

Att.: Nærings – og fiskeridepartementet  
Kongens gate 8  
Oslo

## Innspillsmøte | Sjøfartsdirektoratet onsdag 29.10.2019

Vi lever i en verden som er mer ustabil og uforutsigbar enn på lenge. Russland sitt forhold til Vesten, Brexit og USA sin president er stikkord som har vært med på å endre de sikkerhetspolitiske omgivelsene de senere årene.

I denne sikkerhetspolitiske turbulensen, peker trusselvurderinger fra PST, NSM og Etterretningstjenesten alle på Nettverksoperasjoner, Cybertrusselen, som en av de største og vedvarende truslene mot norske verdier i dag.

I følge Etterretningstjenesten er det spesielt tre utviklingstrekk som utmerker seg innen nettverksoperasjoner. Dette er utnyttelse av tredjeparts infrastruktur, nettverksoperasjoner med sabotasjeformål og bruk av krypteringsvirus til økonomisk utpressing.

Som et eksempel kan vi trekke frem cyberangrepet mot Norsk Hydro, som lammet bedriften i mange måneder, med driftsavbrudd og tap i hundre millioners klassen som konsekvens. Maersk i Danmark beregnet at de hadde mellom 1,6 og 2 milliarder danske kroner i omsetningstap som resultat av et cyberangrep i 2017.

I maritim sektor ser man en overvekt av trusler i form av innblanding i navigeringssystemer og fjernstyrte prosesser. Russland driver jevnlig med GPS forstyrrelser som rammer både luftfart og skipsfart, særlig i nordområdene.

I Rederiforbundets årlige konjunkturundersøkelse i 2018 ble cyberangrep rangert som den største trusselen for drift av skip, foran både terror og piratvirksomhet. NSM har registrert flere målrettede cyberangrep mot maritim sektor, og kom senest i august i år med en rekke forslag til tiltak og forhåndsregler til rederier og fartøy. Flere av disse tiltakene er grunnleggende for at sikkerheten skal ivaretas hos de maritime aktørene.

I regjeringens maritime strategi fra 2015 står det svært lite om datasikkerhet. I Havstrategien som kom i juni i år er det fokus på digitalisering, automatisering og bruk av grønn teknologi, men også her er det viet liten plass til viktigheten av datasikkerhet. Med dagens trusselbilde som bakteppe mener vi dette er uheldig.

I maritim sektor har man i dag høy teknologisk utvikling. Dagens moderne fartøy blir stadig mer digitaliserte, og teknologien er også med på å sikre en grønnere skipsfart. Autonome fartøy vil måtte utstyres med robuste, pålitelige og sikre systemer for å kompensere for at mennesket er fjernet fra førstelinje om bord. Cyberkriminalitet vil bli en stadig mer relevant problemstilling etter hvert som flere virksomheter tar i bruk digitaliserte, og automatiserte tjenester.



EMP Secure leverer og drifter komplekse IT- og sikkerhetsløsninger på skip over hele verden. Vår erfaring er at konkrete tiltak knyttet til datasikkerhet må være på plass, både på skip og på rederienes landbaserte infrastruktur, for å sikre stabil, sikker og forutsigbar drift.

Den internasjonale maritime organisasjonen IMO har uttalt at den maritime bransjen må komme med gode løsninger for cybersikkerhet innen 1. januar 2021.

I forbindelse med ny maritim stortingsmelding er vårt innspill at det må legges større vekt på viktigheten av datasikkerhet for næringen. Dette mener vi er helt essensielt for å gjennomføre og oppnå en sikker og effektiv digitalisering, og bidra til viktige konkurransefortrinn i den maritime næringen i årene som kommer.