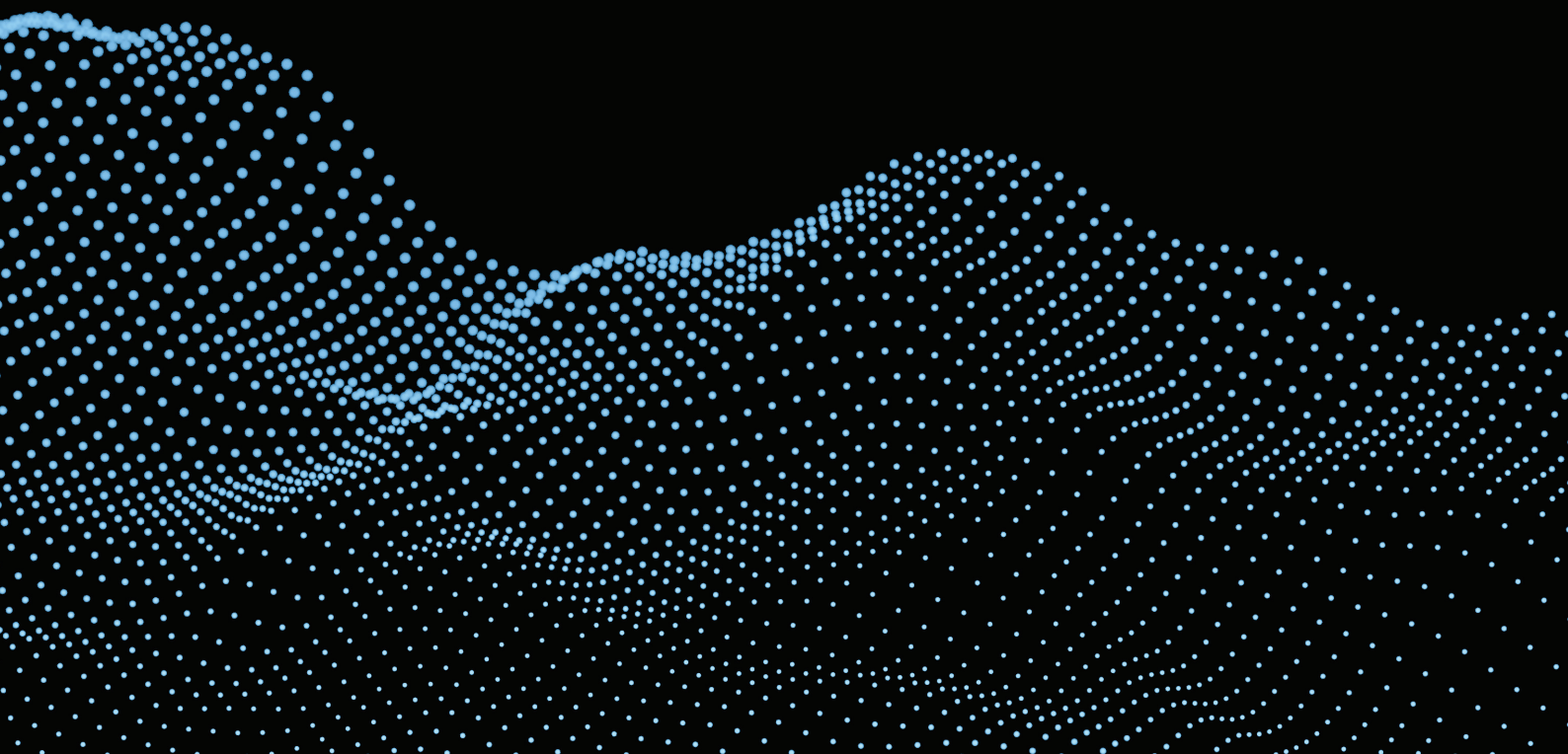
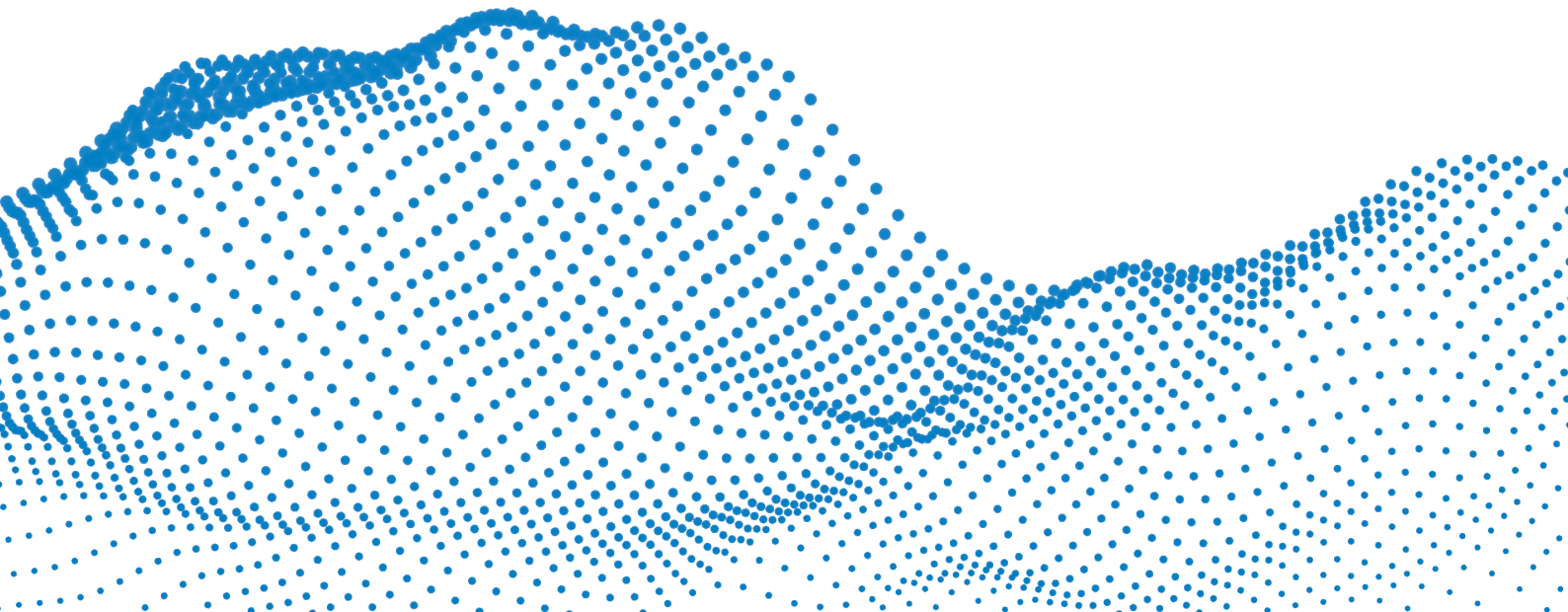
Whitepaper

Hybride trusler kræver hybride løsninger

Et whitepaper om beskyttelse af kritisk maritim infrastruktur





Executive Summary

Danmark står over for et mere komplekst og udfordrende trusselsbillede, hvor kritisk maritim infrastruktur i stigende grad er mål for hybride angreb.

Samtidig er afhængigheden af denne maritime kritiske infrastruktur vokset markant. Beskyttelsesniveauet har dog ikke fulgt med denne udvikling, og evnen til at opdage og reagere rettidigt er i dag utilstrækkelig.

Whitepaperet peger på, at en effektiv beskyttelse kræver en balanceret og risikobaseret tilgang. Skader på undersøisk infrastruktur skyldes ofte utilsigtede hændelser, men risikoen for bevidste angreb er stigende. Løsningen er derfor at styrke robustheden gennem målrettede investeringer og bedre udnyttelse af eksisterende kapaciteter.

Kernen i løsningen er et tættere samarbejde mellem staten og industrien. Vi kalder dette samarbejde for "Den Hybride Koalition". "Hybrid", fordi samarbejdet rummer både statslige myndigheder og private aktører. "Koalition", fordi aktørerne hver især er uundværlige dele af løsningen på et fælles problem. Staten har ansvaret for overvågning, efterretning, afskrækkelse og magtanvendelse, mens private aktører besidder væsentlige kapaciteter inden for overvågning, tilstedeværelse, førsteindsats og reparation. Disse kapaciteter skal i højere grad bringes i spil for at skabe et samlet og effektivt beredskab.

Rapporten identificerer tre centrale indsatsområder: realtidsbaseret overvågning, effektiv operativ respons og hurtig mitigering af konsekvenser. På kort sigt anbefales det at styrke overvågningen gennem pilotprojekter og datadeling, etablere klare kontaktpunkter til myndighederne og indføre mere omfattende forbudszoner omkring kritisk infrastruktur. På længere sigt bør der udvikles en national doktrin, etableres et integreret overvågningssystem og opbygges en styrket maritim responskapacitet.

Konklusionen er, at Danmark allerede har et velfungerende udgangspunkt, men at beskyttelsen skal løftes gennem et tættere og mere struktureret samarbejde mellem offentlige og private aktører. Ved at bygge videre på eksisterende styrker og bringe industrien mere systematisk i spil kan Danmark markant styrke sin modstandskraft mod hybride trusler.

Hybride løsninger på hybride trusler

Havet omkring Danmark er i bevægelse. En analyse fra 2025 fra Center for Militære Studier understreger, at den strategiske betydning af havbunden er vokset. Undervandskabler, rørledninger og energiforbindelser er afgørende for energiforsyning, digitalisering, økonomisk udvikling, klimaindsatser, miljøbeskyttelse, sikkerhed og nationalt forsvar. [1]

Samtidig er grænserne mellem fred, krise og konflikt blevet flydende, og under havets overflade lurer nye trusler, der udfordrer Danmarks sikkerhed. Siden sprængningerne af Nord Stream-rørledningerne i september 2022 er det blevet stadigt tydeligere, at Østersøen udgør en frontlinje i den hybride krig, som Forsvarets Efterretningstjeneste vurderer, at Rusland fører mod NATO. Og det er meget sandsynligt, at den hybride trussel fra Rusland vil stige de kommende år, hvis vi ikke reagerer.

Kritisk maritim infrastruktur er ofte relativt ubeskyttet, dels på grund af de fredstidsbetingelser, vi har levet under, dels fordi infrastrukturen generelt er vanskeligt tilgængelig. Den tid er forbi. Vores modstandere har investeret kraftigt i kapaciteter til at kortlægge, overvåge og angribe og har viljen til at bruge dem. Men vi har ikke fulgt med i nær den samme grad. Vores evne til at holde øje med, hvad der sker på og under havets overflade og på havbunden lader noget tilbage at ønske. Det betyder, at den kritiske maritime infrastruktur er tilgængelig for vores modstandere, uden at vi er i stand til at opdage hybride aktiviteter og angreb i tide.

Vi er derfor nødt til at reagere. Vi skal begrænse muligheden for, at angribere kan gennemføre succesfulde hybride angreb mod vores kritiske maritime infrastruktur. Teknologierne eksisterer, og Danmark har nationale aktører, der er i stand til og villige til at bringe dem frem, men opgaven er så kompleks, at staten og private aktører skal skabe løsningerne i et tæt samspil for at forbedre overvågning og respons.

Danske virksomheder er klar til, sammen med staten, at styrke beskyttelsen af Danmarks kritiske maritime infrastruktur. I dette whitepaper giver vi vores bud på, hvordan det kan ske i praksis.

Bedre beskyttelse kræver styrket overvågning, respons og mitigering

Anvendelsen af hybride virkemidler udnytter et grundvilkår i det moderne samfund: at det ofte er vanskeligt entydigt at skelne mellem uheld, tilfældigheder og bevidste fjendtlige handlinger.

Angriberen har fordelen og har mulighed for at operere i det skjulte før, under og efter en aktion. Det gør det vanskeligt at tilskrive en hændelse til en konkret aktør. Samtidig kan angriberen udnytte *plausible deniability* til at undgå politiske og juridiske konsekvenser. Hvis skaderne ikke hurtigt kan afdækkes og afhjælpes, vil det medføre betydelige fysiske og psykologiske virkninger.

Det er imidlertid vigtigt at fastholde et nuanceret risikobillede. Skader på undersøisk infrastruktur er ikke et nyt fænomen og skyldes ofte utilsigtede hændelser som ankring, fiskeri, slid eller ændringer i havbunden.

Selvom risikoen for sabotage og hybride handlinger er reel og stigende, udgør disse fortsat kun en del af det samlede trusselsbillede. En effektiv beskyttelse for- udsætter derfor, at indsatsen baseres på en fakta- og risikobaseret tilgang, hvor både utilsigtede hændelser og bevidste angreb håndteres proportionelt. Ellers risikerer vi at træffe beslutninger, der er drevet af usikkerhed frem for et retvisende billede af truslerne.

At øge beskyttelsen af kritisk maritim infrastruktur mod hybride angreb kræver robuste kapaciteter på disse tre konkrete områder:

- Overvågning i realtid
- Operativ respons
- Hurtig mitigering af konsekvenser

De tre dele af opgaven er for omfattende og komplekse til, at de kan løses af de enkelte private ejere, operatører og leverandører alene.

1. Havbundens strategiske betydning. Muligheder og udfordringer for Forsvaret. Tobias Liebetrau, Københavns Universitet, Center for Militære Studier, September 2025

De gensidige afhængigheder mellem private og staten er for store, og derfor kan problemet kun løses i et tæt og omfattende samarbejde.

Ejere, operatører, leverandører og staten har hver især vigtige og nødvendige kapaciteter, kompetencer, ressourcer, teknologier og mandater, som vil give en langt større effekt, hvis de indgår i en samlet, fælles indsats for at beskytte vores kritiske maritime infrastruktur. Opgavens omfang betyder, at graden af overvågning, respons og mitigering skal afhænge af infrastrukturens samfundskritiske betydning.

For at løse opgaven skal rollerne også være klare. Staten foretager den nationale overvågning, efterretningsindhentning, militær afskrækkelse og i sidste ende magtanvendelsen. Det er således også statens ansvar at have det samlede overblik. Private aktører kan dog bidrage til opgaven ved at levere datakilder til at etablere et retvisende normalbillede.

Private kapaciteter har også potentialet til at afskrække fjendtligtsindede handlinger. Ved synlighed og dokumentationsevne øges risikoen for at blive opdaget, og gennem evnen til hurtig genopretning mindskes fjendens gevinster ved angrebet, dermed bliver angrebet mindre attraktivt for modstanderen. Afskrækkelsen forudsætter, at ansvar følger ejerskab. Ejere og operatører af kritisk maritim infrastruktur bør mødes med klare og ensartede krav til overvågning, beredskab, datadeling og reparationskapacitet.

Tydelige rammer vil ikke alene styrke den samlede beskyttelse, men også skabe forudsigelighed for industrien og sikre, at eksisterende kapaciteter udnyttes bedst muligt i samspillet med staten.

Danske virksomheder har verdensførende teknologier, som vi skal bruge til at løse disse opgaver. Nedenfor giver vi eksempler på, hvordan danske virksomheder vil kunne bidrage til gavn for Danmarks nationale sikkerhed.

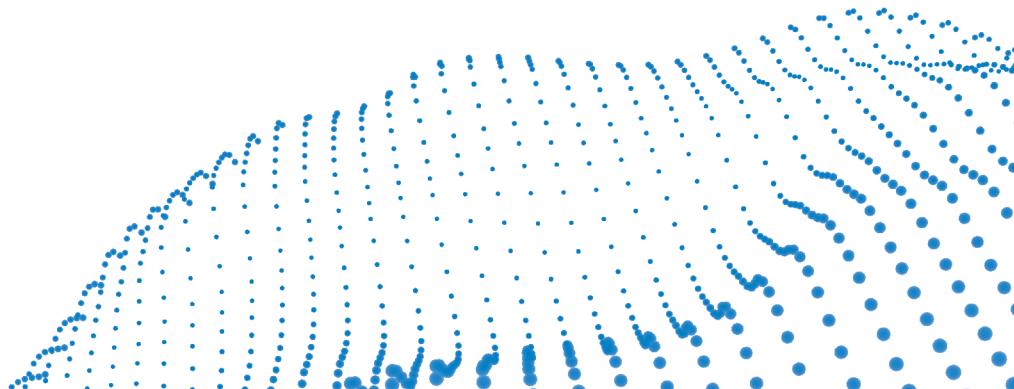
Overvågning i realtid

Overvågning har til formål at etablere et pålideligt normalbillede. Kun derved kan forsøg på uønsket indtrængen, faktisk indtrængen og kritiske hændelser adskilles fra den betydelige mængde legitim aktivitet, der finder sted på havet døgnet rundt. For at understøtte rettidig varsling og en effektiv indsats, er det afgørende, at overvågningen sker i realtid.

En fuldt dækkende overvågning af hele Danmarks søterritorium er imidlertid ikke realistisk. Indsatsen må derfor prioriteres mod de mest kritiske dele af den maritime infrastruktur, hvor skærpet overvågning kan bidrage til at reducere risikoen for hybride aktiviteter og angreb.

Private aktører kan bidrage til at styrke den nationale overvågning ved at udbygge og supplere de eksisterende kilder til dataindhentning, som i dag bl.a. omfatter satellitovervågning, AIS, radar, kameraer og fysiske observationer. Under havoverfladen kan private aktører bidrage med hydrofoner, fiberoptiske kabler med sensing-teknologi, undervandsdroner og dedikerede overfladefartøjer med sonarer til at give os et indblik i, hvad der sker i dybet. Kombinationen af teknologierne kan give et mere detaljeret og retvisende indblik i situationsbilledet på havbunden og i vandsøjlen.

Private aktørers eksisterende systemer og løbende overvågning af installationer kan nyttiggøres i forhold til den samlede overvågning af Danmarks kritiske maritime infrastruktur. Det kan fx ske ved at dele observationer, varsler og alarmer fra egne systemer til myndigheder eller ved at give myndigheder adgang til datafeeds, fx fra kameraer.



Private aktører kan desuden bidrage med systemer, som kan samle og analysere data fra mange forskellige sensorer og præsentere et samlet overblik *(common operational picture)*, som kan understøtte både myndigheders og ejere og operatørers operative opgaveløsning. Eksempelvis kunne det nye situationscenter, der blev oprettet i december 2025 åbne for at kunne gøre nytte af private aktørers systemer til at forbedre myndighedernes situationsforståelse.

Endvidere kan private aktørers søopmålingsdata (bathymetriske data), som allerede indberettes til Geodatastyrelsen, nyttiggøres til at danne et overblik over havbunden, fx som grundlag for et normalbillede.

Effektiv operativ respons

Operativ respons handler om at afværge eller stoppe hybride angreb. Hvis et angreb lykkes, skal vi hurtigt kunne iværksætte tekniske undersøgelser *(forensics)* for at afdække forløbet og identificere angriberen. Det kræver, at aktører med de rette kapaciteter er til stede ved eller i nærheden af den kritiske maritime infrastruktur, og at de har det nødvendige mandat til at gribe ind.

Det er imidlertid kun staten, der har ret til at anvende magt, herunder tilbageholde, afvise, standse eller neutralisere fartøjer, men staten, i form af enheder fra Forsvaret eller politiet, har ikke mulighed for at sikre tilstrækkelig høj tilstedeværelse på egen hånd.

På ethvert givet tidspunkt befinder der sig erhvervsfartøjer på havet omkring Danmark. Nogle af fartøjerne udgør kapaciteter, der kan supplere og dermed forstærke statens tilstedeværelse. Ejeres og operatørers service- og redningsfartøjer, som allerede opererer i områder med kritisk maritim infrastruktur, er eksempler på ressourcer, som i dag ikke udnyttes fuldt ud, men som staten kan bringe i anvendelse. Staten vil i sådanne tilfælde fungere som indsatsleder for både egne og private ressourcer til havs og dermed også have ansvaret for den overordnede koordinering, ligesom ved søredning.

Inddragelse af private maritime kapaciteter i den operative respons rummer et betydeligt potentiale inden for førsteindsats, overvågning, teknisk afklaring og reparation af skader. I mange situationer vil private fartøjer og specialiserede operatører kunne være hurtigere fremme end statslige enheder og dermed bidrage væsentligt til at begrænse skadevirkningerne.

Private kapaciteter bør primært indgå som forstærkere af statens tilstedeværelse – eksempelvis gennem overvågning, situationsopklaring, førsteindsats og teknisk reparation – i tæt samarbejde med statslige myndigheder.

Hurtig mitigering af konsekvenser

Mitigering handler om at begrænse de skadelige fysiske og psykologiske konsekvenser af hybride angreb. Det kræver både forebyggende tiltag såsom etablering af redundante systemer, failover-procedurer og fysisk sikring, men det kræver også evnen til hurtigt at kunne genoprette skader, fx gennem reparationskapaciteter og lagre af kritiske reservedele. Samtidig er det vigtigt, at staten og private ejere og operatører kan kommunikere hurtigt og troværdigt til offentligheden, om hvad der er sket, og hvordan man skal forholde sig.

Private aktørers reparationsberedskaber styrker mitigeringen med klare procedurer, adgang til de nødvendige kapaciteter og lagre af kritiske reservedele. Beredskabets robusthed kan fremmes ved at stille krav til ejere og operatører på disse områder. Samarbejdsaftaler mellem myndigheder, ejere og operatører kan sikre, at de nødvendige ressourcer hurtigt kan mobiliseres, når en hændelse indtræffer.

Der er forskel på, hvor samfundskritiske maritime installationer er. Afbrydelse af en stor havvindmøllepark gør større samfundsmæssig skade end et beskadiget kabel til en mindre dansk ø. Derfor skal niveauet af fysisk sikring følge trusselsniveauet og installationens samfundsmæssige betydning. Dette kræver en differentiering af infrastrukturen.

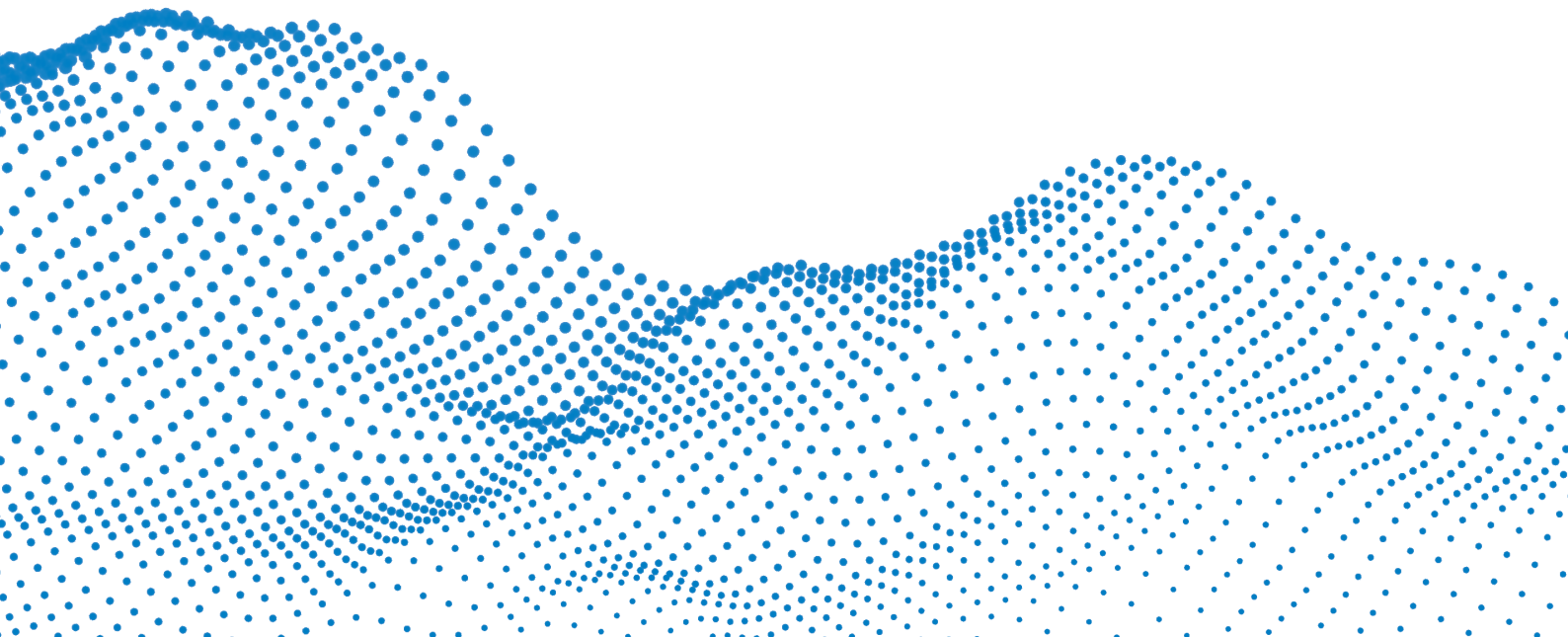
Private ejere og operatører kan forstærke sikringen omkring særligt kritiske anlæg. Kombinationen af fysisk sikring og perimeterovervågning reducerer både sandsynligheden for et angreb og omfanget af de efterfølgende konsekvenser. Industrien har allerede erfaringer med at integrere og kombinere eksisterende teknologier, fx radar, kameraer, sonarer og hydrofoner, så man kan opdage, spore og identificere trusler i luften, på overfladen og under havet.

En række danske virksomheder gennemførte i 2024 et systematisk fuldskalaforsøg ved en havvindmølleinstallation. Forsøget viste bl.a., at det er teknologisk muligt og økonomisk realistisk at forbedre overvågningen af eksisterende anlæg.

I lighed med dronezoner med flyveforbud, kan staten etablere zoner omkring kritisk maritim infrastruktur med restriktioner for færdsel, ankring mv. og med forbud mod brug af flyvende droner samt overflade- og undervandsdroner. Ved at kræve forhåndsgodkendelse af aktiviteter i zonerne vil det være enklere for både staten og private aktører at skelne mellem uønskede og lovlige aktiviteter.

Endelig kan private aktører understøtte en hurtig og koordineret kommunikationsindsats, så myndigheder og operatører kan informere offentligheden præcist og troværdigt – et vigtigt element i at dæmpe de psykologiske følgevirkninger af hybride angreb.

Den Hybride Koalition



Danmark har et stærkt udgangspunkt. Erfaringer fra håndtering af skader på undersøisk infrastruktur viser, at samarbejdet mellem myndigheder, ejere, operatører og specialiserede leverandører fungerer godt sammenlignet med andre lande, bl.a. gennem hurtig mobilisering og korte reparationstider.

Ambitionen med dette whitepaper er ikke at erstatte eksisterende strukturer, men at bygge videre på de styrker, der allerede findes, og udvide dem til også at håndtere et mere komplekst og sikkerhedspolitisk præget trusselsbillede.

I december 2025 besluttede regeringen at etablere et nyt fælles 24/7-situationscenter i forbindelse med National Operativ Stab. Idéen er god, men ikke tilstrækkelig. Centeret har kun til formål at styrke det operative samarbejde mellem myndigheder. Vi tror på, at den rigtige løsning på de hybride trusler, som allerede nu påvirker Danmark og vores allierede, ligger i et endnu tættere statsligt samarbejde med private leverandører af systemer, kapaciteter og sensorer samt ejere og operatører af den kritiske maritime infrastruktur. På denne måde bygger vi videre og er i stand til at styrke modstandskraften over for trusselsbilledet i fremtiden.

Vi kalder et sådant samarbejde for "Den Hybride Koalition". "Hybrid", fordi samarbejdet rummer både statslige myndigheder og private aktører. "Koalition", fordi aktørerne hver især er uundværlige dele af den gode løsning på et fælles problem og er villige til at gå sammen og bidrage.

Det er afgørende, at en styrkelse af beredskabet ikke fører til unødvendig opbygning af parallelle statslige kapaciteter, som risikerer at svække eksisterende civile og markedsbaserede løsninger. Inden for det maritime og undersøiske område er der tale om højt specialiserede kapaciteter, der kræver fartøjer, udstyr, kompetencer og løbende operativ erfaring. Disse kapaciteter findes i vid udstrækning allerede hos private aktører. En effektiv model bør derfor tage afsæt i at bevare og videreudvikle disse styrker i et tæt samspil med staten.

Vi løser ikke alle problemer og udfordringer på én gang, men vi tror på, at vi kan opnå en bedre beskyttelse af kritisk maritim infrastruktur allerede på kort sigt. Men der er brug for at komme hurtigt i gang – både for at kunne imødegå de hybride trusler og angreb, og for at gøre os konkrete erfaringer med teknologi og tværgående samarbejde. På den måde kan vi løbende forbedre vores forsvar mod trusler, som hele tiden udvikler sig.

De små og hurtige løsninger er ikke nok i sig selv. Vi skal være parate til at sammensætte de store og mere komplekse løsninger, hvor vi for alvor binder statens og private aktørers ressourcer sammen.

Vi giver derfor vores bud på initiativer på kort og længere sigt.

Kort sigt

Styrk overvågningen ved at inddrage private kapaciteter og investér i eksisterende overvågningsløsninger, der er hurtige at implementere.

Staten skal indgå samarbejdsaftaler med private ejere og operatører om at nyttiggøre den eksisterende overvågning. Staten bør investere i to til tre pilotprojekter (fx i Nordsøen, Kattegat og ved Bornholm), hvor myndigheder og private sammen tester overvågningssystemer med droner, undervandssensorer og datadeling. Erfaringerne skal bruges til at udvikle løsninger baseret på teknologi, dataindhentning og -behandling samt sikre robuste procedurer. Investeringer i eksisterende teknologier vil også bidrage til innovation af nye og bedre løsninger.

Hotline til myndighederne.

Staten skal udvide kendskabet til den eksisterende Maritime Assistance Service (MAS) og udvide den fra at være en hotline for civil skibstrafik til også at være hotline for ejere og operatører af kritisk maritim infrastruktur. Dette vil styrke varslingen af potentielle trusler.

Etablér maritime forbuds- og overvågningszoner omkring kritisk infrastruktur.

Opret særlige zoner med forbud mod uautoriseret sejlads, droner og undervandsaktiviteter, fx omkring udvalgte havvindmølleparker, kabellandinger og rørledninger. Formålet er dobbelt: at begrænse adgang, men også at signalere overvågning og tilstedeværelse. Lignende tiltag er gennemført i bl.a. Belgien og omkring offshore vindmølleparker.

Længere sigt

Udarbejd en national doktrin for beskyttelse af kritisk maritim infrastruktur.

Doktrinen skal definere mål, roller, ansvar og samarbejdsprincipper mellem stat, private aktører og internationale partnere.

Doktrinen kan bl.a. bygge på de tidlige erfaringer fra luftfartsområdet (dronelovgivning) og NATO's Baltic Sentry-koncept, men også erfaringer fra pilotprojekterne omtalt i anbefalingerne på kort sigt.

Etablér et integreret nationalt overvågningssystem.

Udvid det nyoprettede 24/7-situationscenter til at være et samlet system, hvor operationscenteret kan behandle, præsentere og reagere på data i realtid. Systemet skal bygges gennem offentlig-privat samarbejde, særligt pga. den store dataudveksling, systemet kræver. Systemet vil sikre et reelt situationsbillede og begrænse blinde vinkler på og under havoverfladen.

Myndighederne har brug for, at industrien understøtter med kapaciteter og ressourcer for at kunne løse den langt større overvågnings- og reaktionsopgave, som de nye trusler medfører. Derfor skal staten inddrage datakilder fra ejere og operatører til at supplere og styrke den statslige overvågning.

Styrk den maritime responskapacitet.

Udvikl en model for øget tilstedeværelse ved kritisk maritim infrastruktur og hurtig indsættelse til søs, fx gennem specialiserede offentlige og private enheder, der kan sikre tilstedeværelse, reagere på hændelser, observere aktivitet og bistå med dokumentation ifm. skader på kritisk maritim infrastruktur.

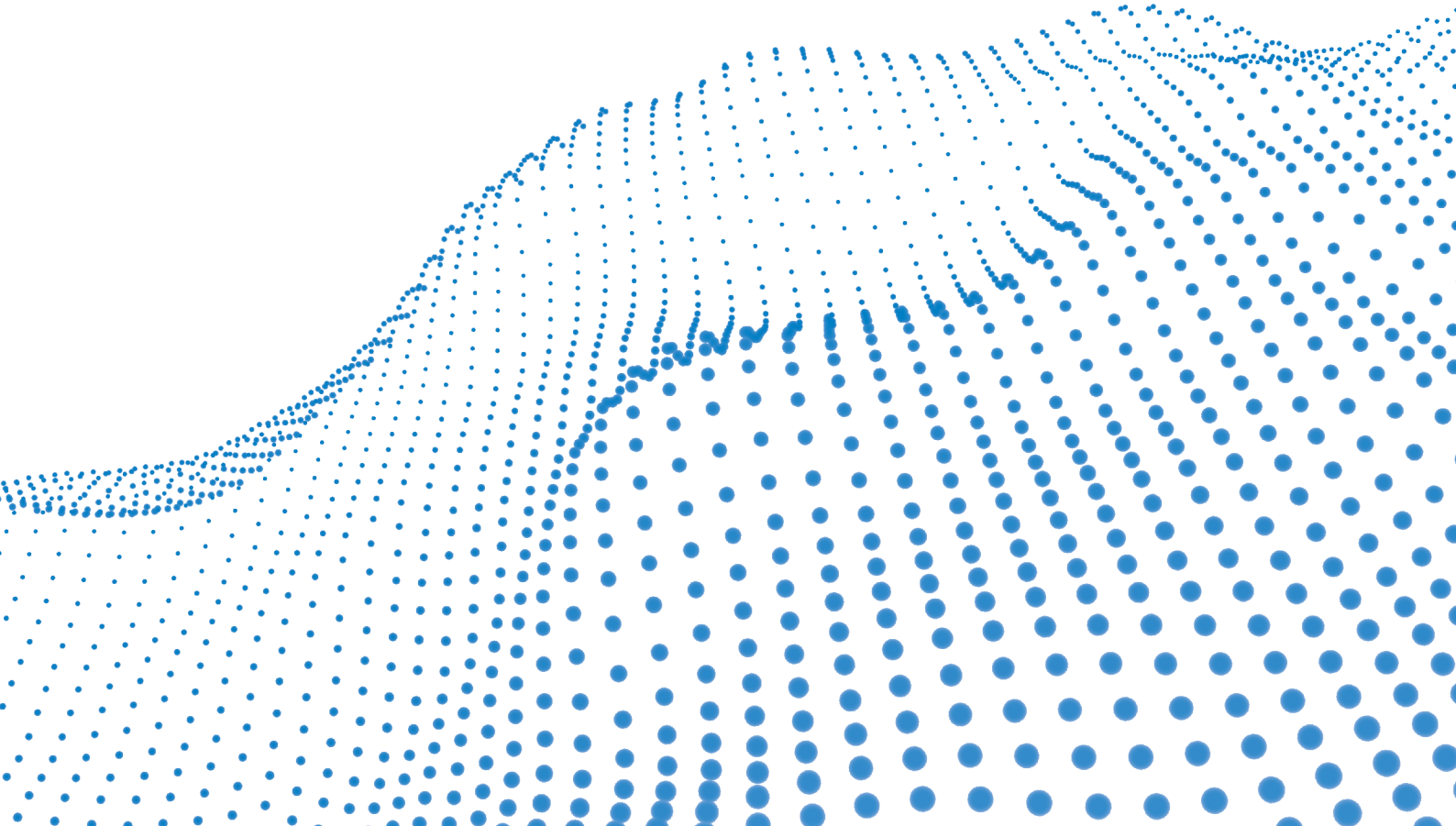
Løsningen skal drives i et tæt samarbejde mellem private aktører og myndigheder. Hurtig respons har en afskrækkende effekt og er et vigtigt værktøj til at signalere større risiko over for fjendtlige aktører.

Konklusion

Danmark kan med det rette samarbejde forbedre beskyttelsen af den kritiske maritime infrastruktur markant. Gennem den hybride koalition kan vi drage nytte af danske virksomheders stærke teknologiske positioner og private aktørers vilje til at bidrage.

Danske virksomheder har dokumenterede styrkepositioner inden for bl.a. sensorer, dataanalyse, systemintegration, maritime operationer og reparationsberedskaber, som kan omsættes til konkret national sikkerhed. Modstandskraft skal sikres gennem partnerskab – ikke centralisering.

Et tæt partnerskab vil gøre Danmark mere modstandsdygtigt over for hybride trusler i fred, krise og krig og sikre stabil forsyning og operationel kontrol i et stadig mere udfordret maritimt domæne. Sammen kan vi opbygge et sammenhængende maritimt forsvar og beredskab, der både afskrækker trusler, opdager dem tidligt og sikrer hurtig genopretning, når det gælder mest.



TELEDYNE | RESON

Kontakt: RESON@Teledyne.com

Teledyne RESON A/S
Fabriksvangen 13
3550 Slangerup
Danmark