Myndigheten för
samhällsskydd
och beredskap

Missiv

Datum
2025-06-19
Ert datum
2025-06-19

Ärendenr
MSB 2025-06083
Er referens
Fö2025/00713

Enheten för det operativa ledningssystemet
(OA-LS)
Kajsa Nordmark
010-240 5097
Kajsa.Nordmark@msb.se

Regeringskansliet
Försvarsdepartementet
103 33 Stockholm

Redovisning av uppdraget att stärka det civila försvarets förmågeutveckling för att hantera incidenter kopplade till undervattensinfrastruktur

Regeringen gav 16 april 2025 ett uppdrag till Myndigheten för samhällsskydd och beredskap (MSB), Statens energimyndighet, Affärsverket svenska kraftnät, Post- och telestyrelsen, Polismyndigheten och Kustbevakningen. Myndigheterna fick i uppdrag att i samverkan vidta åtgärder för att stärka förmågan att upptäcka och rapportera incidenter och störningar på undervattensinfrastruktur för energiförsörjning respektive elektroniska kommunikationer till och från Sverige som kan innebära risk för påverkan på samhällsviktig verksamhet. MSB skulle ansvara för att inhämta synpunkter från Försvarsmakten och dialog med ytterligare myndigheter skulle initieras vid behov.

MSB fick i uppdrag att sammanställa redovisningen av uppdraget för överlämnande till regeringskansliet (Försvarsdepartementet) senast den 25 juni 2025.

Uppdraget har genomförts i nära samarbete med de i utpekade myndigheterna samt Sjöfartsverket, Myndigheten för psykologiskt försvar och Strålsäkerhetsmyndigheten. Synpunkter har inhämtats från Försvarsmakten. MSB har samordnat arbetet.

Härmed överlämnas myndigheternas gemensamma redovisning av uppdraget med beskrivning av åtgärder för att stärka förmågan att upptäcka och rapportera incidenter och störningar kopplade till undervattensinfrastruktur.

Enligt överenskommelse med samtliga myndigheter har generaldirektören för MSB, efter godkännande från övriga myndigheter, fattat beslut i ärendet.

I detta ärende har generaldirektör för MSB Mikael Frisell beslutat. Kajsa Nordmark och Carl-Johan Breitholtz har varit föredragande. I den slutliga handläggningen har också biträdande avdelningschef Susanna Trehörning deltagit. I uppdraget har flera avdelningar deltagit både på chefs- och handläggarnivå.

Mikael Frisell

Kajsa Nordmark/Carl-Johan Breitholtz

Dokument

- Myndighetsgemensam slutrapport för regeringsuppdrag Fö2025/00713

- Bilaga 1 – Försvarsmaktens synpunkter på MSB utkast 3 "Åtgärder för att stärka det civila försvarets förmågeutveckling för att hantera incidenter kopplade till undervattensinfrastruktur"

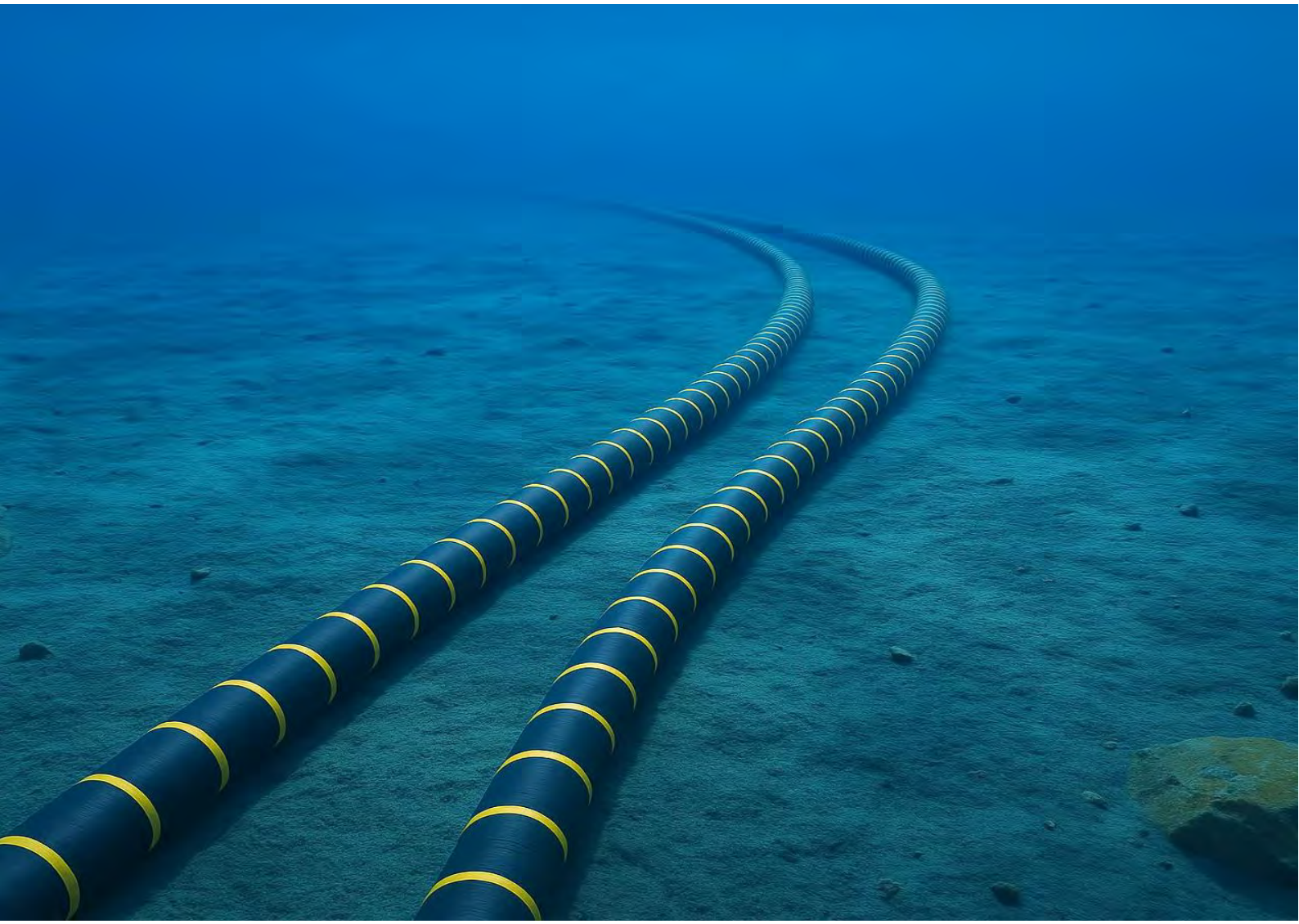
Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240
Fax: 010-240 56 00
registrator@msb.se
www.msb.se
Org.nr: 202100-5984

Åtgärder för att stärka det civila försvarets förmågeutveckling för att hantera incidenter kopplade till undervattensinfrastruktur

Myndighetsgemensam redovisning av regeringsuppdrag

(Fö2025/00713)



Sammanfattning och slutsatser

Denna rapport redovisar ett regeringsuppdrag som syftar till att stärka det civila försvarets förmågeutveckling för att hantera incidenter kopplade till kritisk undervattensinfrastruktur. Undervattensinfrastruktur utgör en central del i upprätthållandet av det svenska samhällets funktionalitet. Incidenter eller angrepp kan medföra allvarliga direkta och indirekta konsekvenser för samhällsviktig verksamhet.

Uppdraget har haft en begränsad tidsram och det bör betonas att myndigheterna redan har omhändertagit lärdomar från den senaste tidens incidenter och störningar, vilket har resulterat i en förbättrad operativ hantering. Redan påbörjat effektiviseringsarbete har ytterligare förstärkts genom detta regeringsuppdrag.

Även om uppdraget har inriktats på kritisk undervattensinfrastruktur har förmågeutvecklingen gynnat aktörsgemensam operativ hantering i stort. De aktiviteter som genomförts inom ramen för regeringsuppdraget har höjt kunskapen och stärkt förmågan inom och mellan de deltagande aktörerna. Åtgärder, synergier med annan utveckling, samt rekommendationer kommer att bidra till en ökad operativ förmåga även inom andra områden.

Ett genomgripande förhållningssätt i arbetet med uppdraget är att alla involverande aktörer har haft ett helhetsperspektiv – helheten är större än summan av de enskilda delarna. Åtgärderna och rekommendationerna får tyngd och relevans genom att aktörerna har arbetat genom fokusområden som är ömsesidigt förstärkande.

Följande tre fokusområden har använts i arbetet:

- Stärkt förmåga att upptäcka, larma och informationsförsörja
- Stärkt förmåga till aktörsgemensam inriktning och samordning
- Stärkt förmåga till säker kommunikation för ledning och samverkan

Synergier med angränsande utveckling har identifierats och rekommendationer har formulerats för att ytterligare stärka den samlade förmågan att hantera störningar och incidenter mot kritisk undervattensinfrastruktur.

Ett viktigt budskap är att vi måste vara uppmärksamma på det som sker och vara beredda att agera när det behövs. Samtidigt måste vi behålla lugnet och i så stor utsträckning som möjligt ta reda på fakta. För snabbt dragna slutsatser riskerar att gynna dem som inte vill Sverige väl och här har vi ett gemensamt ansvar både för den information som vi delar myndigheter emellan och de budskap vi sänder till allmänheten.

Det är i sammanhanget också viktigt att lyfta fram betydelsen av kommunikation. Det finns en risk i att alltför snabbt benämna incidenter och störningar som

händelser av hybridkaraktär. Med hybrida hot avses aktiviteter från statliga aktörer som försöker utnyttja sårbarheter i ett samhälle för egen nytta genom att använda en blandning av olika metoder under tröskeln för krig. Det är därför viktigt att kunna särskilja hybridhändelser från rena olyckor och andra händelser och i så stor utsträckning som möjligt ta reda på fakta.

Genomförandet av regeringsuppdraget har sammanfattningsvis lett till följande:

- Ökad kunskap om vilka aktörer som faktiskt berörs och därmed behöver information för effektiv operativ hantering, både för brottsutredning, men också för att minimera konsekvenser på samhällsviktig verksamhet.
- ”Sänkta trösklar” mellan aktörer utifrån den senaste tidens operativa hantering av störningar och incidenter på kritisk undervattensinfrastruktur, men även genomförda övningar har bidragit. För att bibehålla relationer och tillit som uppnåtts är det av stor vikt att fortsätta att öva både hanterande operativa funktioner och beslutsfattande nivåer.
- Ökad helhetssyn och perspektivförståelse hos aktörerna, vilket ger högre effekt i den samlade hanteringen vid störningar och incidenter på kritisk undervattensinfrastruktur.
- Ökad förmåga att upptäcka, larma och informationsförsörja redan vid indikation på störning eller incident hos aktörerna har uppnåtts genom bl.a. förbättrade larmrutiner och rapportering från infrastrukturägare och leverantörer som i många fall är privata aktörer.
- Ökad förmåga till koordinerat beslutsfattande har uppnåtts genom en utvecklad sjölägesbild och 24/7-övervakning för att snabbt upptäcka avvikelser, samt samlad lägesbild med tvärsektoriell analys vid händelsehantering, men också genom de initiativ som tagits för att stärka och förtydliga befintliga samverkansstrukturer.
- Ökad förmåga till att minimera målkonflikter som kan uppstå, exempelvis vid genomförande av brottsutredande insatser i relation till att åtgärda konsekvenser på samhällsviktig verksamhet. Genom fortsatt arbete med tillståndsgivning utifrån befintligt regelverk möjliggörs en snabbare och mer effektiv genomförande av besiktning och reparationer.
- En förutsättning för ledning och samverkan är robusta, tillgängliga och säkra kommunikationer för informationsdelning. Omfattande arbete inom området sker redan, men tidigare erfarenheter och uppdraget har tydliggjort behovet av att säkerställa det civila försvarets förmåga till säkra kommunikationer i alla lägen.

I den verklighet vi lever i idag är det uppenbart att förmågeutveckling, förberedelser och hantering går in i varandra och vi behöver direkt omsätta gjorda erfarenheter i vårt samlade responssystem. Detta uppdrag har gett oss möjligheter att säkerställa strukturer, rutiner och arbetssätt för att korta tiden från upptäckt till hantering och vid behov inriktning och samordning.

Trots olika förutsättningar har vi strävat efter att identifiera gemensamma lösningar för att öka den samlade förmågan. Samsyn och en bredare förståelse för att flera aktörer behöver vara involverade är nödvändig för effektiv händelsehantering och undanröjande av målkonflikter som riskerar fördröjning. ”Sänkta trösklar” och att ta initiativ till samverkan redan vid indikation ger oss möjlighet till att vara proaktiva och träffsäkra i vår rapportering till Regeringskansliet.

Innehåll

Inledning och bakgrund

I sitt beslut från 16 april 2025 (Fö2025/00713) gav regeringen i uppdrag till sex myndigheter att stärka det civila försvarets förmågeutveckling för att hantera incidenter kopplade till undervattensinfrastruktur, vilket motiveras av det försämrade säkerhetsläget och tidigare inträffade incidenter. Denna redovisning presenterar resultatet av detta myndighetsgemensamma uppdrag och fokuserar, i linje med det givna uppdraget, på hur myndigheternas samlade förmåga att upptäcka, dela information och hantera avvikelser i maritim miljö kan stärkas.

Grundläggande för att stärka förmågan att hantera incidenter kopplade till undervattensinfrastruktur är att säkerställa att information om risker, störningar och incidenter delas tillräckligt snabbt så att den når rätt aktörer i tid. För att samhällets samlade resurser ska användas effektivt krävs en helhetssyn avseende behov, resurser och åtgärder. Det krävs även att aktörerna förstår hur olika delar av hanteringen hänger samman i olika beroenden och hur den aktörsgemensamma strukturen är tänkt att användas. Perspektivförståelse ger bättre förutsättningar att uppnå aktörsgemensam inriktning och samordning. Hantering av en incident kräver samordnade åtgärder i flera parallella spår: att avhjälpa skadan, att hantera samhällskonsekvenserna, att bemöta en antagonist och att utreda eventuella brott. Detta har därför varit genomgående utmaningar som har adresserats i uppdraget.

Det antagonistiska perspektivet är ständigt närvarande. En stärkt gemensam förmåga i denna domän har även en viktig avskräckande effekt. Därutöver behöver Sverige ta höjd för att alla former av incidenter kan följas av desinformation och annan vilseledande information. Erfarenheter visar att otillbörlig informationspåverkan i dag ofta fokuserar på Nato-anknutna aktiviteter i Östersjöområdet. För denna typ av incidenter är därför beredskap på informationsarenan central. Hur vi väljer att kommunicera är också en avgörande faktor inte minst för att möta riskerna med desinformation men också för att säkerställa att medborgarna får relevant och samordnad information kopplat till läget.

De aktörer som berörs av incidenter i undervattensinfrastruktur har olika mandat och uppdrag. Effektiv hantering förutsätter gemensam förståelse, samordnad analys och snabba kontaktvägar. Arbetet inom ramen för detta uppdrag har bidragit till ökad kunskap om de olika aktörernas roller och ansvar, fördjupade relationer och därmed förbättrade grunder för ett samlat agerande.

Flera av initiativen som beskrivs i rapporten hade påbörjats redan före uppdraget, men har genom detta arbete samordnats, fördjupats och konkretiserats. Många lärdomar har dragits i den operativa hanteringen som genomförts under perioden från 2023 fram till idag. Det innebär att regeringsuppdraget inte bara bidragit till nya åtgärdsförslag, utan även till förstärkt riktning, tempo och genomförandeförmåga.

Även om detta uppdrag är avgränsat till kritisk undervattensinfrastruktur medför åtgärdsförslagen att förmågan att upptäcka och hantera även andra hot och störningar har ökat.

Uppdraget

Den 16 april 2025 gav regeringen Myndigheten för samhällsskydd och beredskap (MSB), Energimyndigheten, Svenska kraftnät, Post- och telestyrelsen (PTS), Polismyndigheten och Kustbevakningen i uppdrag att i samverkan vidta åtgärder för att stärka förmågan att upptäcka och rapportera incidenter och störningar på undervattensinfrastruktur för energiförsörjning och elektroniska kommunikationer till och från Sverige. Syftet är att motverka påverkan på samhällsviktig verksamhet.

Myndigheterna ska, utifrån sina respektive mandat och ramar:

- vidta nödvändiga åtgärder och stärka förmågan att snabbt upptäcka och rapportera incidenter,
- utveckla en normalbild och tvärsektoriell lägesbild på nationell nivå,
- analysera möjliga händelseutvecklingar och samhällskonsekvenser,

Myndigheterna får i uppdraget lämna författningsförslag eller andra förslag vid behov.

Uppdraget ska genomföras med beaktande av relevanta internationella samarbeten och etablerade strukturer för rapportering och lägesbild, inklusive Sjöövervakningsrådet roll.

MSB ansvarar för samordning av redovisningen samt för att inhämta synpunkter från Försvarsmakten. Försvarsmakten har inkommit med ett yttrande på en beredningsversion av slutrapporten. Yttrandet har bilagts rapporten, se bilaga 1. Flera av synpunkterna gällde delar som har omarbetats och vissa sakfrågor i yttrandet har arbetats in i redovisningen. Försvarsmakten yttrande behöver fortsatt analyseras efter inlämnandet av svar på uppdraget. Arbete med förslagen i yttrandet bör även hanteras med beaktande av redovisningen av uppdrag till Försvarsmakten och Kustbevakningen att stärka sin operativa samverkan i syfte att höja den samlade förmågan till sjöövervakning (Fö2025/00038).

Uppdraget ska slutredovisas till Regeringskansliet senast den 25 juni 2025.

Tolkning och avgränsning av uppdraget

Regeringsuppdraget avser civila aktörers hantering av incidenter och störningar som påverkar kritisk undervattensinfrastruktur med betydelse för samhällsviktig verksamhet. Fokus i genomförandet har varit att stärka civila aktörers förmåga att upptäcka, identifiera och agera vid förhöjd risk och händelser i maritim miljö. Arbetet har genomgående hållits inom ramen för respektive aktörs ansvar. Varje medverkande myndighet har rådighet över de utfall från åtgärderna som faller inom deras respektive ansvarsområden, och har därmed godkänt rapportens slutliga innehåll i den del som berör dem.

Uppdraget omfattar således civila aktörer och civila system – inte Försvarsmaktens ansvarsområde. Flera aktörer däribland Svenska kraftnät, Kustbevakningen och MSB har lyft fram att flera av förslagen har bredare relevans än endast incidenter kopplat till kritisk undervattensinfrastruktur. Kustbevakningen roll är i sammanhanget central, men uppdraget har inte fokuserat på enskilda aktörer, utan på gemensamma lösningar.

I fredstid utgörs verksamheten inom det civila försvaret av beredskapsplanering och förmågehöjande åtgärder. Under höjd beredskap och ytterst i krig utgörs verksamheten av nödvändiga åtgärder för att upprätthålla målet för det civila försvaret. Det civila försvaret som verksamhet och aktörer inom det civila försvaret genomför inte insatser/operationer/operativa åtgärder som en del av totalförsvaret i fred. Sådana åtgärder vidtas genom ordinarie uppgifter, myndighetssamverkan samt inom ramen för den fredstida krisberedskapen.

Givet tidsramen för genomförandet av uppdraget omfattar redovisningen både åtgärder som gjorts för att stärka förmågan under uppdragsperioden, och även åtgärder på längre sikt.

Sjöövervakningsrådet

Arbetet med regeringsuppdraget har utgått från befintliga ansvarsförhållanden och etablerade samverkansstrukturer, där Sjöövervakningsrådet1 utgör ett centralt samrådsorgan som har till uppgift att bistå Kustbevakningen i arbetet med att samordna civil sjöövervakning och förmedla sjölägesinformation enligt förordningen (2019:84) med instruktion för Kustbevakningen.

Rådet har inte en operativ roll vid händelser, men bidrar till samordning och gemensam analys i det förebyggande och kapacitetshöjande arbetet. I nuläget omfattar rådet elva myndigheter och är organiserat i tre nivåer (strategisk, operativ och taktisk) som ska säkerställa tydliga beställningar och leveranser. Ett pågående utvecklingsarbete syftar till att effektivisera strukturen ytterligare, vilket bedöms vara relevant även för förmågan att upptäcka och hantera störningar i undervattensinfrastruktur.

[1] I Sjöövervakningsrådet deltar representanter från Försvarsmakten, MSB, Polismyndigheten, Sjöfartsverket, SMHI, Sveriges geologiska undersökning, Transportstyrelsen, Tullverket, Post och telestyrelsen och Svenska kraftnät.

Genomförande och utgångspunkter

Uppdraget har genomförts under en mycket kort tidsperiod givet de aktuella frågornas komplexitet. Den korta tiden till trots har uppdraget genomförts med ett iterativt arbetssätt och i ett nära samarbete mellan myndigheterna som fått uppdraget och andra berörda. På så vis har gemensamma behov, utmaningar och möjliga åtgärder på kort och lång sikt identifierats, arbetssätt effektiviserats och gemensam förståelse för roller och förutsättningar vid hantering av incidenter i inom området kritisk undervattensstruktur förstärkts.

Tre aktörsgemensamma workshoppar har genomförts med fokus på skeenden, informationsflöden och behov av åtgärder. Dessa har gett en gemensam analysgrund, en förankrad behovsbild och tillsammans med bl.a. erfarenheter från operativ hantering av den aktuella typen av händelser legat till grund för de fokusområden och åtgärdsförslag som redovisas i kommande avsnitt.

Utöver de myndigheter som pekats ut i uppdraget har även Försvarsmakten, Myndigheten för psykologiskt försvar, Sjöfartsverket och Strålsäkerhetsmyndigheten bidragit i olika delar. Deras medverkan har varierat i omfattning beroende på uppdrag och behov, men sammantaget varit viktiga för att skapa en helhetsbild. Flera myndigheter har samtidigt kunnat använda uppdraget för att tidigarelägga eller samordna pågående utvecklingsinsatser, särskilt inom teknik, analyskapacitet och rapporteringskedjor.

Gemensamma grunder för ledning och samverkan

Gemensamma grunder – ramverk för ledning och samverkan är en central utgångspunkt för aktörsgemensam hantering. Det ger stöd till det operativa arbetet och främjar en gemensam förståelse för hur inriktning och samordning ska ske vid samhällsstörningar – både i ordinarie struktur och vid behov av förstärkt samverkan. Modellen för inriktning och samordning i tvärsektoriella frågor på central nivå[2], som ingår i ramverket, är utgångspunkten för hur centrala myndigheter hanterar händelser tillsammans, såväl på samordnande som inriktande nivå.

Samverkan inför och under händelser behöver både ha en tydlig inriktning och vara samordnad för att samhällets resurser ska användas effektivt. Även om kommunikationssamordning inte är i fokus för uppdraget, utgör kommunikation en viktig del i helheten och behandlas därför kort i rapporten.

Internationella samarbeten

Sverige har en stor mängd etablerade internationella samarbeten – såväl bilaterala som multilaterala med bäring på området. I genomförande av uppdraget har en övergripande inventering av existerande samarbeten gjorts. Syftet har dels varit kunskapshöjning och dels att undersöka om det kan finnas mervärden av dessa

[2] Se https://www.msb.se/contentassets/359585e86aff4053a429d8f05bdf9206/pm-inriktning-och-samordning-pa-central-niva.pdf.

samarbeten utifrån olika perspektiv. Exempelvis är återhämtningsförmågan, det vill säga kapaciteten att snabbt reparera skadad infrastruktur, en viktig del av vår motståndskraft och avskräckningsförmåga. Internationella samarbeten är därför en väsentlig del av den samlade nationella förmågan. Det innefattar även internationella övningar.

Andra exempel på nyligen beslutade internationella samarbeten med fokus på skydd av kritisk undervattensinfrastruktur är att Kustbevakningen ska utgöra den nationella operativa kontaktpunkten inom Natos nätverk för skydd av kritisk undervattensinfrastruktur samt gentemot samarbetet för skydd av infrastruktur i Nordsjön (Fö2025/00465).

Kustbevakningen har dessutom fått i uppdrag att samordna det nationella genomförandet av EU:s maritima säkerhetsstrategi (EUMSS) med tillhörande handlingsplan (Fö2025/0465), vilket omfattar alla myndigheter med ansvar i den maritima miljön. Flera av åtgärderna i handlingsplanen syftar till stärkt skydd av kritisk undervattensinfrastruktur.

Informations- och hanteringskedja samt fokusområden

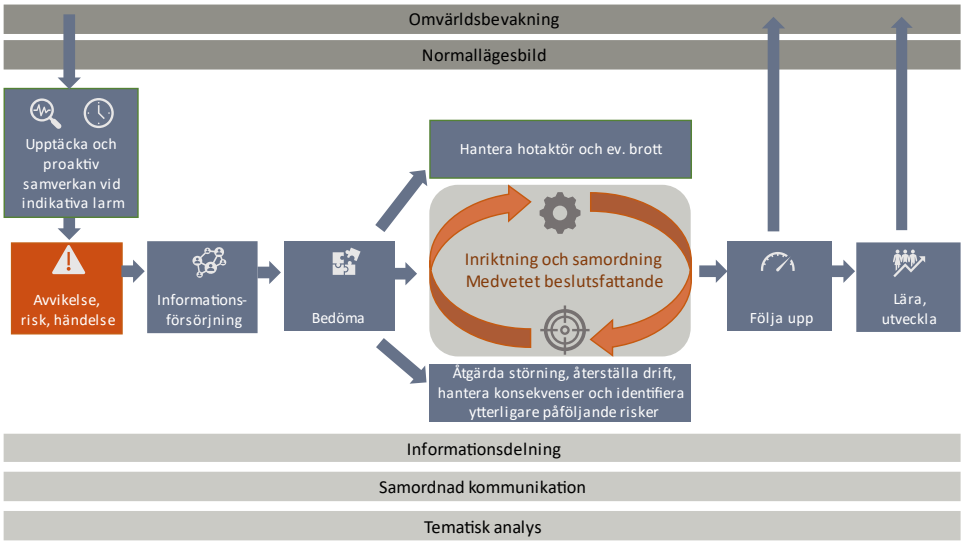
Ett viktigt behov som identifierades tidigt var att åstadkomma en gemensam syn på skeendet och informationsflödet vid störningar och incidenter i undervattensinfrastrukturen i syftet att kunna precisera åtgärder i olika faser. Följande deskriptiva bild har tagits fram aktörsgemensamt, som ett led i arbetet med att kartlägga flödet i en händelse och skapa förståelse för problemområdet. Bilden har också hjälpt att identifiera och sortera tänkbara åtgärdsförslag. Den har bidragit till att skapa samsyn kring gemensamma arbetssätt och förhållningssätt och en gemensam förståelse avseende andra närliggande risker och vikten av att kunna omhänderta direkta och indirekta konsekvenser av en händelse. Processbilden är en förenkling och har fungerat som ett stöd under arbetet och ska inte tolkas som en processbild av hur hanteringen bör se ut. För en normativ bild hänvisas till process för aktörsgemensam inriktning och samordning i ramverket.[3]

Utifrån bilden har tre fokusområden, som anses särskilt avgörande för att stärka Sveriges samlade förmåga, identifierats:

- stärkt förmåga till att upptäcka, larma[4] och informationsförsörja
- stärkt förmåga till inriktning och samordning
- samt stärkt förmåga till säkra kommunikationer[5]

I nästkommande avsnitt fördjupas resonemangen kring dessa områden.

[3] https://rib.msb.se/filer/pdf/30889.pdf
[4] Termen *larma* används oftast i aktörsinterna sammanhang men används här i en aktörsgemensam kontext.
[5] MSB har genom arbetet med sammanställandet av rapporten identifierat att säkra kommunikationer är förutsättningsskapande för de åtgärder som lyfts fram. Därefter har det tagits med som ett fokusområde.



Figur 1. Skeende hantering av händelse

Bilden visar schematiskt olika steg i ett skeende – från normalläge till avvikelser, förhöjd risk, störning och hantering av en händelse. I normalläget genomför olika aktörer omvärldsbevakning och övervakning av infrastruktur inom sina respektive ansvarsområden för att följa och upptäcka störningar vad gäller såväl sjötrafik som infrastruktur. Detta ska användas för att ta fram en normallägesbild över tid och för att utifrån denna normallägesbild kunna identifiera störningar och incidenter.

Om infrastrukturen är skadad vidtas åtgärder omedelbart, vissa mycket viktiga sker helt automatiskt. Händelser hanteras i många fall direkt av infrastrukturägare. Vid upptäckt av eller misstanke om en incident behöver berörda aktörer informeras för att få kännedom om situationen och kunna påbörja en eventuell hantering. Information delas mellan aktörer som gör en bedömning av om och hur händelsen bör hanteras.

Hanteringen av en händelse kan parallellt omfatta en hantering av ett misstänkt brott och en hantering av en skada eller störning som har uppstått samt de direkta och indirekta konsekvenserna av detta. Arbetet behöver inriktas och samordnas både inom dessa parallella spår och mellan spåren och information behöver delas mellan inblandade aktörer. En tvärsektoriell lägesbild över störningar, händelseutveckling och samhällskonsekvenser behöver tas fram som underlag för inriktning och samordning.

Vid återgång till normalläge efter en händelse genomförs uppföljning och aktiviteter för lärande.

Under hela skeendet och även under normalläget behöver information delas mellan aktörer. Tematiska analyser bör genomföras och kommunikation externt behöver samordnas.

Fokusområden för utvecklad förmåga

Som metod för genomförande av uppdraget har processbilden (figur 1) i avsnittet ovan tagits fram för att åskådliggöra ett skeende men också för att ringa in områden där fortsatt utveckling är angelägen. Dessa benämns här fokusområden och används för att gruppera konkreta åtgärdsförslag inom respektive område. Fokusområdena är ömsesidigt förstärkande.

Samtliga frågeställningar i uppdraget har adresserats, men uppdelningen i fokusområden har utformats för att stämma in på det övergripande syftet med uppdraget. Därför motsvarar inte fokusområdena fullt ut de tre olika frågeställningar som ges i uppdraget (se Uppdraget). De första två frågeställningarna (*vidta nödvändiga åtgärder och stärka förmågan att snabbt upptäcka och rapportera incidenter* samt *utveckla en normalbild och tvärsektoriell lägesbild på nationell nivå)* adresseras i första hand i det första fokusområdet. Det andra fokusområdet adresserar i huvudsak den tredje frågeställningen (*analysera möjliga händelseutvecklingar och samhällskonsekvenser).* Det tredje fokusområdet *stärkt förmåga till säkra kommunikationer* har lagts till eftersom det är en förutsättning för samverkan vid tidig upptäckt, larmning och informationsförsörjning och även för att uppnå aktörsgemensam inriktning och samordning.

I följande avsnitt beskrivs dessa fokusområden styrkor och utmaningar kopplade till dem.

Stärkt förmåga till att upptäcka, larma och informationsförsörja

Förmågan att snabbt upptäcka och dela information i ett inledande skede behöver fortsatt stärkas. Som av resultat av erfarenheter och arbetet med uppdraget har trösklarna för informationsförsörjning sänkts vilket också bör omsättas i beredskapsrutiner. Vidare krävs en löpande dialog om trösklar behöver justeras ytterligare samt överenskomna rutiner om vad t.ex. ”indikativa larm” ska leda till för ”motreaktioner”.

Informationsförsörjning vid händelser avseende undervattensinfrastruktur omfattar även myndigheter och aktörer såsom Kustbevakningen, Polismyndigheten, Säkerhetspolisen och Försvarsmakten, som ansvarar för initialt omhändertagande av händelser, liksom MSB som sammanställer nationell samlad lägesbild. Arbetet bygger på att det i ett tidigt skede finns en gemensam syn på skeendet och ett tydligt informationsflöde, vilket skapar bättre förutsättningar att precisera åtgärder i olika faser.

Tydlig och effektiv informationsförsörjning, som möjliggör tidig samverkan, är avgörande för att snabbare kunna uppnå aktörsgemensam inriktning och samordning samt stöd till medvetet beslutsfattande.

En utmaning avseende larmning till svenska myndigheter är att infrastrukturen i många fall ägs av privata och utländska aktörer. Störningar upptäcks regelmässigt först av dessa aktörer eftersom de övervakar infrastrukturen aktivt. Det innebär att informationskedjan vanligen inleds utanför myndigheternas direkta kontroll.

I och med att aktörerna har vitt skilda förutsättningar är det viktigt att ändå i möjligaste mån säkerställa effektiva kontaktvägar på alla nivåer som kan förstås av och fungera för alla aktörer.

Förmågan att samla in information om havsbottenförhållanden begränsas av den lagstiftning som reglerar skyddet av sjögeografisk information.[6] Detta är kritiskt för att skapa en lägesbild både i proaktivt underhållssyfte och för att påskynda reparationsförmågan vid en incident.

Stärkt förmåga till inriktning och samordning

Förmågan att snabbt inrikta och samordna, samt ta fram och upprätthålla en samlad lägesbild, behöver stärkas utifrån befintliga strukturer och arbetssätt. Det innebär bland annat en utveckling inom forum för operativa chefer (OpC) och inriktnings- och samordningsfunktion (ISF).

Forum för operativa chefer (OpC) ingår i strukturen för inriktning och samordning på central nivå. I forumet deltar MSB, sektorsansvariga myndigheter, Försvarsmakten, en representant från de civilområdesansvariga länsstyrelserna samt några berörda myndigheter. MSB är sammankallande aktör för OpC. Forumet syftar till att stärka relationerna mellan operativa verksamheter, delgivning kring aktuella händelse samt gemensam lägesuppfattning. Forumet kan bidra till en effektiv situationsanpassad hantering vid händelse.

Aktörsgemensam hantering initieras när behov uppstår. Vid identifierad förhöjd risk eller inträffad incident eller störning kan organiseringen av det aktörsgemensamma arbetet ske i en ISF som inrättas i stärkt samverkan. En ISF möjliggör ett koordinerat beslutsfattande. För att driva och koordinera det aktörsgemensamma arbetet behövs en sammankallande aktör. Vilken aktör som är sammankallande är beroende av händelsen. Integrerad kommunikation är en förutsättning för ledning och samverkan. Kommunikationsdirektörsnätverket (KOMDIR) har därför en viktig roll i det arbetet.

Kommunikationssamordning med tillhörande forum är en integrerad del i hanteringen. En utmaning är just den kommunikativa aspekten av hanteringen, exempelvis avskräckande eller dämpande strategisk kommunikation och förmågan att kommunicera samordnat och förstärkande. En svag kommunikativ hantering kan öppna för informationspåverkan och kan leda till ytterligare krishantering. En

[6] Lag (2016:319) om skydd av geografisk information samt Lag (1966:314) om kontinentalsockeln

annan utmaning är informationsdelning när lägesbilden bygger på osäkerhet. Det aktörsgemensamma kommunikationsarbetet kan behöva fortgå längre, även om hanteringen i övrigt har avslutats.

En ytterligare utmaning är att flera aktörer hanterar samma händelse utifrån sina respektive roller, ansvar och mandat. Det är således viktigt att säkerställa att eventuella målkonflikter hanteras. Ett tydligt exempel är att en förundersökning avseende misstänkt brott behöver hanteras parallellt med hanteringen av de konsekvenser som uppstår i samhället. Det är Polismyndigheten och Säkerhetspolisen som huvudsakligen ansvarar för att utreda och via åklagare leda eventuella förundersökningar samt Säkerhetspolisens ansvar att potentiellt attribuera om främmande makt ligger bakom en incident. Då kan det anses vara ett hybridhot. Om en statlig aktör är inblandad tar det sannolikt lång tid innan en sådan eventuell attribuering kan ske.

Om det finns brottsmisstanke behöver brottsplatsen säkras och förundersökningsåtgärder genomföras. Dessa åtgärder kan innebära att aktörer som har uppdraget att reparera skadan och återställa funktionaliteten inte ges tillträde till aktuell plats vilket i sin tur kan leda till mer omfattande konsekvenser eftersom reparationsarbetet inte får fördröjas. För att genomföra reparation kan exempelvis reparationsresurser behöva beställas och finnas tillgängliga, vilket innebär ett behov av framförhållning och samverkan mellan infrastrukturägaren och förundersökningen.

Detta exempel belyser vikten av helhetssyn och perspektivförståelse samt aktörsgemensam samordning av åtgärder.

Stärkt förmåga till säkra kommunikationer

Tillgången till robusta, säkra, tillgängliga och interoperabla kommunikationssystem är en förutsättning för samverkan inom det civila beredskapssystemet både i fred och under höjd beredskap och för att säkerställa samverkan med det militära försvaret. Civila aktörer använder en bred flora av informationssystem och sambandsmedel för allt från öppen information upp till högsta säkerhetsskyddsklass.

PTS bidrar till att stärka robustheten hos de kommersiella operatörerna för att säkerställa att tillgången till elektroniska kommunikationer är tillräckligt god. Därutöver har MSB ett ansvar för att tillsammans med Försvarsmakten säkerställa att samhällsviktiga aktörer har tillgång till robusta kommunikationstjänster som svarar mot krigets krav.

En grundläggande utmaning för de civila aktörerna är tillgången till gemensamma lösningar för informationsdelning av säkerhetskyddsklassificerade uppgifter. I totalförsvaret och för den fredstida krisberedskapen efterfrågas överlag gemensamma system både för nivåerna begränsat hemlig och hemlig, med funktionalitet såsom videokonferens, tal, meddelanden. Det finns tjänster som kan uppfylla flera av de grundläggande behoven, men en utmaning för de olika

tjänsterna som erbjuds är att majoriteten inte är kompatibla och sammankopplade med varandra. Detta kan i många fall åtgärdas rent tekniskt, men en del rättsliga och ekonomiska aspekter behöver förtydligas. Det är dock viktigt att poängtera att även om det relativt skyndsamt går att få fram nya tekniska system för informationsdelning så tar det vanligtvis längre tid att inrätta relevanta stödjande interna funktioner vid respektive myndighet som kan hantera systemen, exempelvis en signalskyddsorganisation, eller skapa rätt fysiska förutsättningar hos aktörerna, exempelvis säkra lokaler och skyddade anslutningar.

Försvarsmakten arbetar med ledningsstödsystem för totalförsvaret genom uppdrag i regleringsbrev (Fö2022/01572). Uppdraget ska slutredovisas 22 februari 2026. Till dess att uppdraget är klart och till dess ett sådant system är implementerat behöver det civila försvarets grundförmåga säkerställas. Vid framtagningen av totalförsvarssystem behöver behoven från både civila och militära försvaret tillgodoses. Sådana system är viktiga för att kunna användas i fred, i planering och förberedelser, samt för hantering av allvarliga händelser inom ramen för krisberedskapen.

Åtgärder

Uppdraget har resulterat i en rad åtgärder och åtgärdsförslag som har genomförts eller initierats inom ramen för uppdraget. Dessa åtgärder, grupperad per fokusområde, redovisas först i detta avsnitt. Därefter beskrivs förväntade resultat av genomförda åtgärder.

Genomförda och initierade åtgärder

I tabellen nedan finns en översikt över genomförda och initierade åtgärder grupperat på fokusområde. Därefter beskrivs de olika åtgärderna.

Fokusområde	Genomförda och initierade åtgärder	Ansvarig/ medverkande	När
Upptäcka, larma och informationsförsörja	Stärkt informationsförsörjning från privata aktörer	PTS, Svenska kraftnät	Start hösten 2025
	Utveckla normallägesbild över tid	Kustbevakningen	Juni 2025
	Stärkt informationsförsörjning till berörda myndigheter vid händelser	PTS, Energi-myndigheten, Svenska kraftnät, Kustbevakningen och MSB	Juni 2025

	Höja kunskapen hos och stärka samverkan mellan operativa funktioner (TiB och motsvarande)	Samtliga myndigheter i uppdraget deltog	Juni 2025
	Aktörsanalys för att identifiera vilka aktörer som berörs av olika typhändelser	MSB	Start juni 2025
	Larmövning med fokus på hantering vid händelse	Samtliga myndigheter i uppdraget deltog	Juni 2025
Aktörsgemensam inriktning och samordning	Stärka Forum för operativa chefer	MSB	Under 2025
	Stärka tvärsektoriell analysförmåga till stöd för inriktning och samordning	MSB, Sjöövervaknings-rådet	Under 2025
	Utveckla händelsespecifik samlad lägesbild med tvärsektoriell analys vid en händelse eller förhöjd risk	MSB	Juni 2025 (version 1)
	Övning med fokus på att stärka operativ hantering i OpC-forum	Samtliga myndigheter i OpC samt tillkommande aktörer	Dec 2024
	Deltagande i relevanta övningar avseende kritisk undervattensinfrastruktur	Samtliga	Löpande
Stärkt förmåga till säkra kommunikationer	Inventering av nuläge och gemensamma behov utifrån typhändelsen i regeringsuppdraget	MSB	Under 2025

Stärkt informationsförsörjning från privata aktörer

Åtgärden syftar till att utreda möjligheter till snabbare informationsdelning från infrastrukturägare till berörda myndigheter, bland annat vid incidenter och störningar avseende undervattensinfrastruktur. Fokus ligger på att undersöka både frivilliga och författningsstyrda alternativ.

Inom sektorn elektroniska kommunikationer och post finns undervattensinfrastruktur i form av fiberkablar som förmedlar datatrafik inom Sverige samt mellan Sverige och utlandet. Infrastrukturen i fråga ägs främst av privata aktörer. Detta medför ett behov av att säkerställa att information från

privata aktörer gällande möjliga incidenter och störningar rapporteras skyndsamt. Viss infrastruktur ägs även av bolag som är statligt ägda i andra länder än Sverige, vilket innebär samverkan med myndigheter och aktörer i dessa länder. Gällande sjöförlagda kraftkablar ägs dessa i största utsträckning av Svenska kraftnät men också av privata och utländska aktörer. Svensk kraftnät anser att en utredning om skyndsam informationsplikt vid incident på kraftkablar som ägs av privata aktörer bör genomföras.

Infrastrukturen är på systemnivå uppbyggd så att förbindelser som upprätthåller förmågan till elektronisk kommunikation är redundanta. Bortfall i enstaka kablar leder normalt inte till påverkan hos slutkunder, dvs. leder inte till avbrott eller omfattande kapacitetsförsämring. Enskilda fiberkablar är således vanligen inte kritiska för förmågan att upprätthålla elektroniska kommunikationstjänster. Eftersom incidenter typiskt sett ska nå upp till särskilda tröskelvärden för att omfattas av krav på incidentrapportering enligt lagen (2022:482) om elektronisk kommunikation och NIS[7], om incidenterna i övrigt inte haft viss betydande påverkan, faller i dagsläget många incidenter avseende undervattensinfrastruktur utanför befintliga rapporteringskrav.

Genom dialog med berörda aktörer inom sektorn har PTS inskärpt vikten av tidig information vid incidenter. Denna frivilliga informationsdelning bygger på förtroende och dialog mellan PTS och berörda aktörer. Berörda aktörer uppmanas att skyndsamt rapportera incidenter och störningar till PTS TiB.

För att stärka förmågan att utan dröjsmål upptäcka incidenter och störningar behöver såväl frivilliga som författningsstyrda åtgärder som kan leda till förbättrad rapportering undersökas. Det är av yttersta vikt att säkerställa att krav som ställs i författning är effektiva, inte medför onödig arbetsbelastning på rapporterande aktörer och inte medför en överrapportering som kan ge motsatt effekt jämfört med den önskade.

Under hösten 2025 avser PTS inleda arbete för att ytterligare stärka förmågan att upptäcka och rapportera incidenter som berör kritisk infrastruktur, inklusive undervattensinfrastruktur. I detta arbete kommer PTS att arbeta vidare med sådan förmågeutveckling som inte kunnat göras inom regeringsuppdragets tidsramar. PTS avser genomföra en juridisk analys avseende möjligheter att reglera rapportering av vissa typer av händelser, i syfte att ta fram handlingsalternativ och konsekvenser för dessa. PTS har initialt identifierat ett antal alternativ för eventuell reglering som bör utredas vidare. Ett sådant alternativ är att använda de bemyndiganden som föreligger vid en implementering av NIS2-direktivet[8], under förutsättning att PTS erhåller erforderlig föreskriftsrätt.

[7] NIS-direktivet är ett EU-direktiv som ställer krav på säkerhet i nätverk och informationssystem och som började gälla 2018. NIS ersätts av NIS2-direktivet, eller NIS2, och är en EU-omfattande reglering om cybersäkerhet som omfattar flera sektorer. I Sverige genomföras genom den så kallade cybersäkerhetslagen (CSL) som föreslås träda ikraft under 2025.
[8] NIS2 – Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen.

Utveckla normallägesbild över tid

Åtgärden syftar till att ytterligare stärka lägesbilden avseende typhändelser kopplat till kritisk undervattensinfrastruktur inom den maritima domänen. En lägesbild redogör för aktuellt läge, identifierade risker och bedömd förmåga hos berörda aktörer. Genom att följa utvecklingen över tid förbättras möjligheten att tidigt upptäcka avvikelser och respondera på förändringar i läget.

För att få en så komplett lägesbild som möjligt är det centralt att aktörerna rapporterar in förändringar, avvikelser och operativ kapacitet utifrån sina respektive ansvarsområden. Detta möjliggör en gemensam helhetsbild och bättre överblick över såväl normalläget som förändringar som kan kräva åtgärder. Bilden kommer att utvecklas och uppdateras regelbundet inom ramen för de processer som Kustbevakningen etablerar.

Lägesbilden ska fungera som ett gemensamt referensunderlag för att stödja proaktiv ledning, gemensam lägesanalys och prioritering av resurser. Den produceras, förvaltas och delas via Kustbevakningen och är ett viktigt verktyg för att skapa ökad handlingsberedskap i den maritima miljön.

Sektorsansvariga myndigheter kan bidra med sektorsspecifik kompetens och kontakt med aktörer inom sina respektive ansvarsområden.

Stärkt informationsförsörjning till berörda myndigheter vid händelser

Myndigheterna har genomfört förbättringsåtgärder som stärkt förmågan avseende att tidigt upptäcka, larma och informationsförsörja såväl internt som aktörsgemensamt mellan berörda myndigheter, regeringskansliet och MSB. Genom lärdomar och erfarenhetshanering från skarpa händelser har Energimyndigheten, Svenska kraftnät och PTS ytterligare stärkt förmågan att snabbt larma, informera och skapa en samlad lägesbild i tidigt skede av incidenter och störningar. I arbetet har befintliga rutiner setts över och vidareutvecklats, särskilt med fokus på situationer där det finns indikationer på incident men där osäkerheten är hög – så kallade indikativa larm. Dessa utgör ett proaktivt verktyg för att kunna agera tidigt utan att skapa otydlighet eller onödig aktivering.

Kustbevakningen har sedan tidigare tagit fram en överenskommelse med Svenska kraftnät och el-aktörer som beskriver rutiner för snabb larmning. Inom ramen för regeringsuppdraget har Kustbevakningen och PTS tagit fram en motsvarande överenskommen, bilateral rutin. Detta arbete kommer fortsätta med strävan att inkludera privata infrastrukturägare.

Baserat på erfarenheter från skarp hantering samt genom samverkan med berörda aktörer och myndigheter har PTS tagit fram en operativ plan för hantering av händelser i undervattensinfrastruktur, som innefattar en rutin för PTS TiB. Under 2025 kommer ovanstående arbete vidareutvecklas i samarbete med berörda aktörer. PTS avser även att se över ytterligare åtgärder, exempelvis tekniska

lösningar, för att stärka förmågan och korta ledtider. Detta inkluderar fortsatt dialog med både privata och offentliga aktörer inom sektorn.

Utvecklingsverksamheterna vid Polismyndigheten och Åklagarmyndigheten bör inleda en dialog för att hitta en mer enhetlig tolkning av vad som kan delges inom ramen för en pågående förundersökning för att säkerställa stärkt informationsförsörjning vid en aktörsgemensam hantering.

Höja kunskapen hos och stärka samverkan mellan operativa funktioner (TiB och motsvarande)

Åtgärden syftade till att öka samsyn, förtroende och förståelse mellan berörda myndigheters operativa funktioner, som tjänsteman i beredskap (TiB) och motsvarande roller.

Representanter från deltagande aktörers operativa funktioner möttes i juni 2025. Fokus låg på att dela arbetssätt, mandat, informationsbehov och nivåer för larmning – med särskilt fokus på tidig upptäckt, gemensam lägesbild och effektiv rapportering till MSB, Regeringskansliet och andra aktörer. Vidare syftade åtgärden till att stärka operativ förmåga och samverkan även innan en formell krisledning aktiveras.

Åtgärden möjliggjorde dialog kring skillnader i förutsättningar och ansvar, inklusive vilka tekniska och praktiska verktyg som finns för informationsförsörjning, sambandsplanering och larmning. Dialogen bidrog också till att tydliggöra kopplingen mellan operativ upptäckt och behovet av att snabbt kunna aktivera eller stärka ledningsfunktioner.

Den genomförda åtgärden har visat att samverkan mellan TiB-funktioner kan stärka operativ förmåga även innan en formell krisledning aktiveras, men det är viktigt att över tid vidmakthålla denna typ av närmare samverkan. Erfarenheterna pekar också på att liknande initiativ kan användas för kunskapsöverföring, tester och övningar inom andra fokusområden i det civila försvaret.

Aktörsanalys för att identifiera behov av samverkan

Med utgångspunkt i MSB:s metod har arbete med en aktörsanalys påbörjats för att stärka förmågan till snabb och anpassad samverkan genom att kartlägga viktiga aktörer som behöver samordnas, på vilket sätt och i vilka skeden. En hantering kräver alltid en situationsanpassad aktörsanalys och planering för att bli effektiv. Metoden kommer att användas av myndigheterna för att beskriva berörda aktörer anpassat till den specifika kontexten där beroenden ofta är tekniska, sektorsövergripande och geografiskt utspridda.

Analysen är avsedd att användas både i planering, hantering och för att stödja snabb etablering av gemensam inriktning. Genom att konkretisera vilka aktörer som behöver kopplas in, när och hur informationsflödet kan struktureras, stärker åtgärden förmågan att snabbt orientera sig och agera samordnat.

Aktörsanalysen kan potentiellt att fungera som en modell för liknande områden där samverkan behöver ske snabbt, gränsöverskridande och mellan aktörer med olika förutsättningar och utgör även ett viktigt verktyg för den samlade lägesbilden.

Larmövning med fokus på hantering vid händelse

Åtgärden syftade till att genom övning stärka förmågan hos berörda aktörers operativa funktioner att upptäcka, larma och informationsförsörja vid en händelse.

I juni 2025 genomfördes en larmövning som en riktad insats inom ramen för uppdraget. Övningen fokuserade på konkreta moment i hantering – särskilt tidig upptäckt, informationsdelning och samverkan mellan operativa roller så som TiB och motsvarande. Målet var att öka kunskapen hos aktörer i nätverket, identifiera förbättringsförslag och bidra till att stärka grupperingen av operativa fokalpunkter genom att sänka trösklar för informationsdelning.

Då incidenter kopplade till kritisk undervattensinfrastruktur ofta involverar aktörer från flera sektorer och kräver snabb samordning under osäkerhet, utgör övning ett avgörande verktyg för att pröva och förbereda samverkan i praktiken.

Övning utgör ett av verktygen för att höja kunskapen om hantering och de ingående aktörernas arbetssätt, samt synliggör behov av utveckling. Ett mervärde med övning är att det bidrar till att bygga relationer och att stärka nätverket vilket kan sänka trösklar i en skarp hantering.

Stärka Forum för operativa chefer

Åtgärden syftar till att förtydliga forumet för operativa chefer samt säkerställa att deltagande myndigheters representanter har tydliga mandat för aktörsgemensam inriktning och samordning.

Det befintliga forumet för operativa chefer är inte utformat eller bemannat för den operativa rytm som krävs vid händelser. Däremot skulle det kunna utvecklas för att ge stöd vid hantering av händelser, särskilt med avsikt att hantera gemensamma behov, frågeställningar och målkonflikter som inte kan hanteras bilateralt eller i en eventuell ISF.

OpC-forum är en del av strukturen för inriktning och samordning på central nivå och är utgångspunkten för ordinarie samverkan. Erfarenheter från tidigare händelser har visat att det finns behov av att stärka forumets funktionalitet även i skarpa lägen. För att OpC-forum ska kunna användas som ett effektivt forum även vid stärkt samverkan anser därför MSB att:

- Deltagande och tillkommande myndigheter säkerställer att representanten i forumet har ett relevant beslutsmandat, i linje med myndighetens uppdrag och interna ledningsprinciper.
- Forumets roll och användning i skarp händelse bör tydliggöras i respektive myndighets rutiner för operativ samverkan.

- Stödjande strukturer för forumet bör ses över – inklusive kontinuitet, sambandslösningar och sekretesshantering.

Stärka tvärsektoriell analysförmåga till stöd för inriktning och samordning

Åtgärden syftar till att skapa analys- och beslutsstöd vid hantering av händelser kopplade till kritisk undervattenstruktur. I *Gemensamma grunder – ramverk för ledning och samverkan* beskrivs aktörsgemensamt analys- och beslutsstöd som ett komplement till ISF vid hantering av händelser. Förberedande tematisk samverkan mellan berörda aktörer skulle kunna skapa goda förutsättningar för både ISF och analys- och beslutsstöd genom att skapa gemensam förståelse för hot, risker, sårbarheter och konsekvenser kopplat till undervattensinfrastruktur. För att skapa en sådan förståelse bör en tvärsektoriell analysgrupp inrättas.

Syftet med analysgruppen är att skapa relationer, sänka trösklar för informationsdelning och samverkan, samt diskutera risk- och hotbilder kopplade till undervattensinfrastruktur. Detta forum ska också kunna verka för en samlad analys över tid och successivt bidra till att bredda perspektivet mot den maritima domänens samlade riskbild.

För att merutnyttja befintliga forum och strukturer bör Sjöövervakningsrådet användas som värdstruktur för detta syfte. Utveckling pågår under ledning av Kustbevakningen.

MSB har initierat ett uppstartsmöte i juni 2025 med representanter från samtliga myndigheter i regeringsuppdraget, med fokus på kontaktskapande och gemensam förståelse för hur analysförmåga kan stärkas som stöd till operativ ledning. Under mötet diskuterades särskilt hur Sjöövervakningsrådet kan nyttjas för det föreslagna syftet.

Mot bakgrund av Sjöövervakningsrådets struktur kommer analysgruppen främst verka inom ramen för samordning och gemensam analys i det förebyggande och kapacitetshöjande arbetet, snarare än vid operativ hantering. Men vid en händelse ska analysgruppen vid behov kunna samverka med syfte att skapa en tvärsektoriell förståelse för konsekvenser och förändrade hot- och riskbilder vid behov.

Utveckla händelsespecifik lägesbild med tvärsektoriell analys vid en händelse eller förhöjd risk

Åtgärden syftar till att ta fram en lägesbild som ger samlad överblick, förståelse och underlag till beslut och åtgärder i det aktörsgemensamma arbetet. MSB ska ha förmåga att vid en händelse eller förhöjd risk rörande skada på kritisk undervattensinfrastruktur skapa en händelsespecifik lägesbild som innehåller tvärsektoriella analyser och bedömningar. Lägesbilden ska vara ett urval av information från flera aktörer och andra källor som analyseras och sammanställs i form av beskrivningar och bedömningar av läget.

Fokus ligger på att skapa ett snabbt och relevant beslutsunderlag. En viktig förutsättning för att producera en händelsespecifik lägesbild med tvärsektoriella analyser är effektiv informationsförsörjning. Den händelsespecifika lägesbilden avseende skada på kritisk undervattensinfrastruktur ska bygga på den sjölägesbild som Kustbevakningen ansvarar för, tillsammans med lägesbilder och information från andra, på förhand, utpekade aktörer som bedöms vara centrala vid en händelse eller förhöjd risk. Inhämtning sker både via löpande informationsdelning och riktade informationsbegäranden om behov uppstår.

Målgruppen för den händelsespecifika lägesbilden ska främst vara berörda aktörer för att skyndsamt bidra till en samordnad aktörsgemensam hantering. Lägesbilden ska delges Regeringskansliet i syfte att hålla regeringen informerad och möjliggöra beslutsfattande på nationell nivå.

Övning med fokus på att stärka operativ hantering i OpC-forum

Åtgärden syftar till att genom kontinuerlig övning stärka OpC som forum för inriktning och samordning. Fokus ligger på att fördjupa kunskap, bygga relationer och säkerställa förmåga till gemensam hantering i stärkt samverkan.

I april 2025 genomfördes en första övning i OpC-forum med deltagande från flera aktörer inom både kritisk infrastruktur och hybridproblematik. Övningen visade på behov av att tydliggöra OpC roll, fortsätta öva och vikten av ändamålsenliga tekniska ledningsstödssystem.

En ytterligare övning i OpC-forum kommer genomförs under hösten 2025, med fokus på att pröva forumets funktion i scenario präglat av hybrid påverkan. Syftet är att ytterligare utveckla forumets förmåga till snabb samverkan, koordinering och beslutsfattande – med tydlig koppling till det civila försvarets förmågeuppbyggnad samt Nato/EU-samarbete.

Deltagande i relevanta övningar avseende kritisk undervattensinfrastruktur

Åtgärden syftar till att stärka förmågan till aktörsgemensam hantering av incidenter och störningar kopplade till kritisk undervattensinfrastruktur, både nationellt och internationellt genom övningar som rör både energiförsörjning och elektronisk kommunikation.

Ett exempel är Nato-övningen *Coherent Resilience 2025 (CorEX25),* som genomförs i Sverige under hösten 2025. Övningen fokuserar på energisäkerhet och resiliens i Arktis, och omfattar analys och hantering av hybridhot såsom cyberattacker, desinformation och sabotage. Den syftar även till att stärka samverkan mellan Nato-länder, partnerorganisationer och civila aktörer samt att utveckla strategier för krisberedskap inom energisektorn. Deltagande i CorEX25 fördjupar det svenska Nato-engagemanget och stärker förståelsen för hur maritima incidenter och hybridhot påverkar Sverige som allierad. Övningen ger också möjlighet att pröva planer i ett internationellt sammanhang och stärka civilt-militärt samspel.

Inventering av nuläge och gemensamma behov utifrån typhändelsen i regeringsuppdraget

I april 2025 genomfördes en övning i forum för operativa chefer, med fokus på undervattensinfrastruktur. En utkomst av denna övning är en fördjupad behovsanalys av sambandsmedel och tekniska stödsystem utifrån typhändelsen. Regeringsuppdraget ger en möjlighet att tydliggöra de samlade behoven som en effektiv aktörsgemensam hantering kräver.

Fokus i inventeringen har legat på gemensamma och interoperabla lösningar, med utgångspunkt i befintliga systemutbud och tekniskt kompatibla alternativ. Behovet av tydlighet har förstärkts kring vilka tekniska stödsystem som ska användas när och av vem för informationsdelning vid operativ hantering i fred, höjd beredskap och krig – samt att säkerställa att dessa system är tillgängliga för de aktörer som behöver dem.

Bedömda effekter av genomförda och initierade åtgärder

De genomförda och initierade åtgärderna bedöms sammantaget stärkt samhällets förmåga att upptäcka avvikelser, snabbt larma alla relevanta aktörer och skapa en samlad lägesbild vid incidenter och störningar i kritisk undervattensinfrastruktur. Omhändertagande av lärdomar från operativ hantering har pågått intensivt sedan hösten 2024.

Inom fokusområdet *stärkt förmåga till att upptäcka, larma och informationsförsörja* har flera initiativ initierats för att förbättra möjligheten till tidig upptäckt och snabb informationsförsörjning. Kustbevakningens uppbyggnad av en civil sjöövervakningscentral, utvecklingen av en gemensam normallägesbild och utbyggnad av maritim underrättelseverksamhet samt förtydligade larmrutiner kommer skapa bättre förutsättningar för kontinuerlig övervakning och kortare ledtider i larmkedjan. Informationsflöden har setts över och testats genom övning, vilket stärkt förmågan att agera redan vid indikation om händelser. Inom området fortsätter arbetet med att förbättra informationsförsörjning, särskilt från privata aktörer vars infrastruktur är avgörande men där dagens rapporteringsvägar inte alltid fångar upp tidiga signaler. PTS har påbörjat ett arbete som kombinerar juridisk analys med praktiska lösningar för att möjliggöra snabbare och mer träffsäker rapportering och Sjöfartsverket har arbetat med att stärka kapaciteten i sjötrafikcentralerna (VTS, Sweden Traffic), vilket kan möjliggöra effektivare övervakning, trafikledning och förebyggande åtgärder som kan bidra till att stärka den gemensamma lägesbilden.

Inom fokusområdet *stärkt förmåga till inriktning och samordning* har förmågan till gemensam samordning och inriktning förstärks genom ett påbörjat arbete att förtydliga OpC Forums roll och mandat. Forumet har stärkts genom att dess roll tydliggjorts med stöd av tvärsektoriella analyser som på sikt kan fungera som ett effektivt analys- och beslutsstöd vid en hantering. För att merutnyttja befintliga

forum och strukturer kommer Sjöövervakningsrådet användas med förslaget att inrätta en analysgrupp på den taktiska nivån i rådet eller motsvarande existerande analysplattformar. Mot bakgrund av att Sjöövervakningsrådet inte är operativt vid en händelse, kommer analysgruppen främst verka inom ramen för samordning och gemensam analys i det förebyggande och kapacitetshöjande arbetet. Vid en händelse ska en tvärsektoriell analysgrupp kunna sättas samman, med fördel bestående av samma kompetens som finns i Sjöövervakningsrådet, i syfte att skapa en tvärsektoriell förståelse för konsekvenser och förändrade hot- och riskbilder. Denna ska kunna ta fram underlag för beslut på flera nivåer i systemet. Därutöver har förmågan till framtagande av en händelsespecifik samlad lägesbild stärkts. Gemensam begreppsförståelse har ökat och ett proaktivt förhållningssätt har stärkts.

Inom området förstärks dessutom den operativa samordningen genom planerade övningar, bland annat i OpC-forum, med syftet att befästa roller, kontaktvägar och gemensam beslutsförmåga vid komplexa händelser. Genom återkommande deltagande i relevanta övningar utvecklas också förmågan att agera koordinerat i en bredare totalförsvarskontext.

För att möta de behovs som finns inom fokusområdet *stärkt förmåga till säkra kommunikationer* inleds åtgärder för att tydliggöra och säkra tekniska system som krävs för ledning och informationsförsörjning vid operativ hantering, utifrån den behovsanalys som genomförts. Fokus ligger dels på vilka system som ska nyttjas, dels på hur de faktiskt ska användas i praktiken – inklusive tilläggstjänster, användarstöd och säkerhetsaspekter. Den förväntade effekten är att olika funktioner vid respektive myndighet snabbt ska kunna kommunicera via tal, skrift och video i alla lägen.

Synergier med angränsande utveckling

Parallellt med uppdraget pågår ett antal utvecklingsarbeten som inte startats inom ramen för regeringsuppdraget, men som tydligt ökar förmågan inom detta område. Genom att inkludera dessa utvecklingsarbeten i rapporten tydliggörs synergier som sammantaget stärker den samlade förmågan.

Utveckling av Sjöövervakningsrådets roll

Sjöövervakningsrådet bör vara det forum som används för att se till att flera av de åtgärdsförslag och rekommendationer som har identifierats i uppdraget omhändertas. Det kan också handla om vidare analys avseende resurser, förmågor och sårbarheter som alla myndigheter i rådet identifierar. Inom ramen för Sjöövervakningsrådet har bland annat ett arbete för att ta fram en ny nationell sjöövervakningsstrategi påbörjats.

Det finns en begränsning i förordning (2019:84) med instruktion för Kustbevakningen för hur många ledamöter som kan ingå i rådet. För att ytterligare förstärka arbetet att skydda kritisk undervattensinfrastruktur kan det övervägas att fler myndigheter ingår i rådet eller adjungeras utifrån behov. En hemställan har skickats till regeringen om vissa regeländringar för att underlätta informationsdelning mellan myndigheterna samt möjliggöra utveckling av Kustbevakningens underrättelseverksamhet.

Skapa civil sjöövervakningscentral för förstärkt sjölägesbild

Kustbevakningen har initierat en organisationsförändring för att förstärka sin dygnet-runt-kapacitet i syfte att upprätthålla en mer taktisk sjölägesbild, tidigare identifiera och detektera avvikelser för att säkerställa proaktivitet, avskräckning och snabba rapporteringsvägar. Organisationsförändringen är en del av Kustbevakningens förstärkning av sin underrättelseverksamhet.

En civil sjöövervakningscentral för förstärkt övervakning av exempelvis sjötrafik, ett geografiskt område och förmedling av aktuell sjölägesinformation är under uppbyggnad. Informationsinhämtningen sker genom information från Kustbevakningens plattform för sjöövervakning, Sjöbasis. Syftet är dels att bli mer proaktiva och kunna planera och leda den egna verksamheten på ett mer riktat sätt, dels för att andra myndigheter ska kunna göra motsvarande i sina uppdrag.

Sjöövervakningscentralen ska ses som ett komplement till Kustbevakningens operativa ledningscentral och kunna ge en mer analyserad bild av sjölägesinformationen, eventuella anomalier och bidra till högre beredskap för att skyndsamt kunna hantera incidenter i den maritima miljön. En samlad sjölägesbild är beroende av Försvarsmaktens ansvar att samla in, bearbeta och lämna Kustbevakningen sjölägesinformation som är sammanställd för civila behov.[9]

Sjöövervakningscentralen kommer att vara igång dygnet runt och säkerställa direktkommunikation, via Kustbevakningens ledningscentral, med de samverkansmyndigheter som behöver tidiga uppdateringar av sjölägesbilden och identifierade risker.

Sjöövervakningscentralen ska vara inrättad och uppstartad i september 2025. Därefter följer fortsatt uppbyggnad och utveckling där informationsdelning och samverkan med andra aktörer kommer att vara avgörande för sjöövervakningscentralens förmåga att tidigt identifiera och detektera avvikelser.

Utveckling av tvärsektoriell lägesbild genom ökad digitalisering

Störningar av undervattensinfrastruktur är en av många slags incidenter som inträffar och som riskerar att påverka ett flertal sektorer och stora geografiska

[9] Se 17 § förordning (2024:1333) med instruktion för Försvarsmakten

områden, på land såväl som till sjöss med omfattande samhällsstörningar som följd. Dessa händelser ingår ofta i ett sammanhang där flera parallella incidenter påverkar varandra och där aktörers förmåga inte enbart påverkas i den maritima miljön. För att snabbt upptäcka kritiska händelser av hybridkaraktär och för att initiera effektiva och relevanta aktörsgemensamma åtgärder krävs en överblick över hybridhotets hela kontext. Det involverar större och bredare informationsmängder samt påverkar fler aktörer än vad det här uppdraget har omfattat.

MSB har ett pågående arbete att som ledande myndighet för civilt försvar och utifrån ett tvärsektoriellt perspektiv stärka förmågan till tidig upptäckt samt stärka förmågan att förse regeringen med information. Inom ramen för detta arbete utvecklas metoder för automatiserad insamling och bearbetning av data, inklusive information rörande kritisk undervatteninfrastruktur. Metoden bygger på ett nära samspel med berörda myndigheter och organisationer, vars analyser och kvalitetssäkring utgör centrala komponenter för att uppnå en relevant lägesbild samt att korta tiden från upptäckt till medvetet beslutsfattande.

Behovsanalys för system och sensorutveckling samt övrig utveckling

Störningar i kraftnät och elektronisk kommunikation upptäcks i regel omedelbart av nätägare med egna sensorer för leverans av energi eller kommunikation. Information om sådana störningar behöver snabbt delas mellan privata aktörer och ansvariga myndigheter. Framtagande av en fördjupad analys avseende system och sensorutveckling med koppling till sjöövervakningscentralen och Kustbevakningens uppdrag inom den civila sjölägesbilden utvecklas.

För att säkerställa en än säkrare och mer verifierad sjölägesbild behövs en utökning av sensorinhämtning i kombination med ökad samverkan i underrättelseverksamheten. Detta kommer att vara en del av den fördjupande analysen. Kustbevakningen planerar även att fördjupa underrättelsearbetet kopplat till sjöövervakningsuppdraget, där hemställan om lagändring skickats till Regeringskansliet.

PTS bedriver, med stöd i form av finansiering från MSB och Anslag 2:4, ett projekt som syftar till investeringar i sensorer för övervakning av fiberoptiska kablar på havsbotten. Detta och andra liknande satsningar kan på sikt förhoppningsvis förbättra förutsättningarna för att utreda vad som skett och utpeka ansvar vid skador på fiberoptiska kablar, och även möjligheten till viss förvarning innan ett brott av en kabel har inträffat.

Sambandsmedel för civila myndigheter

Det finns detaljerade nationella riktlinjer för hur Rakel ska nyttjas ur ett beredskapsperspektiv. I MSB:s föreskrifter om civila myndigheters

signalskyddsberedskap (MSBFS 2025:3)[10] om civila myndigheters signalskyddsberedskap regleras vilka signalskyddssystem som ska nyttjas av civila myndigheter. MSB:s föreskrifter och allmänna råd om statliga myndigheters uppgifter inför och vid höjd beredskap (MSBFS 2025:4) gör vidare gällande att Rakel, SGSI och WIS ska användas av samtliga beredskapsmyndigheter senast den 1 juni 2026.[11] Alla beredskapsmyndigheter har tillgång till Rakel och WIS, men en handfull av dessa saknar idag anslutning till SGSI.

MSB anser att samtliga beredskapsmyndigheter bör ansluta sig till MSB:s tjänst PGAI mobil för tal och meddelanden till nivå BH samt SGSI videokonferens BH när den är tillgänglig i slutet på 2025. Om de aktörer som är anslutna till SGSI även ansluter sig till tjänsterna PGAI mobil och SGSI videokonferens ökar möjligheterna för effektiv samordning markant.

MSB har möjlighet att även erbjuda SGSI, Rakel och WIS till kommuner, regioner och annan samhällsviktig verksamhet men det finns inget krav att dessa ansluter sig. Skulle fler aktörer utöver beredskapsmyndigheter ansluta sig ökar förutsättningar för effektiv aktörsgemensam samordning ytterligare.

Arbete i Kommunikationsdirektörsnätverket

Med anledning av det förändrade säkerhetsläget har inriktningar avseende kommunikation och budskap uppdaterats. Arbetet med de aktörsgemensamma dokumenten leds av Kommunikationsdirektörsnätverket (KOMDIR). Uppdraget gavs till KOMDIR och Kommunikatörsforumet av Polismyndigheten och OpC Forum att ta fram ett underlag för att tydligare adressera osäkerheter vid hanteringen av potentiella hybrida hot. Underlaget redovisas i juni och ska därefter implementeras genom ordinarie strukturer och arbetsmetoder på central nivå.

Rekommendationer

Utöver de åtgärder som genomförts eller initierats inom ramen för uppdraget lämnas också ett antal rekommendationer med sikte på fortsatt utveckling. Dessa avser huvudsakligen strukturella eller långsiktiga åtgärder till exempel förändringar i regelverk, organisatoriska förutsättningar eller systemstöd.

Flera av dessa rekommendationer berör inte enskilda aktörer, utan förutsätter fortsatt dialog, förankring och samverkan mellan myndigheter och andra centrala aktörer. Vissa rekommendationer kan även kräva initiativ på politisk nivå eller från Regeringskansliet.

[10] MSB:s föreskrifter om civila myndigheters signalskyddsberedskap MSBFS 2025:3. Föreskrifterna träder i kraft den 1 juli 2025 och ersätter föreskrifterna i MSBFS 2023:3 som då upphör att gälla.
[11] Föreskrifterna och de allmänna råden trädde i kraft den 1 juni 2025. Enligt föreskrifternas övergångsbestämmelser ska 15 § och 5 § om gemensamma tekniska system för ledning och samverkan vara uppfylld senast 1 juni 2026, https://www.msb.se/sv/aktuellt/nyheter/2025/maj/msb-ger-ut-foreskrifter-och-allmanna-rad-om-statliga-myndigheters-uppgifter-infor-och-vid-hojd-beredskap/.

Stärkt informationsförsörjning till Regeringskansliet

Rekommendationen syftar till att säkerställa snabbare och mer samordnad informationsförsörjning om incidenter och störningar till Regeringskansliets olika departement och funktioner från berörda myndigheter och MSB.

Myndigheterna föreslår en aktivitet där myndigheternas TiB-funktioner (eller motsvarande) träffas tillsammans med berörda TiB-funktioner i Regeringskansliet i syfte att tydliggöra myndigheternas kontaktvägar in till Regeringskansliet för att ta fram en samlad struktur för effektiv informationsförsörjning.

Uppdrag och finansiering för säkra kommunikationer

Med hänvisning till avsnittet *synergier med angränsande utveckling* förslår MSB utifrån myndighetens roll och ansvar att ett uppdrag med tillhörande finansiering bör ges med särskilt fokus att öka anslutningstakten hos kommuner, regioner och andra samhällsviktiga aktörer. MSB anser att det är önskvärt att få en snabbare effekt och bredare spridning av SGSI med tillhörande tilläggstjänster PGAI Mobil och SGSI videokonferens för att därigenom öka förmågan till aktörsgemensam samordning. Därför anser MSB att ett uppdrag med tillhörande finansiering bör ges med särskilt fokus att öka anslutningstakten hos kommuner, regioner och andra samhällsviktiga aktörer.

Nationell sambandsplanering

De civila aktörernas förmåga att kommunicera på ett effektivt och säkert sätt måste stärkas och påskyndas. Det finns behov av centraliserad styrning för att tillse medvetna val för att säkerställa den samlade operativ förmågan och undvika onödigt kostnadsdrivande åtgärder för berörda myndigheter.

För att säkerställa en effektiv informationsförsörjning behövs en övergripande sambandsplanering för hela totalförsvaret som också kan användas vid operativ hantering i fred inom ramen för krisberedskapen. MSB är sammankallande för det aktörsgemensamma forum för teknik och lokaler för ledning och samverkan som arbetar med att ta fram stöd och struktur för sambandsplanering i form av process för sambandsplanering, begreppsdefinitioner, förslag på organisation m.m.

Behov av skyndsam handläggning av tillstånd för sjömätning

Möjligheten för berörda aktörer att samla in information om bottenförhållanden begränsas av den lagstiftning som reglerar skyddet av sjögeografisk information.[12]

[12] Se 3 § lag (2016:319) om skydd av geografisk information, 2 § Förordning (2016:320) om skydd för geografisk information samt Lag (1966:314) om kontinentalsockeln

Informationen är kritiskt för att skapa en lägesbild både i proaktivt underhållssyfte samt för att påskynda reparationsförmågan vid en incident.

Försvarsmakten bedömer att geografisk information är mycket skyddsvärd och myndighetens ståndpunkt är att sjögeografisk information är särskilt skyddsvärd. Högupplöst djupinformation tillsammans med information om bottentopografi, bottenbeskaffenhet, anläggningar, kablar och andra konstgjorda företeelser ger en detaljerad bild av havsbotten, vilket är viktigt vid planering och genomförande av undervattensföretag. Sådan information kan därför ge främmande makt stora strategiska, operativa eller taktiska fördelar.

Försvarsmaktens intresse av att skydda informationen måste därför balanseras mot intresset av proaktivt underhållsarbete samt att snabbt kunna avhjälpa brott på kablar. Om Svenska kraftnät, Post- och telestyrelsen eller en därtill knuten aktör är i behov av att undersöka botten i proaktivt underhållssyfte eller vid en incident så behöver dessa aktörer snabbt kunna inhämta ett tillstånd av tillräcklig omfattning för att kunna utföra underhållsarbete samt undersöka och utföra reparationer på platsen. Detta kan utan författningsändringar åstadkommas på åtminstone två sätt, antingen genom att en tillståndsansökan kan handläggas i ett snabbspår hos försvarsmakten eller genom att tillstånd för att utföra sjömätning på nödvändiga delar av kabelsträckningen meddelas på förhand och i så fall med de begränsningar som försvarsmakten anser nödvändiga.

I de fall spridning mellan flera iblandade aktörer måste ske behöver tillstånd för detta kunna handläggas med samma skyndsamhet som tillståndet för sjömätningen. Ett förenklat tillståndsförfarande bör utredas. Tillstånden kan och bör förenas med nödvändiga villkor.[13]

[13] Se 9 § 3 st. Lag (2016:319) om skydd för geografisk information

Bilaga

Bilaga 1 - Försvarsmaktens synpunkter på MSB utkast 3 ”Åtgärder för att stärka det civila försvarets förmågeutveckling för att hantera incidenter kopplade till undervattensinfrastruktur”.

Ett samarbete mellan:

FÖRSVARSMAKTEN

Yttrande

Datum
2025-06-10

Beteckning
FM2025-15512:3 Sida 1 (7)

Säkerhetsskyddsklass
ES

Enligt sändlista

Ert tjänsteställe, handläggare | Ert datum | Er beteckning

Vårt tjänsteställe, handläggare | Vårt föregående datum | Vår föregående beteckning
Försvarsstabens Strategienhet,
Anton Arnesson

Försvarsmaktens synpunkter på MSB utkast 3 ”Åtgärder för att stärka det civila försvarets förmågeutveckling för att hantera incidenter kopplade till undervattensinfrastruktur”

Försvarsmakten har fått möjlighet att lämna synpunkter på Myndigheten för samhällsskydd- och beredskaps utkast till svar på regeringsuppdraget att stärka det civila försvarets förmågeutveckling för att hantera incidenter kopplade till undervattensinfrastruktur (Fö2025/00713) och framför följande.

Övergripande

Försvarsmakten anser att det är mycket positivt att berörda myndigheter i det civila försvaret ökar sin förmåga att hantera incidenter kopplade till hot mot undervattensinfrastruktur.

Försvarsmakten har i ett yttrande till Regeringskansliet (Försvarsdepartementet), framfört att Sverige i dag står inför en mångfacetterad hotbild. Antagonistiska åtgärder och angrepp genomförs mot Sverige. Hoten riktar sig främst mot civila funktioner i samhället och måste primärt hanteras inom den ordinarie verksamheten hos civila myndigheter, bl.a. Polismyndigheten, Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap (MSB), Kustbevakningen och Tullverket. Det ställer tydliga krav att man i dessa verksamheter kan identifiera och möta statsunderstödda antagonistiska hot i fredstid. Förmågan att identifiera och hantera denna typ av hot måste förbättras inom olika myndigheter och i det civila försvaret samlat.[1]

[1] Försvarsmakten, *Försvarsmaktens bedömning beträffande befogenheter och ansvar, analys kring risk och sårbarhet samt förslag till åtgärder beträffande kritisk undervattensinfrastruktur*, FM2024-1870:3

Postadress: Försvarsmakten, 107 85 Stockholm
Besöksadress: Lidingövägen 24
Telefon: 08-788 75 00
Telefax: 08-788 77 78
E-post, Internet: exp-hkv@mil.se, www.forsvarsmakten.se

Försvarsmakten välkomnar således initiativet att öka förmågan inom det civila försvaret att hantera incidenter kopplade till hot mot undervattensinfrastruktur.

Försvarsmaktens synpunkter

Försvarsmakten anser att det i den fortsatta beredningen av regeringsuppdraget finns behov av att komplettera eller korrigera utkastet till rapport enligt myndighetens synpunkter nedan och vill särskilt betona vikten av de första tre.

1. *Försvarsmaktens anser att en sammanställd sjölägesbild, i form av ett nationellt sjöläge, ska ligga i Försvarsmakten*

Den absoluta merparten av tillgänglig sjölägesinformation[2] över svenskt territorialvatten och maritima zoner inhämtas av Försvarsmakten, som delger Kustbevakningen sjölägesinformation sammanställd för civila behov.[3] Informationen kompletteras därefter med civil sjölägesinformation och förmedlas[4] till berörda myndigheter, genom Kustbevakningens myndighetsgemensamma system för Sjöövervakning – Sjöbasis. Den uppbyggnad som föreslås av en civil sjöövervakningscentral vid Kustbevakningen är således helt avhängig Försvarsmaktens inhämtning och delgivning, vilket bör beskrivas i svaret på regeringsuppdraget.

Försvarsmakten anser att det finns behov av att ta fram en nationell sjölägesbild[5], d.v.s. att göra en sammanställning av Kustbevakningens civila sjölägesbild och Försvarsmaktens militära sjölägesbild. För att kunna ta fram en sådan sjölägesbild måste det finnas förmåga att hantera säkerhetsskyddsklassificerad information, samt att utbyta information med våra allierade inom Nato. Försvarsmakten konstaterar att flera andra nationer har dedikerade funktioner/organisationer[6] för samordning och koordinering beträffande undervattensinfrastruktur, där relevanta offentliga eller privata aktörer som äger kritisk undervattensinfrastruktur ingår.[7] Försvarsmakten anser att en motsvarande funktion behövs i Sverige, exempelvis i form av ett nationellt maritimt säkerhets- och ledningscenter, samt att det vore lämpligt om ansvaret för ett aktuellt och sammanställt sjöläge låg hos Försvarsmakten. Det senare genom en sammanställning av egen sensorinformation och andra informationskällor vid berörda myndigheter eller aktörer.[8] Med anledning av ovan anser Försvarsmakten därför att

[2] Sjölägesinformation är aktuella eller historiska uppgifter om till exempel fartyg och andra föremål som rör sig på sjön. Uppgifterna kan t.ex. vara fartygets kurs, fart, position och identitet (fartygsnamn och flaggstat)
[3] Enligt 17 § förordning (2024:1333) med instruktion för Försvarsmakten
[4] Enligt 15 § förordning (2019:84) med instruktion för Kustbevakningen
[5] Sjölägesbild är flera olika aktuella eller historiska data med indirekt eller direkt geografisk koppling som täcker en eller flera verksamheter
[6] Inom Nato benämns det sammanställda sjöläget som MSA (Maritime Situational Awarness) och består både av militär och civil (MPOL-Maritime Patterns of Life) information
[7] Försvarsmakten, *Försvarsmaktens bedömning beträffande befogenheter och ansvar, analys kring risk och sårbarhet samt förslag till åtgärder beträffande kritisk undervattensinfrastruktur*, FM2024-1870:3
[8] Försvarsmakten, *Försvarsmaktens remissyttrande över Kustbevakningens hemställan om lag- och förordningsändringar,* FM2025-9520:2

förslaget om att inrätta en civil sjöövervakningscentral vid Kustbevakningen bör strykas.

Som Försvarsmakten tidigare framfört med anledning av Försvarsberedningens rapport Kraftsamling, utgör Kustbevakningens sjöövervakning ett viktigt komplement till Försvarsmaktens verksamhet.[9] Det är således viktigt att det genomförs samverkan och operativ informationsdelning mellan Försvarsmakten, Kustbevakningen och övriga statliga maritima myndigheter. Försvarsmakten anser att det är av särskild betydelse att Kustbevakningen kan komplettera Försvarsmaktens sjölägesbild med en uppdaterad civil sjölägesbild och därmed bidra till en mer sammansatt och komplett militär sjölägesbild. Bland annat med anledning av detta så finns det skäl att närmare analysera vilken typ av information som är avsedd att behandlas i Sjöbasis, både avseende analysernas innehåll och eventuellt behov av att tillföra ytterligare information från de olika myndigheterna. Om det är fråga om uppgifter som enskilt eller aggregerat är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585) behöver också förutsättningarna finnas på plats för att hantera sådan information.

Angående samverkan och informationsdelning mellan Försvarsmakten och Kustbevakningen bör arbetet med den fortsatta beredningen av rapporten beakta slutsatserna från regeringens uppdrag till Försvarsmakten och Kustbevakningen om stärkt samverkan till sjöss. [10]

Försvarsmakten vill i sammanhanget även lyfta behovet av att det görs en mer samlad översyn av ansvarsfördelningen och samordningen mellan totalförsvarets aktörer i fråga om maritim säkerhet (inkluderande en dedikerad funktion/organisationer för samordning, koordinering och samanställd sjölägesbild) i en nationell och internationell kontext, exempelvis i form av en statlig utredning. Transportstyrelsen har i en rapport[11] nyligen tryckt på behov av en statlig utredning beträffande maritim säkerhet. Försvarsmakten delar uppfattningen att en sådan utredning är angelägen och anser att en sådan med fördel kan föreslås i aktuellt uppdrag om kritisk undervattensinfrastruktur.

Beträffande samrådsorganet för civil sjöövervakning (Sjöövervakningsrådet) samverkar Försvarsmakten i dagsläget med Kustbevakningen på såväl strategisk som operativ och taktisk nivå. Försvarsmakten anser att Sjöövervakningsrådet är ett värdefullt forum för samordnat stöd till Kustbevakningen och instämmer i att det finns en potential i att utveckla Sjöövervakningsrådets arbete. Det är dock viktigt att det tydligt framgår att Sjöövervakningsrådet endast är ett samverkansorgan utan eget mandat att fatta beslut för respektive myndighets räkning och att myndigheterna som deltar i rådet själva styr över de resurser som de bidrar med, d.v.s. att

[9] Försvarsmakten, *Försvarsmaktens svar på regeringsuppdrag Kraftsamling,* FM2024-6830:2
[10] Försvarsmakten, *Slutredovisning Uppdrag till Försvarsmakten och Kustbevakningen om stärkt samverkan till sjöss (Fö2025/00038),* FM2025-6182:5
[11] Transportstyrelsen, *Ett ökat hamnskydd*, TSG 2024-3102, 2025-03-31

Kustbevakningen inte har mandat att fatta beslut om hur resurserna i Sjöövervakningsrådet ska nyttjas.

2. *Försvarsmakten ser ytterst begränsade möjligheter till lättnader i skyddet eller spridningen av djupdata eller annan sjögeografisk information med hänsyn till behovet av säkerhetsskydd kring dessa*

Av utkastet till rapport framgår att ”trösklarna för informationsdelning behöver sänkas”, samt att ”förmågan att samla in information om bottenförhållanden begränsas av den lagstiftning som reglerar skyddet av sjögeografisk information”. Rapporten rekommenderar därför att lagstiftningen[12] kring skydd för geografisk information ses över. Försvarsmakten anser denna rekommendation vara mycket problematisk. Försvarsmakten delar regeringens bedömning[13] att regelverket gällande skydd för geografisk information är av stor betydelse givet det försämrade säkerhetsläget och avstyrker rekommendationen att se över lagstiftningen, med nedan motivering.

Betydande delar av den svenska kusten har en unik geografi i form av skärgårdar med stora djup och avsevärda bottentopografiska variationer, samt områden med stora mängder av grund, vilket historiskt har utnyttjats som en naturlig del i försvaret av landet och som basområden för egna stridskrafter. Detta tillsammans med informationens mycket långa varaktighet samt de strategiska, operativa och taktiska fördelar som högupplöst djupinformation kan ge, innebär att djupinformationen inom vissa geografiska områden fortsatt är skyddsvärd. Ett frisläppande av djupinformation över det svenska sjöterritoriet kan få stora operativa och taktiska negativa konsekvenser. [14]

Försvarsmakten bedömer att sammanställda[15] uppgifter om militärgeografiska förhållanden underlättar en främmande makts krigsplanläggning. Mot denna bakgrund bedömer Försvarsmakten att geografisk information är mycket skyddsvärd och myndighetens ståndpunkt är att sjögeografisk information är särskilt skyddsvärd. Högupplöst djupinformation tillsammans med information om bottentopografi, bottenbeskaffenhet, anläggningar, kablar och andra konstgjorda företeelser ger en detaljerad bild av havsbotten, vilket är viktigt vid planering och genomförande av undervattensföretag. Sådan information kan därför ge främmande makt stora strategiska, operativa eller taktiska fördelar. Ett frisläppande av sjögeografisk information skulle på kort sikt medföra att Försvarsmaktens uppgift att hävda den territoriella integriteten mot framförallt främmande undervattensverksamhet försvåras avsevärt. På längre sikt kan förmågan att försvara Sverige mot väpnat angrepp

[12] Lag (2016:319) och förordning (2016:320) om skydd för geografisk information
[13] Regeringen, *Översyn av lagstiftningen om spridningstillstånd,* Fö2022/01294, 2022-10-26
[14] Försvarsmakten, *Försvarsmaktens hantering av lag (2016:319) och förordning (2016:320) om skydd för geografisk information*, FM2024-12662:1, 2024-05-06
[15] ”Geografisk information i form av avbildning, beskrivning eller mätning”, enligt 2 § lag (2016) om skydd för geografisk information

begränsas. [16] Med hänsyn till ovan bedömningar anser Försvarsmakten att inga *generella* lättnader ska göras av regelverket för skydd av geografisk information.

3. *Försvarsmakten anser att svaret på regeringsuppdraget i ökad utsträckning bör beakta regeringens styrning att det väpnade angreppet är dimensionerande för utvecklingen av totalförsvaret*

Försvarsmakten anser att rapporten på ett tydligare sätt bör beskriva hur det civila försvarets förmåga att hantera incidenter kopplade till undervattensinfrastruktur, ska fungera vid höjd beredskap och krig. Detta bedöms vara av särskild vikt med anledning av regeringens styrning att det väpnade angreppet är dimensionerande för totalförsvaret och ska ligga till grund för planering för att stärka förmågan inom det civila försvaret. [17, 18]

Försvarsmakten konstaterar att många av förslagen i utkastet till rapport berör Kustbevakningen. Av förordningen (1982:314) om utnyttjande av Kustbevakningen inom Försvarsmakten (den så kallade utnyttjandeförordningen) framgår av 1 § att under krig skall personal och materiel ur Kustbevakningen inom Försvarsmakten användas för övervakning, transporter och andra uppgifter enligt närmare överenskommelse mellan Försvarsmakten och Kustbevakningen. Vidare anges att regeringen får föreskriva att detsamma ska gälla även annars under höjd beredskap. Försvarsmaktens föreskrifter[19] och myndigheternas gemensamma överenskommelse tydliggör bland annat operativt ianspråktagande och så kallad särskild samverkan, det vill säga när Kustbevakningen ska samverka med Försvarsmakten om beredskapen höjs inom myndigheten eller Försvarsmakten i andra fall ingriper mot utländska statsfartyg enligt IKFN-förordningen. Försvarsmakten anser att rapporten inte i tillräcklig omfattning beaktat Kustbevakningens roll i höjd beredskap och krig.

För närvarande pågår en dialog mellan Försvarsmakten och Kustbevakningen gällande operativt ianspråktagande av Kustbevakningen. Även detta arbete påverkar de frågor som behandlas i utkastet till rapport, eftersom frågan om hur Försvarsmakten och Kustbevakningen ska agera tillsammans under högsta beredskap påverkar hur systemet kring sjöövervakning bör vara uppbyggt.

4. *Åtgärder inom det civila försvaret för att stärka förmågan att upptäcka och rapportera incidenter, inklusive samverkan med verksamhetsutövare*

Av regeringsuppdraget framgår att ”Myndigheterna ska utifrån sina respektive författningsstyrda uppgifter och mandat, samt inom givna ekonomiska ramar, stärka myndighetens förmåga att utan dröjsmål upptäcka incidenter och störningar i undervattensinfrastrukturen som riskerar att hota funktionaliteten för samhällsviktig

[16] Försvarsmakten, *Försvarsmaktens hantering av lag (2016:319) och förordning (2016:320) om skydd för geografisk information*, FM2024-12662:1, 2024-05-06
[17] Regeringen, *Gemensamma förutsättningar för utvecklingen av totalförsvaret 2025 – 2030,* Fö2024/02054,
[18] Regeringen, *Inriktning för civilt försvar 2025 – 2030*, Fö2024/02054
[19] FFS 2019:1 Försvarsmaktens föreskrifter om utnyttjande av Kustbevakningen inom Försvarsmakten

verksamhet, samt skyndsamt rapportera dessa händelser till Regeringskansliet och andra berörda myndigheter". I nuvarande utkast av rapporten handlar många av åtgärdsförslagen om *stärkt myndighetssamverkan*, vilket förvisso är viktigt och bra. En stärkt samverkan behöver också genomföras i en gränsöverskridande kontext mellan svenska aktörer och deras motsvarigheter i andra länder. Här är länder i Sveriges närhet av särskild vikt men även samarbeten inom ramen för andra strukturer, exempelvis Nato, EU, Nordefco och JEF. Försvarsmakten bedömer dock att rapporten skulle stärkas om åtgärdsförslagen utvecklades så att den på ett tydligare sätt beskriver hur förmågan inom det civila försvaret att *upptäcka incidenter och störningar* kan öka.

Försvarsmakten konstaterar att det inom svenskt havsområde finns både egna och andra länders kablar för överföring av el, rörledningar för gas och olja samt fiberkablar för telekommunikation och datatrafik. Ägare av berörd infrastruktur är främst privata bolag och operatörer, men utgörs även av statliga bolag eller affärsverk. Säkerhetsskyddslagen (2018:585) gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet. Det kan bl.a. innefatta samhällsviktig infrastruktur för kommunikation och energiförsörjning. Verksamhetsutövaren ska vidta de säkerhetsskyddsåtgärder som behövs med hänsyn till verksamhetens art och omfattning samt övriga omständigheter. Verksamhetsutövaren ska bl.a. förebygga skadlig inverkan på anläggningar eller objekt där säkerhetskänslig verksamhet bedrivs. Med hänsyn till ovan bör rapporten, om möjligt, tydliggöra hur samverkan med berörda verksamhetsutövare kan öka och hur verksamhetsutövarna kan bidra till att upptäcka incidenter och störningar samt delge sådan information till berörda myndigheter.

- o 0 o -

I beredningen av detta ärende har deltagit kommendör Marko Petkovic, kommendörkapten Peter Laurin, överstelöjtnant Morgan Petersson, kommendörkapten Tobias Söderblom, kommendörkapten Fredrik Hansson, överstelöjtnant Martin Skoglund, försvarsjurist Michael Bergström och försvarsjurist Sara Westerlund.

Detta yttrande har beslutats av generalmajor Johan Pekkari. I den slutliga handläggningen har deltagit kommendör Anders Bäckström, sektionschef Jenny Marklund och handläggare Anton Arnesson, den sistnämnda som föredragande.

Pekkari, Johan

Chef för försvarsstabens strategienhet

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.

Sändlista
Myndigheten för samhällsskydd- och beredskap

Inom Försvarsmakten
ÖB/GD Stöd
FST
OPL
MUST
MS