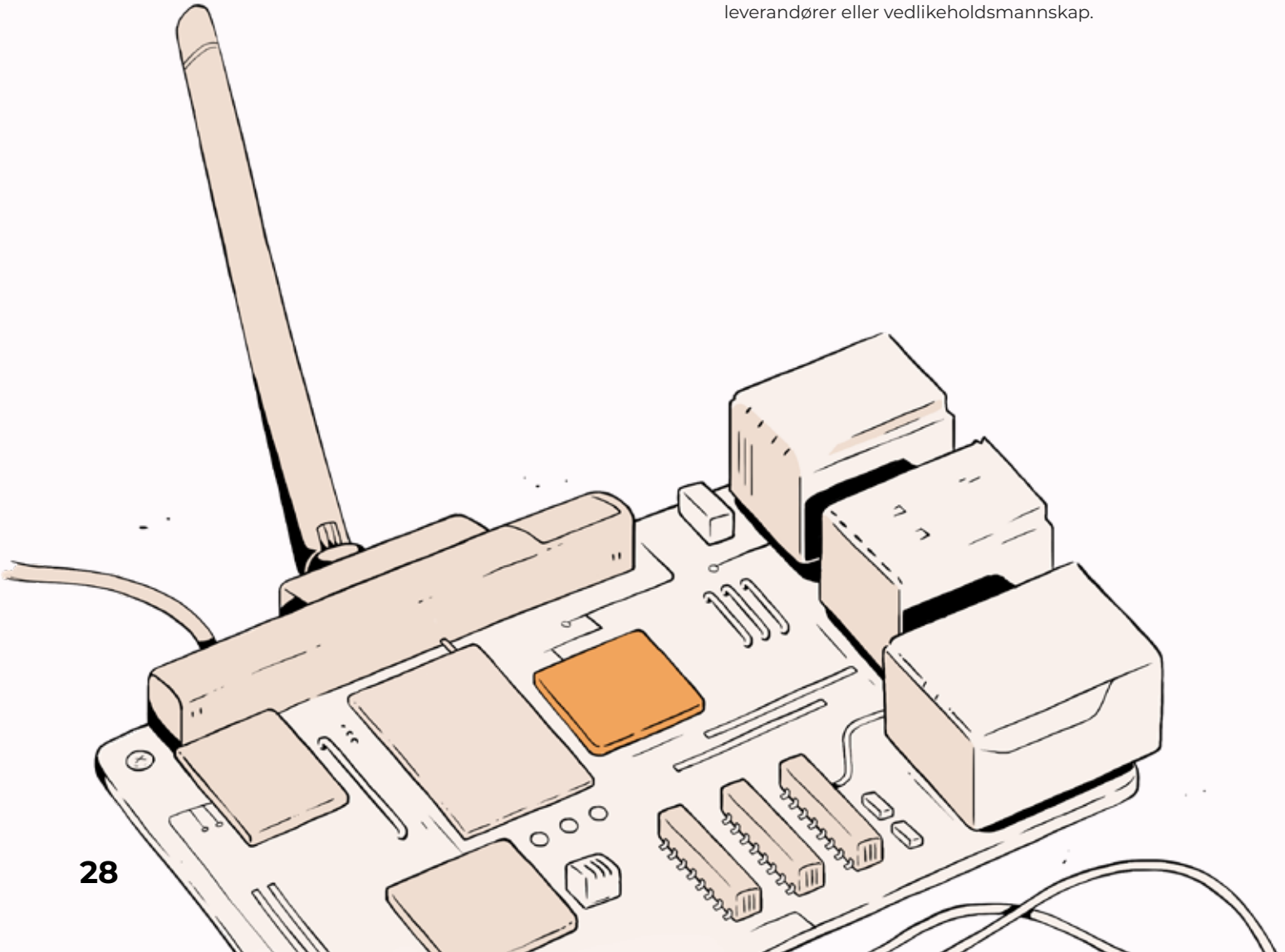
Trusler mot operasjonell teknologi

Den generelle trusselen mot maritim operasjonell teknologi (OT) er lav. Maritim OT vil imidlertid meget sannsynlig møte et stadig mer komplekst trusselbilde. I løpet av 2025 pekte to hovedtemaer seg ut: risikoen for eksponering av sensitiv informasjon fra produsenter av originalutstyr (OEM-er) og integratorer, samt den vedvarende trusselen fra ondsinnede innsidere.

Innsidetrusler og maskinvarebaserte angrep

Det er sannsynlig at trusselaktører vil forsøke å plassere maskinvare ombord på fartøy i 2026. Den mest utbredte hensikten vil sannsynlig være å tilrettelegge for organisert kriminalitet, men forhåndsposisjonering og spionasje kan ikke utelukkes. En viktig driver bak den økte trusselen er offentlig kjennskap til tilfeller der aktører har lykkes med denne taktikken, noe som bekrefter at metoden er levedyktig og kan inspirere andre. En annen muliggjørende faktor er økt tilgjengelighet av hjelpemidler som maskinvare og tilpasset KI-veiledning.

Avhengig av formålet og aktivitetene som utføres via en slik implantasjon, kan uautoriserte enheter være nær umulige å oppdage uten endepunkts- og nettverksovervåking på tvers av både OT- og IT-miljøer. Trenden med å bruke ondsinnede innsidere til å plassere maskinvare er særlig bekymringsfull for fartøy som opererer i geopolitisk sensitive områder eller er involvert i kritisk infrastruktur. Den lave tekniske terskelen, kombinert med utfordringer knyttet til avdekking, gjør dette til en attraktiv angrepsvektor. Trusselaktører vil sannsynlig fortsette å utnytte fysisk tilgang gjennom kompromittert personell, leverandører eller vedlikeholdsmannskap.



Skjult enhet ombord på fartøy

Oppdagelsen av en maskinvareimplantasjon ombord på et passasjerfartøy i desember 2025 representerer en betydelig utvikling i maritime cybermetoder. En Raspberry Pi Zero, utstyrt med mobilmodem, var fysisk koblet til fartøyets kontornettverk. Dette etablerte en vedvarende bak kanal som omgikk ordinære sikkerhetskontroller. Enheten var konfigurert til å opprette en skjult nettverkstunnel, som muliggjorde fjernaksess, tyveri av legitimasjon og nettverksrekognosering – uavhengig av fartøyets autoriserte internett tilkobling.

Sannsynlig involvering av mannskap i utplasseringen av enheten understreker alvoret i innsidetrusselen. Fysisk tilgang til nettverksinfrastruktur er fortsatt en av de mest effektive måtene å omgå cybersikkerhetstiltak på, særlig når det kombineres med avansert maskinvare som opererer utenfor ordinær nettverksovervåking. Den mobile komponenten gjorde det mulig for trusselaktører å opprettholde kommunikasjon uavhengig av fartøyets internettilkobling, begrenset kun av mobildekning langs kysten.

Økt trussel som følge av informasjonslekkasjer
Nordiske maritime virksomheter står overfor en moderat trussel for eksponering av sensitiv informasjon gjennom leverandørkjedeangrep. Ved målrettet angrep mot OT-systemer vil en trusselaktørs suksess meget sannsynlig avhenge av inngående systemforståelse. Når angripere får tilgang til detaljert dokumentasjon – som nettverkstopologier, IO-lister og funksjonsdiagrammer – blir det betydelig enklere å utvikle angrep som kan manipulere fartøyskontroller.

Kriminelle som eksfiltrerer proprietær programvare, kildekode og funksjonell dokumentasjon for OT-utstyr brukt ombord, og deretter publiserer dette på det mørke nettet, vil meget sannsynlig legge til rette for fremtidig utnyttelse av berørte komponenter. Slike hendelser skaper kjedereaksjoner i eksponering, ettersom én kompromittert produsent kan sitte på tekniske spesifikasjoner for utstyr installert på hundrevis av fartøy og hos flere operatører. Eksfiltrert kildekode og dokumentasjon gir trusselaktører dyp innsikt i systemenes indre struktur, potensielle sårbarheter og integrasjonspunkter som ellers ville krevd omfattende reversering for å avdekke. Når informasjonen først er tilgjengelig på nett, senkes terskelen for avanserte angrep betydelig.

I løpet av 2025 har flere verft og utstyrsprodusenter blitt rammet av sikkerhetsbrudd som førte til eksfiltrering av proprietær programvare, kildekode og funksjonell dokumentasjon for OT-utstyr installert på fartøy.

Den raske utviklingen innen KI forsterker trusselen knyttet til lekket teknisk informasjon betydelig. Tidligere krevde analyse av store mengder kildekode eller komplekse funksjonsdiagrammer høy fagkompetanse og betydelig tidsbruk. Med KI kan trusselaktører nå automatisere store deler av analysearbeidet. Ved å kombinere eksponert teknisk dokumentasjon med KI-drevet analyse forkortes tiden fra datatyveri til et gjennomførbart angrep drastisk.

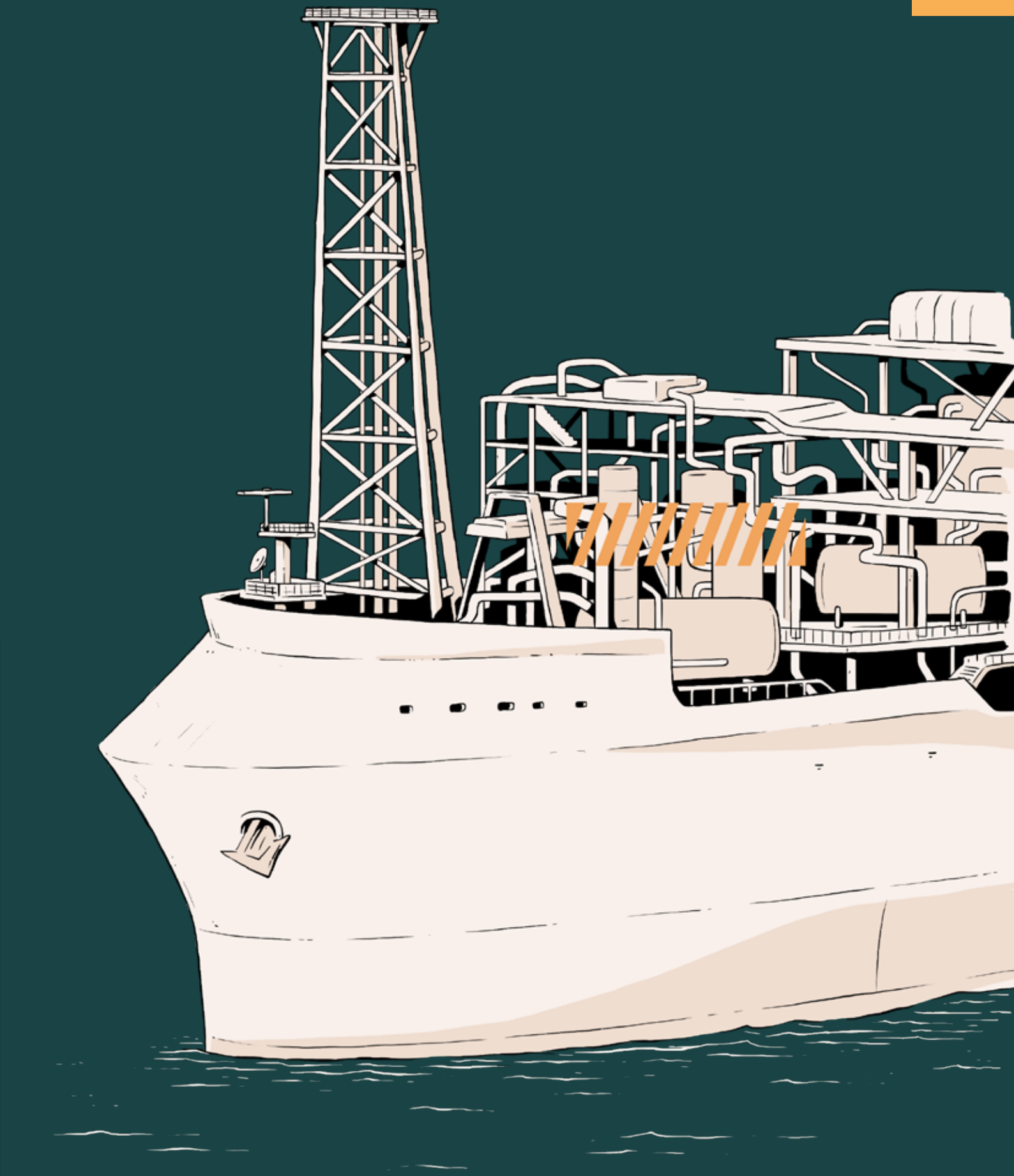
Hvordan sikre OT-ressurser?

Styrke fysisk sikkerhet: Forbedre adgangskontroll og overvåking av mannskap, leverandører og vedlikeholdspersonell.

Overvåking: Implementere endepunktsdeteksjon og -respons (EDR) samt nettverksovervåking for å avdekke uautorisert maskinvare og unormal trafikk.

Robust leverandørkjede: Etablere strengere cybersikkerhetskrav til OEM-er og integratorer for å begrense eksponering av sensitiv systemdokumentasjon.

Ved å erkjenne at OT-sikkerhet ikke lenger kun handler om brannmurer, men også om fysisk integritet og streng informasjonsforvaltning, kan maritim sektor styrke sin motstandskraft mot neste generasjon målrettede cybertrusler.



Økonomisk kriminalitet

Trusselen fra kriminelle mot nordisk maritim sektor er høy. Det kriminelle økosystemet forventes å fortsette profesjonaliseringen og utviklingen av spesialiserte roller. Profitt-motiverte kriminelle vil sannsynlig være opportunistiske i målutvelgelsen. Signifikante angrep i 2025 rammet ikke bare primærmålet, men fikk også konsekvenser for virksomheter som var avhengige av offeret. Disse trendene vil sannsynlig fortsette i 2026.

Innledende tilgang
Identitetsbasert tilgang vil sannsynlig være den dominerende metoden for å kompromittere maritim sektor det kommende året. Utnyttelse av identiteter gjør det mulig for angripere å logge inn uten å benytte sårbarheter. Angripere kan stjele identiteten til både mennesker og maskiner.

Phishing vil sannsynlig være den primære teknikken for å skaffe gyldige identiteter. Angriper-i-Midten (AiTM)-phishing, der angripere stjeler tokens for å omgå multifaktorautentisering (MFA), har vært særlig utbredt det siste året. Denne trenden vil sannsynlig fortsette. Phishing utgjør en høy trussel for økonomisk svindel, datatyveri og nettverkskompromittering av både land- og sjøbaserte maritime verdier.

En annen teknikk det er sannsynlig at kriminelle vil bruke mot nordiske virksomheter i 2026 er varianter av ClickFix, hvor de lurer brukere til å kopiere og kjøre ondsinnet kode. At brukere uvitende utfører skadelige handlinger bidrar til å omgå tradisjonelle deteksjonsmekanismer. Kriminelle vil sannsynlig fortsette å utvikle og automatisere nye måter å bruke ClickFix-teknikken på for å unngå deteksjon og skalere kampanjer mer effektivt.

Informasjonstyveri
Det er sannsynlig at bruken av informasjonsstjelende skadevare, såkalte infostealers, vil fortsette å utvikle seg det kommende året. Infostealers har vært populære blant trusselaktører i flere år og tilbys ofte som abonnementstjenester. Infostealers er en type lettvekts skadevare som vanligvis spres gjennom for eksempel gratis programvare, falske annonser og metoder som ClickFix. De er særlig kjent for å stjele brukernavn, passord og finansielle data lagret i nettlesere, men mange kan også hente ut andre typer data og samle systeminformasjon.

Det er sannsynlig at trusselaktører i økende grad vil bruke infostealers for å laste ned sekundær skadevare eller verktøy. NORMA Cyber observerer jevnlig brukernavn og passord, inkludert medlemsdomene-e-postadresser, i infostealer-logger som legges ut for salg på undergrunnsmarkedsplasser. I de fleste tilfeller er det meget sannsynlig at dette stammer fra infiserte private enheter som brukes til å logge på virksomhetens ressurser. At profesjonelle e-postadresser brukes til private tjenester, som for eksempel spill, er også et vanlig syn.

Det er meget sannsynlig at tilgangsmeglere vil fortsette å modnes og utvide porteføljen sin. En tilgangsmegler er en trusselaktør som spesialiserer seg på å kompromittere organisasjoner og selge tilgangen videre. I takt med profesjonaliseringen av det kriminelle økosystemet er det sannsynlig at sentrale tilgangsmeglere vil etablere forretningsforhold med grupper som gjennomfører videre operasjoner i nettverket for rask utnyttelse og økonomisk gevinst. De vanligste tilgangstypene som legges ut for salg på undergrunnsmarkedsplasser er fjernaksess via Remote Desktop Protocol (RDP) og tilgang til nettjenester gjennom gyldige brukernavn og passord. Det er sannsynlig at dette vil fortsette i 2026.

Utpressing
Nordiske maritime virksomheter står overfor en moderat trussel for utpressing fra økonomisk motiverte trusselaktører. Disse aktørene bruker ofte datatyveri, løsepengevirus og datasletting til å presse ofre til å betale. For maritime virksomheter er det også en vedvarende trussel for at tjenester de er avhengige av i daglig drift kan bli forstyrret av kriminelle aktører.

NORMA Cyber er kjent med 60 løsepengeangrep mot maritim sektor globalt i 2025. Det finnes utvilsomt mørketall. Flertallet av de kjente hendelsene ble publisert på lekkasjenettsteder, der trusselaktører

Det er meget sannsynlig at kriminelle som bedriver AiTM-phishing benytter kommersielt tilgjengelige phishing-sett med innebygde funksjoner for å omgå multifaktorautentisering. Det er meget sannsynlig at de utgir seg for å være kjente tjenester for å øke troverdigheten slik at ofrene interagerer med phishen. I den innledende fasen bruker de ofte legitim infrastruktur, noe som gjør angrepene vanskeligere å avdekke.

I et typisk AiTM-angrep ber angriperen offeret om å logge inn på Microsoft O365-kontoen sin for å få tilgang til et dokument eller en melding. Samtidig infiltrerer angriperen autentiseringsflyten og fanger opp brukernavn, passord og sesjonskapselen. Med sesjonskapselen kan angriperen logge inn som brukeren uten å utløse ytterligere autentisering.

NORMA Cyber varslet **77 virksomheter** i 2025 om kompromitteringer der angripere omgikk MFA-sikkerhetstiltak.

henger ut virksomheter som ikke betaler. Mange publiserer også stjålne data på disse sidene. Det er sannsynlig at løsepengeangrep i hovedsak er opportunistiske og antallet hendelser forventes å variere fra år til år. Selv om det totale volumet av angrep har stabilisert seg, har antallet navngitte løsepengegrupper økt gjennom 2025. Økosystemet har dermed gått fra noen få dominerende grupper med mange tilknyttede aktører til et mer fragmentert landskap med mange grupper. Det er sannsynlig at de kriminelle bytter mellom ulike grupper etter behov.

Økonomisk motiverte trusselaktører beveger seg raskere enn tidligere og reduserer tiden fra initial kompromittering til måloppnåelse. Det økte tempoet vil sannsynlig føre til mer aggressive angrepskjeder. Tidlig deteksjon er avgjørende for å begrense konsekvensene.

Det er meget sannsynlig at cyberkriminelle vil fortsette å bruke legitime verktøy og funksjoner for å nå sine mål, noe som gjør det vanskeligere å oppdage aktiviteten. For eksempel bruker trusselaktører ofte verktøy for fjernovervåking og -administrasjon (RMM) for å få tilgang, gjennomføre handlinger og kamuflere seg i det normale aktivitetsbildet. Det er meget sannsynlig at misbruk av slike verktøy vil fortsette i 2026. Vanlige metoder for å få tilgang til RMM-løsninger inkluderer innlogging med stjålne brukernavn og passord, sosial manipulering for å få brukere til å installere RMM-programvare, samt utnyttelse av sårbarheter i selve programvaren.

Leverandørkjedeangrep

Det maritime økosystemet er komplekst, og ingen virksomheter opererer uavhengig av andre. Nordiske maritime virksomheter står overfor en moderat trussel om dataeksponering, datatap og driftsstans som følge av angrep mot leverandørkjeden.
Selv om selve angrepet kan være enkelt, vil fysiske prosesser sannsynlig bli stanset under hendelseshåndtering av sikkerhetshensyn. Dette kan igjen forstyrre operasjoner. I 2025 observerte vi flere løsepengeangrep mot leverandører, der proprietære data og kundedata ble stjålet og publisert.
Det er lite sannsynlig at lekkasje av proprietære data fra skips- og terminalsystmer på det mørke nettet utgjør en umiddelbar trussel mot maritime systemer.

Løsepenge-virusangrep 2025

Andre typer

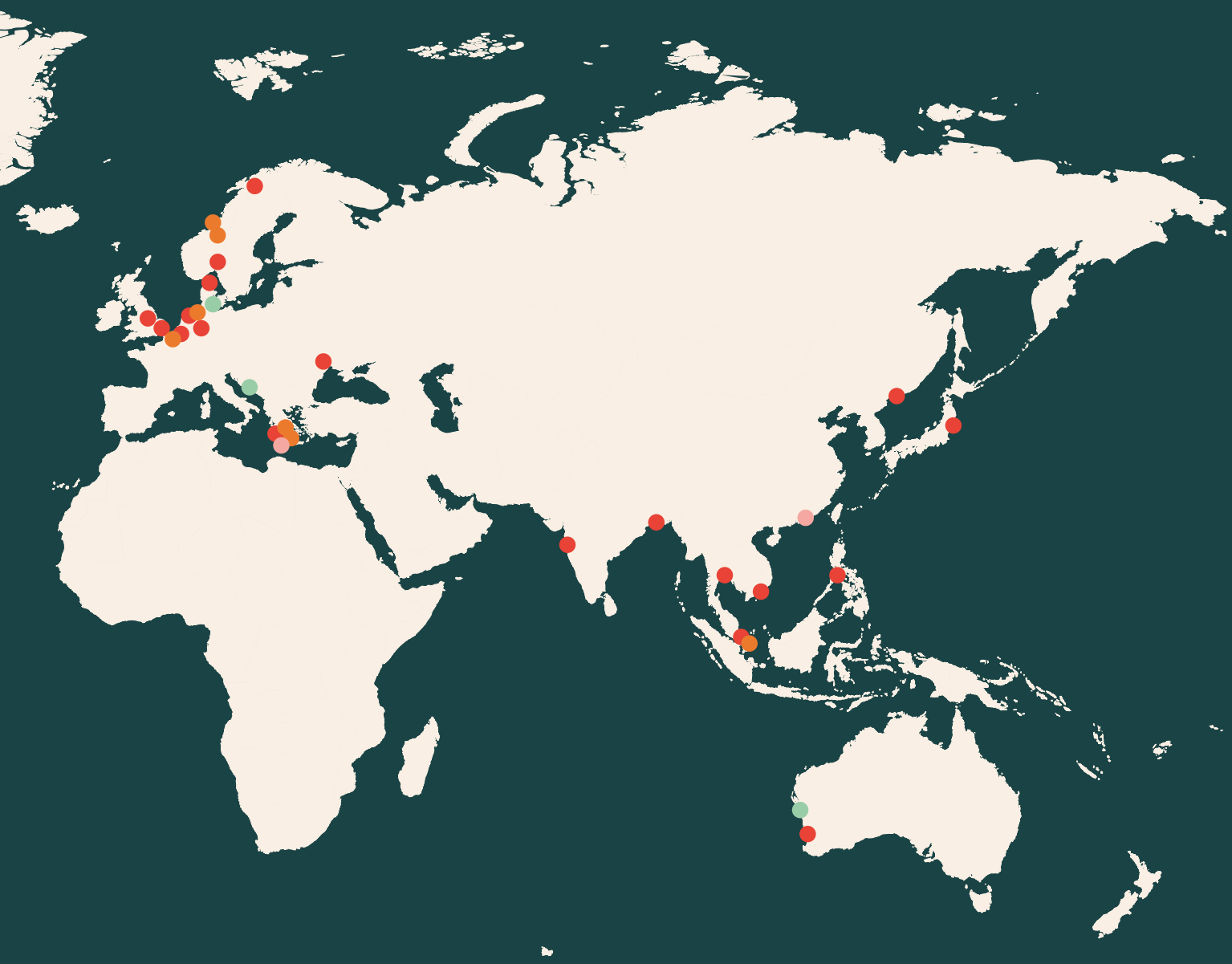
Babuk - Navarino (Greece)
Bert - S5 Agency World (UK)
Cactus - Contender Boats (USA)
Chaos - Hutchison Ports Duisburg (Germany)
Coinbasecartel - DSV (Danmark)
Devman - China Harbour Engineering Company (China)
Dire Wolf - K Subsea Group (Singapore)
Dragonforce - Grupo Serex (Costa Rica)
Everest - Petrobras (Brazil)
Funksec - Bangladesh Navy (Bangladesh)
Hunters - PetroVietnam Exploration Production Corporation (Vietnam)
Incransom - ASI Group Ltd. (Canada)
Incransom - National Boat Owners Association (USA)
J group - IKAD Engineering (Australia)
Kawa4096 - Tokio Marine Nichido (Japan)
Killsec - Docklyne (USA)
Lynx - Terport (USA)
Lynx - Margaritaville at Sea (USA)
Minteye - Inter-American Tropical Tuna Commission (USA)
Nightspire - Pioneer Ocean Freight Co., Ltd. (Thailand)
Nova - Stark Shipping (Ukraine)
Ransomhub - Jindal Group (India)
Ragroup - SK Gas (Korea)
Rhysida - Furuno USA (USA)
Safepay - Bannenberg & Rowell (UK)
Securotrop - Mill Bay Marine Group (Canada)
Sinobi - Quality Companies (USA)
Team XXX - Narvik Havn (Norway)
Thegentlemen - 2GO Group (Philippines)
Unknown - NORMA Cyber member (Norway)
Warlock - Ferus Smit (Netherland)
Worldleaks - Nuclebrás Equipamentos Pesados (Brazil)

Clop

Fleet Management Limited (Hong Kong)
Helix ESG (USA)
Kirby Corporation (USA)
Sea Jet (Greece)

Qilin

Atlantis Submarines (Barbados)
Brodosplit (Croatia)
Buffalo Marine Service, Inc. (USA)
Haeger & Schmidt Logistics (Germany)
Malibu Boats Australia (Australia)
Marine Turbine Technologies (USA)
Montship (Canada)



Akira

Ab Ovo (Netherland)
Del Corona & Scardigli Canada (Canada)
Extend AS (Norway)
Ghent Dredging (Belgium)
Keystone Shipping (USA)
Møre Maritime AS (Norway)
Multilift Logistic Group (Singapore)
Stratascorp Technologies (USA)
TOP Ships Inc (Greece)
TOP Ships Inc (Greece)
Watermark Marine Systems (USA)

Play

Anchor Industries (USA)
Bluewater Yacht Sales (USA)
Energy Fishing and Rental (USA)
Katch Kan (Canada)
Marine Technical Surveyors (USA)
NEAS (Canada)

Maritime sårbarheter

Antallet rapporterte maritime sårbarheter vil sannsynlig øke i 2026, men sannsynligheten for utbredt utnyttelse forblir lav. Denne utviklingen indikerer ikke nødvendigvis flere usikre systemer, men reflekterer en overgang fra «security by obscurity» til mer proaktiv sikkerhetsforskning, drevet av regulatorisk press. Sårbarhetsbildet i maritim sektor vil sannsynlig bli stadig mer komplekst.

Det er sannsynlig at leverandører vil bidra til et økende antall publiserte sårbarheter i 2026. Sikkerhetsforskning innen operasjonell teknologi vokser betydelig, og flere leverandører og forskere identifiserer og offentliggjør sårbarheter på en ansvarlig måte. Nye regulatoriske krav, inkludert krav spesifikke for maritim sektor, presser leverandører til å etablere transparente prosesser for sårbarhetshåndtering. Viktigheten av risikobasert sårbarhetsstyring vil meget sannsynlig øke, inkludert evnen til å identifisere og prioritere sårbarheter basert på reell risiko.

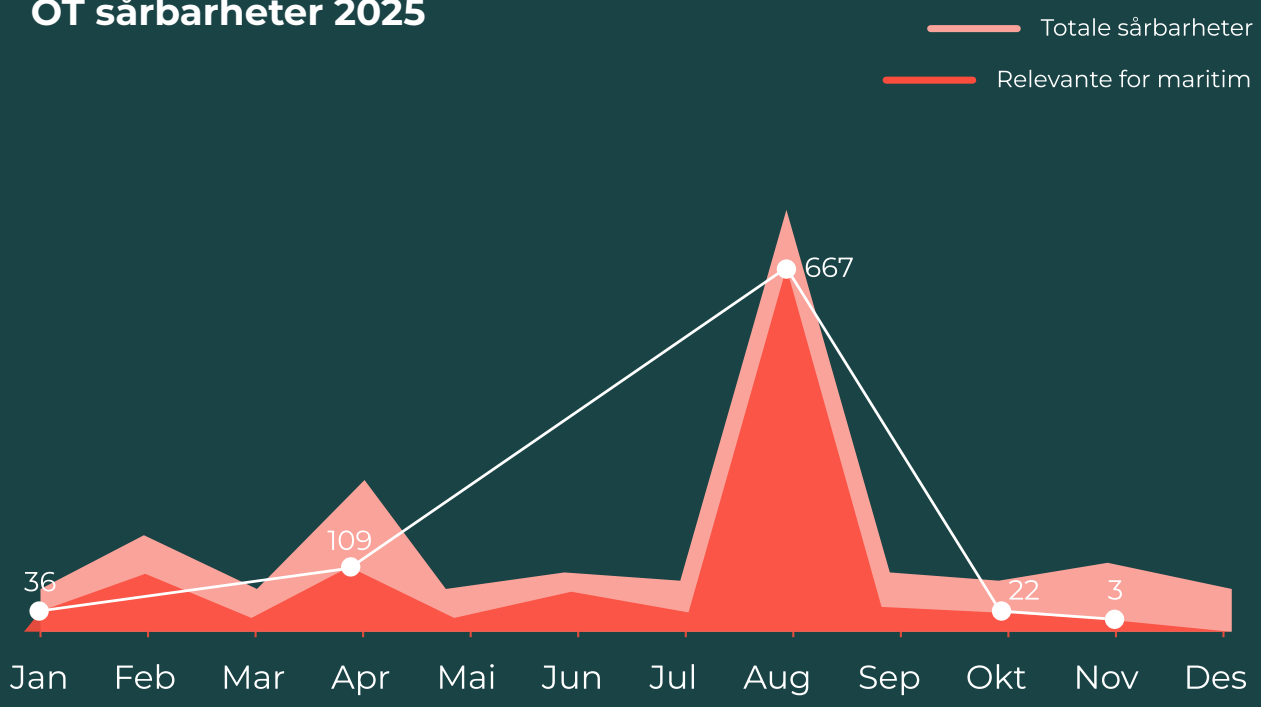
Sårbarheter i maritim operasjonell teknologi.
I 2025 ble 1 122 sårbarheter (CVE-er) vurdert å påvirke maritim operasjonell teknologi, hvorav de fleste ble klassifisert som høy eller kritisk. Dette inkluderer utstyr sertifisert for bruk ombord. To av sårbarhetene var klassifisert som kjente, aktivt utnyttede sårbarheter, men det foreligger ingen rapporter om at disse er brukt spesifikt mot maritimt utstyr. Antallet sårbarheter som påvirker maritimt utstyr vil meget sannsynlig fortsette å øke årlig i takt med økt digitalisering og innføring av nye prosesser for ansvarlig offentliggjøring hos maritime leverandører. Vellykket utnyttelse av sårbarheter i maritim OT forblir imidlertid lite sannsynlig.

Andre sårbarheter og svakheter
Gjennom penetrasjonstester og sikkerhetsvurderinger ombord på ulike fartøy er det identifisert ytterligere sårbarheter og svakheter som ikke er offentlig kjent eller tildelt CVE. Disse knytter seg ofte til usikre designvalg og svake sikkerhetsarkitekturer som oppstår ved ettermontering av ny teknologi, og som utilsiktet kan eksponere kritiske systemer for økt risiko. Siden cybersikkerhet i maritim sektor i stor grad er etterlevelsesdrevet, oppstår slike risikoer ofte når ikke-kritiske støttesystemer med få sikkerhetskrav kobles til kritiske systemer med formål som blant annet datainnsamling til sky. Andre svakheter oppstår når midlertidige løsninger blir permanente. Eksempler inkluderer mobilmodemer brukt for fjernaksess, Wi-Fi-tilkobling i kontrollsystemer og bruk av uadministrerte bærbare service-PC-er. Disse sårbarhetene og svake arkitekturene understreker behovet for proaktive sikkerhetsprogrammer som går utover ren regelverksetterlevelse. Denne trenden vil sannsynlig fortsette og særlig påvirke virksomheter med lav sikkerhetsmodenhet.

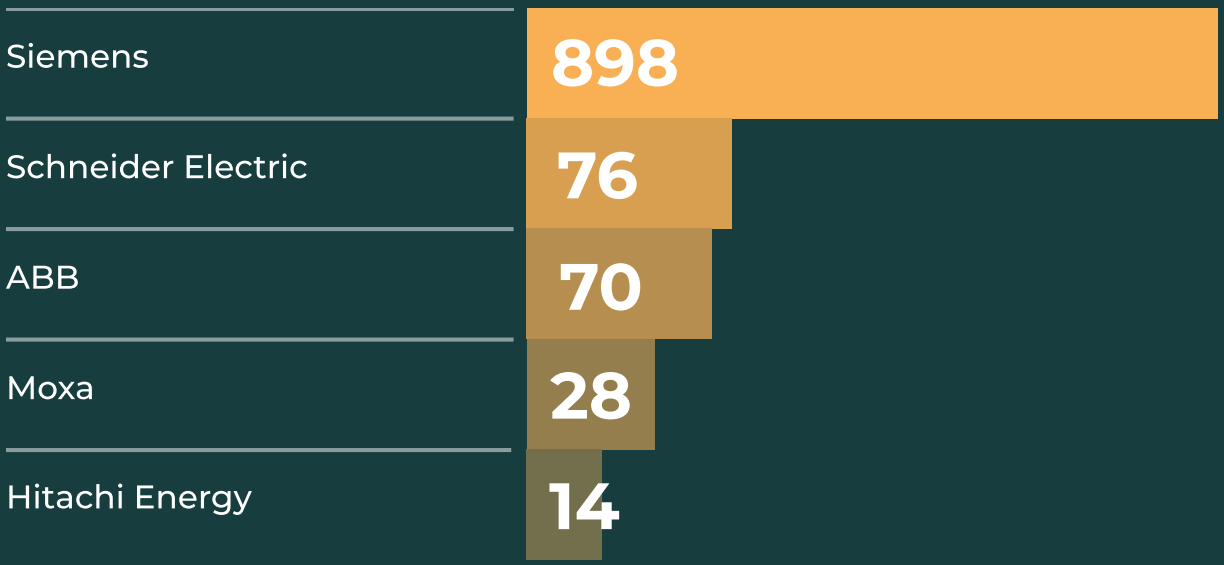
IT-sårbarheter med OT-påvirkning
Grensebeskyttelsesenheter som skal sikre IT- og OT-nettverk ombord, er ofte utilstrekkelig beskyttet. I løpet av 2025 ble det rapportert flere alvorlige sårbarheter i sikkerhetsprodukter som brannmurer, VPN-løsninger, fjernaksessløsninger og kantservere. Slike enheter er avgjørende for å etablere sikre grenser mellom ulike nettverk, inkludert mellom IT- og OT-nettverk.
En gjennomgående utfordring er at flere leverandører installerer slike løsninger uten tydelig ansvarsfordeling, noe som fører til manglende oppdateringer. Resultatet er at enheter som utgjør hovedbarrieren mellom IT og OT ofte har flere kritiske sårbarheter, hvorav noen også kan være aktivt utnyttet av trusselaktører. Disse sårbarhetene vil meget sannsynlig fortsette å representere de mest kritiske risikoene for maritim OT, gitt deres eksponering mot IT-nettverk kombinert med den tilgangen til OT-miljøet som kan oppnås ved vellykket utnyttelse.

> I 2025 var 53 % av sårbarhetene som berørte operasjonell teknologi (OT), gjeldende for maritim sektor.

OT sårbarheter 2025



Topp 5 leverandører med CVEer



NORMA Cyber har nå mer enn **170 medlemmer**, representert med over **3 000 fartøy** og offshore-enheter.

Om oss

Nordic Maritime Cyber Resilience Centre

NORMA Cyber tilbyr et medlemskapsmodell som inkluderer kritiske cybersikkerhetsfunksjoner og tjenester for maritime organisasjoner. Med et non-profit-oppsett er vårt overordnede mål å finne synergier og kostnadseffektive løsninger, som bidrar til at medlemmene våre er så sikre og robuste som mulig. Vi arrangerer også arrangementer der medlemmer og partnere kan møtes for å dele beste praksis og finne felles løsninger.

Milepæler 2025

Penetrasjonstesting og OT Sikkerhetsvurdering

NORMA Cyber tilbyr nå Penetrasjonstesting og OT Sikkerhetsvurdering som fullverdige tilleggstjenester til våre medlemmer.

Intel Rapporter og Webinarer

NORMA Cyber har publisert over 40+ rapporter og holdt 14 webinarer for våre medlemmer.

Medlemsportal

NORMA Cyber har utviklet og lansert en ny medlemsportal.

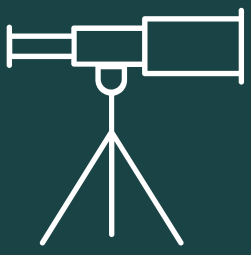
Vårkonferanse Oslo

140+ medlemmer deltok i Oslo, April 2025

Medlemsråd Gøteborg

50+ medlemmer deltok i Gøteborg, Sept. 2025

Våre Tjenester



Trusseletterretning

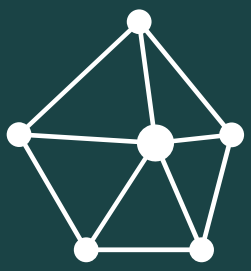
Fortløpende informasjonsdeling av etterretning, sårbarhetsvarsler, og råd om reduserende tiltak

Hendelse- og krisehåndtering

24/7, 365 dager i året beredskap for hendelses- og krisehåndtering for angrep mot fartøy IT, fartøy OT, landbasert IT og skysystemer.

Ekstern monitorering

Monitorering av det dype/mørke nettet, med varsling til medlemmer når sårbarheter eller eksponering er detektert.

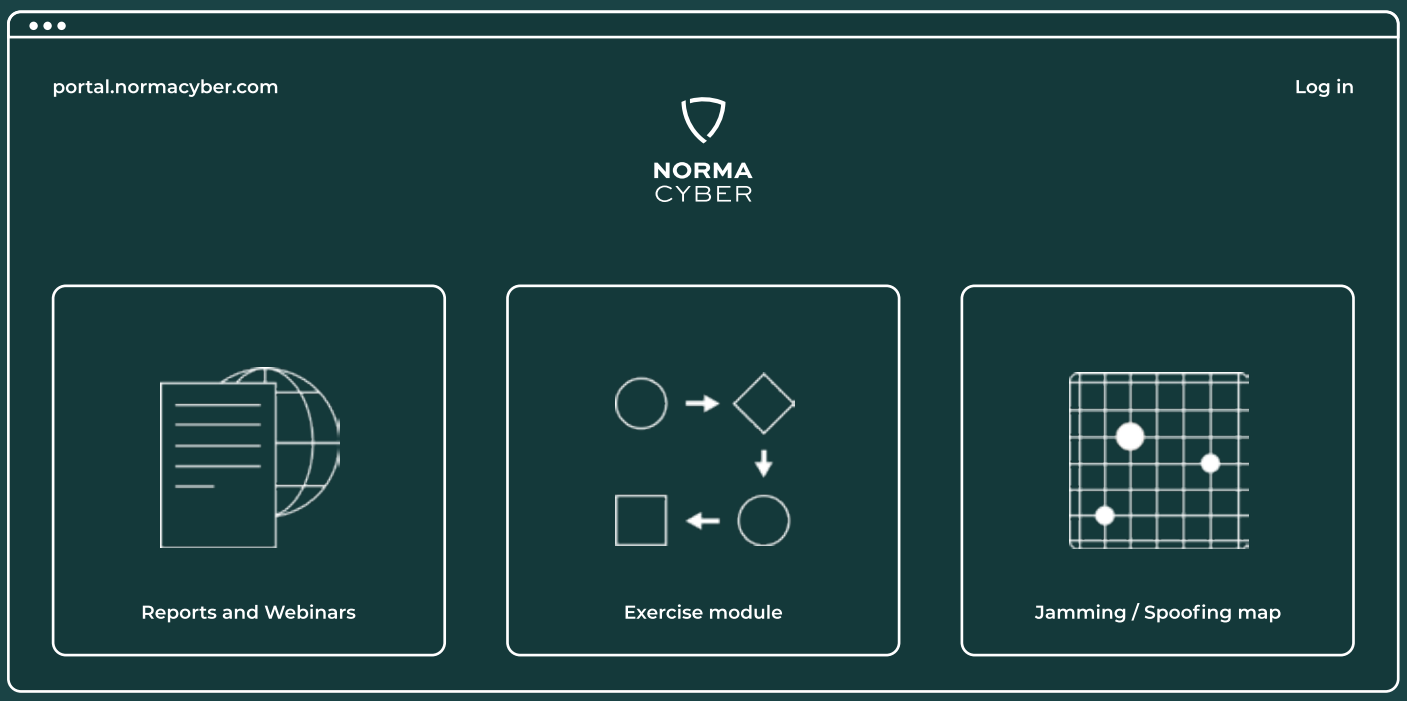


Nettverk

Et samarbeidsnettverk av medlemmer og partnere for å dele kunnskap, samt drive innovasjon og erfaringsutveksling igjennom sammenkomster og tilgang til NORMA Cyber medlemsråd.

For full oversikt over tjenestene,
vennligst besøk normacyber.no/services

NORMA cyber Medlemsportal



Alle medlemmer får ekslusiv tilgang til vår medlemsportal på portal.normacyber.no

Threat Intelligence

- Månedlige trusselvurderinger
- Etterretningsrapporter
- Maritime OT - sårbarhetsvarsler
- Informasjonsdeling av tekniske indikatorer (gjennom MISP)

Ekstern monitorering

- Monitorering av det dype/mørke nettet
- Sårbarhetskan av internetteksponerte tjenester
- Attack Surface Management
- Fortløpende varsling til medlemmer som blir påvirket

Hendelse- og krisehåndtering

- 24/7, 365 dager hendelses- og krisehåndtering
- IT og OT ombord fartøy
- Landbasert IT og skysystemer
- Teknisk støtte og hjelp til ressurshåndtering
- Cyber security øvelser

Nettverk

- Konferanse og medlemsråd
- Bli en del av vårt nettverk av medlemmer og partnere
- Kompetanse- og kunnskapsdeling gjennom forum

Sikkerhetsmonitoreringstjeneste

Hva vi gjør

NORMA Cyber tilbyr sikkerhetsmonitoreringstjeneste (SOC) som en tilleggstjeneste til våre medlemmer. SOCen monitorerer medlemmers systemer 24/7 og utfører analyser, responderer på avvik og varsler medlemmer når hendelser oppdages. .

Vår SOC-filosofi

Agnostisk tilnærming til teknologi og leverandører: Vi kan integrere mot de fleste maritime og kommersielle systemer. Det vil normalt ikke være behov for hardware installasjoner. Ei heller vil det være begrenset til særlig typer brannmurer, anomalibasert antivirus eller svitsjer.

Nøytralitet: Vi har objektivt blikk på infrastrukturen. SOCen gir råd på månedlig basis for å forbedre sikkerheten til medlemmet.

Kompetanse: Vi forstår det maritime landskapet og alle kompleksitetene i næringen.

Synergier: Kunnskapen vi får fra å overvåke flere ulike maritime virksomheter gir oss en unik innsikt. Anonymisert innhold deles tilbake til medlemmer.

Teknisk oppsett

- Oppsettet er fleksibelt og omfanget varierer fra IT og OT ombord til landinfrastruktur og/eller skymiljø.
- Vi benytter de aller nyeste SOC systemer og benytter KI for å redusere falske positive.
- Vi automatiserer så mye som mulig for å øke hastigheten i respons og rapportering.
- Manuell analyse og oppfølging av komplekse saker.
- Vi kan tilby automatisk respons for IT/ skytjenester ved bruk av vårt SOAR system
- Det gjennomføres proaktiv jakt på ondsinnet aktivitet for å oppdage skjulte og avanserte trusler

Nøkkelfunksjoner

- ✓ 24/7 monitorering
- ✓ Hendelseshåndtering
- ✓ Proaktiv jakt på ondsinnet aktivitet/datatrusler
- ✓ Måndelig rapportering med råd
- ✓ Automatisk respons (SOAR) for IT-relaterte plattformer

NORMA Cybers SOC tjeneste

Foretaks-SOC tjenester (IT & Sky)

Utviklet for virksomheter med store flåter og deres behov for sikkerhet i IT infrastruktur på tvers av land og flåte

Funksjon	Detaljer
Omfang	IT på fartøy, landbasert IT, Skytjenester
Forhåndskrav	Ingen, format-tolkere av forskjellige logger er tilgjengelig
Ekstern Implementering	Ja
Deteksjonskapasitet	Regelstyrt, MISP-integrasjon, KI-drevet grunnlinje og deteksjon

Fartøy SOC tjenester

Skreddersydd for maritimt miljø hvor det er begrenset/variabel båndbredde og spesifikke sikkerhetskrav.

Fartøy Tier 1: Kun Brannmurlogger

Funksjon	Detaljer
Omfang	IT på fartøy
Forhåndskrav	Ingen, alle brannmurlogger søttes (krever at brannmur eksporterer systemlogger)
Ekstern Implementering	Ja
Deteksjonskapasitet	Regelstyrt, MISP-integrasjon

Fartøy Tier 2: Mange loggtyper

Funksjon	Detaljer
Omfang	Brannmurlogger, EDR, 0365, epost, og andre typer logger
Forhåndskrav	Ingen, alle brannmur og EDR leverandører støttes (EDR leverandør må eksportere data)
Ekstern Implementering	Ja
Deteksjonskapasitet	Regelstyrt, MISP-integrasjon, KI-drevet grunnlinje og deteksjon

SOC tjeneste for OT på fartøy

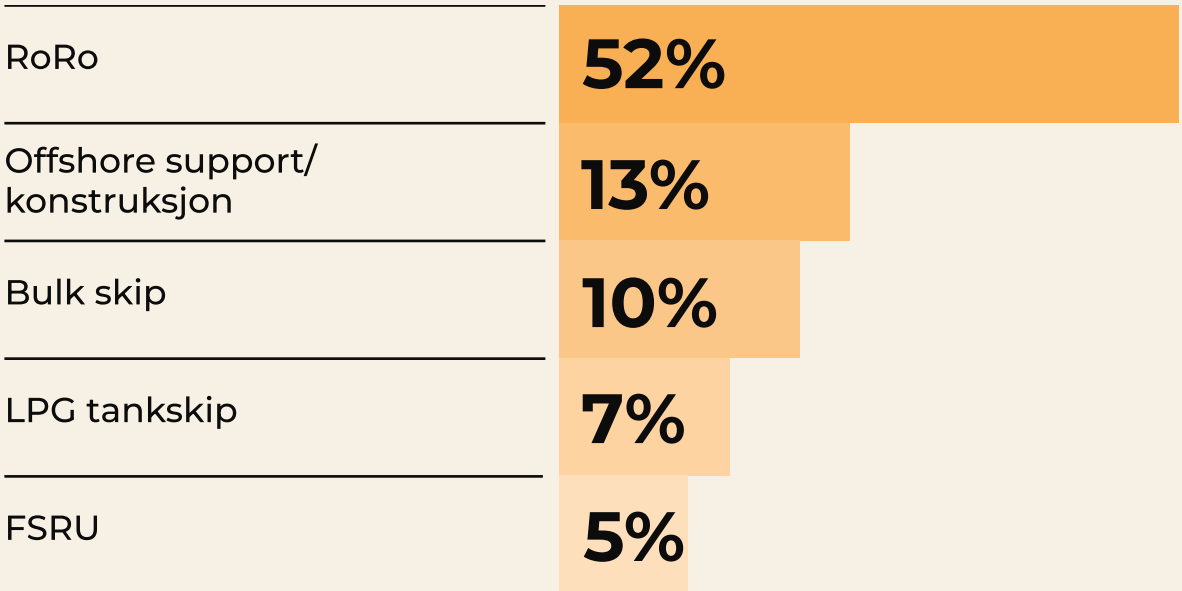
Vårt SOC team monitorerer flere fartøys OT nettverk. Gjennom våre løsninger evner vi å identifisere eiendeler og skape detaljerte lister over digitalt utstyr og identifisere sårbarheter og kontinuerlig vurdere risiko. Tjenestene inkluderer deteksjon av anamalier og trusler og vil agere på varsler og utføre kriminalteknisk analyse av hendelser.

Fartøy Tier 3: OT nettverksovervåkning

Funksjon	Detaljer
Omfang	OT på fartøy
Forhåndskrav	Ingen, kan fungere alene eller i kombinasjon med Tier 1/2
Ekstern Implementering	Ja
Deteksjonskapasitet	KI-drevet grunnlinje og deteksjon, regelstyrt monitorering
Ekstra Fordeler	Eiendelsliste av OT nettverk, sårbarhetsadministrasjon

SOC-medlemmer sortert etter fartøytype

De fem mest vanlige typene av totalt antall fartøy




NORM
CYBE

Penetrasjonstesting og OT sikkerhetsvurdering

NORMA Cyber tilbyr nå penetrasjonstesting og OT sikkerhetsvurderinger som en tilleggstjeneste til våre medlemmer.

NORMA Cyber skreddersyr sikkerhetstesting for fartøyteknologi. En penetrasjonstesting tilpasset fartøy og maritime organisasjoner som ønsker å vurdere cybersikkerhetstilstanden i sin IT-infrastruktur om bord.

Målet er å simulere realistiske angrepsscenarioer, identifisere sårbarheter og evaluere interne nettverkskontroller – med fokus på skillet mellom informasjonsteknologi (IT) og operasjonell teknologi (OT).

Gjennom en OT-sikkerhetsvurdering har NORMA Cyber-teamet som mål å identifisere all operasjonell teknologi om bord. Ved å gå fysisk om bord for inspeksjoner får vi praktisk erfaring som kombineres med en grundig gjennomgang av skipets dokumentasjon.

I denne tjenesten benytter NORMA både maritim og teknisk kompetanse for å gi en oppdatert status over fartøyets systemer, inkludert potensielle svakheter og sårbarheter.

	IT penetrasjonstesting av fartøy	**OT Sikkerhetsvurdering av fartøy**
Hensikt	Identifisere og validere sårbarheter som kan utnyttes i fartøyets IT infrastruktur	Evaluering av sikkerhetsnivået og robustheten til operasjonell teknologi (OT) systemer ombord
Omfang	**Testområder:** • Nettverk og trådløs testing • Testing av påloggingsinformasjon og tilgang • System og enhetsintegrasjon • Sosial manipulering (tilvalg) **Tre angrep-scenario for å simulere forskjellige nivå av angriper:** 1. Gjestenettverk (ikke-autentisert angriper) 2. IT nettverk tilgang (uten påloggingsinformasjon) 3. IT nettverk tilgang (med påloggingsinformasjon) Hovedfokus: IT/OT nettverk segmentering og soneintegritet	**Hovedmål:** • Identifisere koblinger mellom IT og OT • Identifisere udokumenterte komponenter og systemer • Prioritere systemer av høy relevans for Cybersikkerhet **Identifisere:** • Kritiske systemer • Avhengigheter på tvers av systemer og nøkkelkomponenter • Svakheter og sårbarheter i systemarkitekturen • Avvik fra dokumentasjon
Tidslinje	To konsulenter ombord i to dager	To konsulenter ombord i to dager

Offentlig-Privat samarbeid innen cybersikkerhet i Norge

Sektorvis responsmiljø for den norske maritime sektoren
I 2023 ga Nærings- og fiskeridepartementet Kystverket i oppdrag å etablere en sektorvis responsmiljø (SRM) for den norske maritime næringen. Kystverket samarbeider med Sjøfartsdirektoratet om dette oppdraget.

I januar 2024 ble det inngått en avtale mellom Kystverket og NORMA Cyber, der sistnevnte skal bistå med teknisk ekspertise og andre ressurser for å operasjonalisere og støtte Kystverket i SRM oppdraget.

NORMA Cyber deler relevante og tidskritiske sårbarhetsvarsler med den maritime sektoren og bidra til åpenhet og informasjonsdeling om cybersikkerhetshendelser. Videre fungerer NORMA Cyber som et rådgivende organ ved hendelses- og krisehåndtering, samt bidrar med varsler og rapporter.

Om sektorvis responsmiljø (SRM) i Norge
Norge har et sektorfokusert beredskapsoppsett for digitale kriser. Dette betyr at hver sektor har ansvar for å etablere og opprettholde nødvendige informasjonsdelings- og responsfunksjoner. SRMene er ansvarlig for koordinering mellom aktørene i respektive sektor(er) og til Nasjonal Sikkerhetsmyndighet (NSM) og Nasjonalt cybersikkerhetssenter (NCSC). Detaljer om hvordan dette systemet fungerer og hvem som har hvilke roller, er beskrevet i dokumentet “Rammeverk for håndtering av IKT-sikkerhetshendelser” fra NSM.

Eksempler på hvordan sektorvis responsmiljø er organisert i andre sektorer i Norge, som har vært modeller for oppsettet i den maritime næringen:

- **For finanssektoren** er Finanstilsynet overordnet ansvarlig, mens de operative aspektene håndteres av Nordic Financial CERT (NF-CERT).

- **For energisektoren** er Norges vassdrags- og energidirektorat (NVE) og Havindustritilsynet (Havtil) overordnet ansvarlig, mens de operative aspektene håndteres av KraftCERT/InfraCERT..

Sjøfartsdirektoratet
Norwegian Maritime Authority

KYSTVERKET

NORMA CYBER

Deling av informasjon om cyberhendelser

Deling av informasjon om cybersikkerhet er essensielt for et kollektivt forsvar og styrking av cybersikkerheten i den maritime sektoren. NORMA Cyber oppfordrer våre medlemmer til å dele informasjon om cyberrelaterte hendelser som kan bidra til å begrense eksisterende eller fremtidige cybersikkerhetstrusler. Dette inkluderer hendelser relatert til SATCOM, AIS og GNSS-forstyrrelser. Sammen er vi sterkere!

Når cyberhendelser rapporteres raskt, kan NORMA Cyber bruke informasjonen til å yte bistand og sende ut varsler for å forhindre at andre medlemmer eller aktører blir offer for lignende angrep. Tilgang til informasjon er avgjørende for å identifisere trender som kan redusere trusselen mot våre medlemmer, minimere potensielle konsekvenser og forebygge angrep i den maritime sektoren generelt.

Typer aktiviteter du bør dele:

- Uautorisert tilgang til systemet ditt
- Tjenestenektangrep (DoS) som varer i mer enn 12 timer
- Skadevare oppdaget i systemene dine
- Målrettede og gjentatte skanninger mot tjenester i systemene dine
- Gjentatte forsøk på å oppnå uautorisert tilgang til systemet ditt
- E-post, mobil- eller SATCOM-meldinger knyttet til phishing
- Alle typer forstyrrelser, GNSS, AIS, SATCOM, spoofing eller jamming

Behov for assistanse?

Vi oppfordrer deg til å sende en e-post til **ops@normacyber.no** og være så detaljert som mulig. Inkluder kontaktinformasjon slik at vi kan nå deg for å iverksette nødvendige tiltak raskt og effektivt.

GNSS Jamming / Spoofing

Send en epost til **ops@normacyber.no**

Rapportering til myndigheter

Deling av informasjon med NORMA Cyber erstatter ikke lovpålagt rapportering til myndighetene, for eksempel flaggstat, kyststat eller politi. Vi oppfordrer alltid våre medlemmer til å anmelde cyberkriminalitet eller svindel til politiet når man blir utsatt for slike hendelser.

Dersom du har behov for øyeblikkelig hjelp eller er i en nødsituasjon, ring vårt nødnummer: **+47 90 98 97 37**

Samlet motstandskraft mot cybertrusler for nordisk maritim næring