# Styrk kommunens beredskab

En oversættelse af *Nationalt Risikobillede 2025*

August 2025

# Indhold




**Styrk kommunens beredskab**

Bogen er udarbejdet af:
Rasmus Dahlberg, Ph.D., forsker i samfundssikkerhed og beredskab.
Niels Klingenberg Vistisen, cand.mag., krigshistoriker og efterretningsanalytiker.





1. udgave, 1. oplag 2025

KL
Weidekampsgade 10
2300 København S

+45 3370 3370
kl@kl.dk
kl.dk

Produktion: Kommuneforlaget A/S
Design: e-Types
Foto: AdobeStock, Colourbox

Produktionsnr. 831068
ISBN: 978-87-94514-73-6-pdf

# Forord

Ikke siden Anden Verdenskrig har vi set et så alvorligt risiko- og trusselsbillede, som det vi kigger ind i nu. Og det er i høj grad kommunerne, der står forrest, når det handler om at skabe tryghed og beskytte borgerne under længerevarende kriser. Det er her, borgerne for alvor mærker det, hvis eksempelvis et hybrid- eller cyberangreb rammer el-, vand- eller varmeforsyningen eller anden kritisk infrastruktur.

Det Nationale Risikobillede 2025 og de seneste trusselsvurderinger fra Forsvarets Efterretningstjeneste peger derfor på, at der er behov for nye og større krav til kommunernes egne beredskaber og beredskabsplanlægningen på tværs af myndigheder og sektorer.

Det er en stor opgave at opdatere beredskabsplaner til et helt andet niveau, end vi har været vant til. Det Nationale Risikobillede 2025 er en del af det grundlag, der er behov for, men det er langt fra nok. Der er behov for at få oversat truslerne fra det nationale billede til den kommunale kontekst og borgernes hverdag, og hjælpe kommunerne med, hvordan de kan gribe det arbejde an.

Derfor har Rasmus Dahlberg, ph.d., forsker i samfundssikkerhed og beredskab, og Niels Klingenberg Vistisen, cand.mag., krigshistoriker og efterretningsanalytiker, med bidrag fra udvalgte kommuner og beredskaber skrevet denne analyse på foranledning af KL. Analysen skal ses som en del af det videre arbejde med at understøtte kommunerne i deres beredskabsplanlægning og bedst muligt omsætte Det Nationale Risikobillede 2025 til konkrete handlingsplaner.

## Fortsat behov for yderligere meldinger og scenarier

Analysen dækker dog kun noget af behovet. Herunder hvordan man som kommune kan starte med at gribe opgaven an. Det mindsker ikke behovet for, at regeringen og de statslige myndigheder bliver klarere på de risikoscenarier, som vi står overfor, og som vi skal forberede os på.

Der er mange aktører, der gerne vil bidrage til et mere robust samfund – men skal det lykkes, er der behov for, at kommunerne ved, om vi skal planlægge for fx forsyningsnedbrud i 3 dage, en uge eller andet. Og om vi skal forberede os på scenarier, der berører hele landet eller mere lokale nedbrud. Det står fortsat ikke klart, og der er derfor behov for tydelige scenarier og tidshorisonter.

I KL's udspil "Et robust beredskab i en ustabil verden" fra maj 2025 uddyber vi, hvad der er brug for, hvis vores land skal være robust til at kunne klare de kriser, der kan ramme os – både nu og i de kommende år.

God læselyst og beredskabsplanlægning

Martin Damm,
Formand

Kristian Vendelbo,
Adm. direktør

# Styrk kommunens beredskab

Torsdag den 10. april 2025 udgav Styrelsen for Samfundssikkerhed fjerde udgave af rapporten *Nationalt Risikobillede*. I rapportens forord slås det fast, at Danmark i dag "står over for det mest alvorlige og komplekse risiko- og trusselsbillede siden anden verdenskrig". Samtidig beskrives opgaven med at sikre Danmarks modstandsdygtighed over for fremtidens kriser som en fælles opgave.[1]

Helt overordnet viser *Nationalt Risikobillede 2025,* at det ikke længere er en mulighed at sidde på hænderne og afvente udviklingen. Selv om Forsvarets Efterretningstjeneste på nuværende tidspunkt ikke vurderer, at der er en trussel om et regulært militært angreb på Danmark, kan aktiviteter under tærsklen for væbnet konflikt ramme det danske samfund i form af fx cyberangreb, sabotage og påvirkningsoperationer – og kommunerne udgør én af frontlinjerne i denne gråzonekonflikt. Alle kriser, både de intentionelle og de natur- eller teknologiskabte, begynder og slutter nemlig i en kommune.[2] Særligt i forhold til sårbare og udsatte borgere, hvor kommunen har et juridisk eller moralsk ansvar, er det aktuelle risiko- og trusselsbillede relevant.

Denne rapport "oversætter" det nye nationale risikobillede til et kommunalt perspektiv. Formålet er at støtte kommunale beslutningstagere og sagsbehandlere i planlægnings- og prioriteringsarbejdet på beredskabsområdet, sådan at indholdet af det nationale risikobillede bedst muligt omsættes til praktisk og konkret styrkelse af dansk robusthed og beredskab ude i kommunerne. Læsningen af *Nationalt Risikobillede 2025* omsættes i fem konkrete opmærksomhedspunkter rettet mod det kommunale perspektiv. Herefter konkretiseres hybridkrigsbegrebet i kommunal kontekst, og afslutningsvis udfoldes de centrale begreber i *Nationalt Risikobillede 2025*. Dette afsnit kan benyttes som en læsevejledning.

1. https://samsik.dk/nationalt-risikobillede/

2. www.kommunal-rapport.no/meninger/alle-kriser-starter-i-en-kommune/813146

Analysen bygger udelukkende på åbne kilder, først og fremmest *Nationalt Risikobillede 2025,* suppleret med aktuelle trusselsvurderinger fra blandt andet. Forsvarets Efterretningstjeneste, Center for Cybersikkerhed og Energistyrelsen samt interviews med nøglepersoner fra udvalgte kommuner. Der henvises løbende til relevant baggrundsmateriale, men vær opmærksom på altid at anvende seneste version af risiko- og trusselsvurderinger, da situationen konstant udvikler sig.

Det er forfatternes anbefaling, at kommunens politiske og administrative ledelse ofte (som minimum kvartalsvis) modtager en opdateret orientering om det aktuelle risiko- og trusselsbillede for både fysiske forhold og cyberdomænet tilpasset den lokale kontekst – enten udarbejdet af interne rådgivere, af fælleskommunale kompetencecentre eller af statslige myndigheder i det omfang, sådanne er tilgængelige.

# Hvad kan man gøre som kommune?

Der er en lang række forberedelser og tiltag, som kan foretages på kommunalt niveau, og som umiddelbart vil forbedre modstandsdygtigheden over for de aktuelle risici og trusler. Nedenstående fem forslag til indsatsområder er ikke udtømmende, men kan tjene som inspiration og bidrage til at skabe fundamentet for en generel udvikling og mere detaljeret planlægning på kommunalt niveau inden for beredskab og resiliens på baggrund af *Nationalt Risikobillede 2025*.

## 1. Prioritér cybersikkerheden

Danmark er blandt de allermest digitaliserede samfund i verden, og det er ufatteligt nemt og bekvemt, at alt er online – så længe det virker. Men hvis stort set alle samfundsvigtige funktioner er afhængige af digital infrastruktur, bliver det til en sårbarhed, som beredskabsplanlægningen nødvendigvis må tage højde for. I 2024 blev trusselsniveauet for såkaldte "Destruktive cyberangreb" hævet af Center for Cybersikkerhed fra *Begrænset/lav* til *Middel,* mens vurderingen af cyberspionage og -kriminalitet er *Meget alvorlig/høj*.[3] Der er således ingen tvivl om, at cyberområdet bør prioriteres meget højt af alle kommuner. De afledte effekter af en cyberhændelse, hvad enten den er tilsigtet eller utilsigtet, kan være meget omfattende og potentielt lammende for en kommunes evne til at fungere. Det viste TDC-nedbruddet i november 2024 med al tydelighed.[4] Som en kilde udtaler til denne rapport: "Hvis vores sundheds- og omsorgspersonale ikke kan ringe 112, har vi kun brevduer tilbage."

Den væsentligste erkendelse er, at cybersikkerhed er et fælles ansvar i den kommunale organisation frem for noget, der overlades til en IT-afdeling. Hver eneste medarbejder er en frontlinjekæmper i den digitale konflikt, som blandt andet føres med sofistikerede forsøg på at komme ind i kritiske systemer via *social engineering* (manipulation gennem personlige oplysninger etc.). Udviklingen inden for kunstig intelligens gør det stadig vanskeligere at identificere sådanne angreb, hvorfor det er nødvendigt med formaliserede kontrolprocedurer og stringent cyberhygiejne (gode vaner for cybersikkerhed, hvilket nedbringer sandsynligheden for, at organisationen eksempelvis rammes af ransomwareangreb). En vigtig pointe i den forbindelse er, at det kan

3. www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/
4. www.cfcs.dk/da/nyheder/2024/status-pa-driftsforstyrrelser-hos-tdc/


være svært på forhånd at vide, hvilken del af kommunen, der er mest eksponeret for cyberangreb. Eksempelvis har der både i udlandet og i Danmark været angreb på forsyningsvirksomheder via deres bogholderi frem for operationsteknologien, hvilket kan være lige så lammende for driften, hvis der er ikke er passende tiltag i form af adskillelse af netværk og kontinuitetsplanlægning på plads ift. administration.[5]

Med vedtagelsen af ny dansk lovgivning på baggrund af EU's direktiv om cybersikkerhed (NIS2) omfattes kommunerne også, hvilket vil give langt mere stringente fælles retningslinjer, som dog i skrivende stund endnu ikke er fastlagt. Det er imidlertid KL's vurdering, at efterlevelse af ISO27001-standarden og de tekniske minimumskrav er et godt fundament for kommunerne i forbindelse med ikrafttrædelsen af den nye lov om foranstaltninger til sikring af et forhøjet cybersikkerhedsniveau 1. juli 2025.[6]

5. www.version2.dk/artikel/dansk-vandvaerk-ramt-af-hackerangreb-mod-administrative-systemer
6. www.kl.dk/media/rojd4u0o/informationssikkerhed-i-kommunerne-jan-2024.pdf

Konkrete tiltag:

- **Kortlæg** kommunens samfundskritiske funktioner med særligt fokus på afhængigheden af IT-understøttelse, herunder de sårbarheder, som skyldes kritiske leverandørforhold. Findes der analoge backup-planer eller digitale alternativer, som er afprøvet i praksis?
- **Vurdér** sårbarheden heraf op imod risici og trusler gennem scenarieanalyser, som kan tage udgangspunkt i *Nationalt Risikobillede 2025,* men som altid bør tilpasses lokale forhold. Husk at scenariearbejde ikke handler om at være forberedt på X antal scenarier, men konstant at udfordre kommunens beredskabsplanlægning og krisestyringsevne med opdaterede scenarier.
- **Prioritér** de kommunale ydelser ud fra strategiske målsætninger, sådan at dele af eller hele organisationens drift kan videreføres i planlagt nedsat omfang, selvom kritiske IT-systemer er nede. Nogle kommuner har tilladelse til at benytte SINE-terminaler (beredskabsnettet), men brugen heraf eller alternativer såsom satellittelefoni eller VHF-radioer bør indgå i en større plan for at være nyttig. Den borgervendte kommunikation bør sikres gennem forhåndsaftaler med lokale medier og med foreninger og borgergrupper, som via fysisk face-to-face kommunikation kan nå udsatte borgere og bemande fysiske informationsstande.

## 2. Planlæg for strømnedbrud

I slutningen af april 2025 blev Sydeuropa ramt af et meget omfattende strømnedbrud, som mørklagde den iberiske halvø i mange timer. Hændelsen står som et skræmmende eksempel på, hvor sårbart et moderne samfund er over for afbrydelser af elforsyningen. Personer blev fanget i elevatorer, vandforsyningen svigtede, mobilnettet og internettet blev overbelastet og holdt med at fungere, mange butikker lukkede, fordi betalingssystemer gik ned, og nedkøling af fødevarer fejlede – alt sammen i løbet af få timer. Årsagen til strømnedbruddet i Spanien, Portugal og Sydfrankrig er endnu ukendt, men hændelsen viste med al tydelighed de potentielle kaskadeeffekter, der kan opstå. Stabil elforsyning er samfundets rygrad – og dermed potentielt også akilleshælen.

I *Nationalt Risikobillede 2025* beskrives de mange mulige konsekvenser af strømafbrydelser, såsom midlertidigt svigt i mobildækning, internetadgang, vand- og varmeforsyning og betalingssystemer og udfordringer med nedkøling af fødevarer i supermarkeder. Rapporten peger i det kommunale perspektiv specifikt på sundhedsvæsenet, plejehjem og botilbud som områder med funktioner, som er kritisk afhængige af strøm. Nødgeneratorer kan "sikre fortsat drift af visse kritiske funktioner i en periode", men der advares samtidig mod eksempelvis lang reetableringstid på grund af genstart af servere ved omlægning til nødstrøm.

Hændelsen på den iberiske halvø bør ses som et vink med en vognstang til kommunerne om at accelerere arbejdet med beredskabsplanlægning på området. Selv om elforsyningen i Danmark til daglig er ekstrem sikker, kan danske kommuner også blive ramt af planlagte afbrydelser i form af *brownouts* eller mere eller mindre omfattende *blackouts* (uvarslede strømnedbrud). Blot en måned før hændelsen i Sydeuropa var 33.000 husstande i Kolding fx uden strøm en aften, efter at en jordfejl havde slået en transformatorstation ud. Selv om elforsyningen blev reetableret hurtigt (ca. 40 min.), nåede borgerne i det berørte område at opleve afledte problemer med både vand- og varmeforsyning, ligesom mobiltelefoni og internetforbindelse blev påvirket.

Kilder peger i interviews til denne rapport på en omfattende usikkerhed omkring, hvor længe forskellige samfundsvigtige funktioner vil fortsætte med at fungere under omfattende strømnedbrud. Ved strømafbrydelsen i Kolding blev mobilnettet eksempelvis overbelastet allerede efter ti minutter. I et samfund, hvor konstant evne til at kommunikere er så fundamental som i det danske, er tæt dialog med bl.a. teleleverandører afgørende for at sikre borgernes mulighed for at koordinere med hinanden under kriser afgørende for dels at afbøde presset på myndighederne, dels at modvirke utryghed og usikkerhed.

Konkrete tiltag:

- **Planlæg og prioritér** hvis muligt på forhånd elforsyning i situationer med forsyningssvigt til kommunens særligt kritiske lokaliteter såsom krisestyringsfaciliteter samt botilbud for sårbare borgere, plejecentre, midlertidige pladser (hvor de dårligste borgere ofte ligger) med videre, hvor beboerne ikke selv kan efterleve myndighedernes råd om kriseforberedelse til 72 timer. Selv om disse anbefalinger er vejledende, giver de rigtig god mening at planlægge ud fra.
- **Investér** i nødstrømsanlæg til identificerede knudepunkter og udpegede lokaliteter for at sikre kontinuitet i kritiske funktioner, men husk at nødstrøm er nødstrøm, og at man ikke kan forvente at køre fuld drift! Planlæg for prioritering af strøm, sådan at der på forhånd er udarbejdet planer og installeret tekniske løsninger, der gør det muligt at frakoble mindre væsentlige dele af bygningers elnet. Belysning kan i en krisesituation fx være vigtigere end strøm til lifte, som det er muligt kortvarigt at undvære.
- **Vær opmærksom** på eventuelle forhøjede risici som følge af beredskabstiltag på energiforsyningsområdet, eksempelvis lokal oplagring af brændstof eller etablering af powerbanks, UPS'er og lignende. I april 2025 opstod der fx brand i en container med lithiumbatterier i Brøndby.[7]

7. https://ekstrabladet.dk/nyheder/samfund/brand-i-broendby-soegvaek/10601477


## 3. Styrk forsyningssikkerheden

*Nationalt Risikobillede 2025* beskriver, hvordan fx geopolitisk ustabilitet, ekstremt vejr og menneskelige fejl kan resultere i kaskadeeffekter og forstyrrelser i forsyningskæder på tværs af lande og sektorer. Også her er overblik og viden afgørende i det forebyggende arbejde med beredskabsplanlægning. En undersøgelse foretaget i august 2024 af Styrelsen for Forsyningssikkerhed viste, at 32 procent af virksomheder og myndigheder kun i mindre grad eller slet ikke havde overblik over deres forsyningskæder – og at procentdelen var markant højere for myndigheder end for den private sektor.[8] Det er uhensigtsmæssigt. "God forberedelse mindsker kaos i krisen", udtalte en kilde til denne rapport.

Et godt overblik over forsyningskæderne muliggør beredskabstiltag såsom *diversificering* (fordeling på flere leverandører), *nearshoring* (afkortning af forsyningskæder) og *redundans* (opbygning af lagerkapacitet). Kommunerne bør fortsat efterspørge statslig planlægningsvejledning for, om et beredskabslager fx bedst placeres lokalt eller centralt, og om det blot skal omfatte fx plejehjem og botilbud eller tænkes bredere. Risikoen for forstyrrelser af forsyningskæder kan nedbringes ved at indgå beredskabsaftaler med leverandører. Opgaven her er at afklare, hvordan sådanne aftaler og foranstaltninger rummes inden for gældende udbudsregler, force majeure-bestemmelser i leverandørforhold og lignende. Forsyningssikkerheden kan dog også, hvis der er tale om tre døgns beredskab, sikres ved at operere med et større lager af fx madvarer, som løbende anvendes. Muligheden for lokale aftaler med private leverandører om beredskabslagre kan afsøges.

Udfordringen med sikkerhed i forsyningskæder er, at beredskabslogikken ofte går på tværs af effektiviserings- og besparelseslogikker. Det kan være nyttigt at se på området som en investering i at nedbringe potentielle omkostninger ved fremtidige forsyningssvigt. Hvad tidsperspektivet angår, giver det god mening at tage afsæt i anbefalingerne til borgerne generelt fra juni 2024 om at være forberedt på kriser af en varighed på op til 72 timer.[9] Tankegangen er, at kortvarige kriser vil være overstået på mindre end tre døgn, og ved meget langvarige kriser giver tre døgns forberedelse samfundets samlede beredskab tid til at komme "op i gear".

Konkrete tiltag:

- **Kortlæg** relevante forsyningskæder med særlig opmærksomhed på afhængigheder og analysér de mulige konsekvenser af forstyrrelser i kommunens forsyningskæder (fx fødevarer, medicin, værnemidler), herunder afledte kaskadeeffekter ved afbrydelser.
- **Prioritér** kommunens leverancer og forbrug, sådan at det bliver muligt at fastlægge et passende beredskabsmæssigt investeringsniveau i forsyningskædesikkerhed. Alt kan ikke videreføres under en krise – men noget skal fortsætte med at fungere. Hvilke varer og ydelser kan om nødvendigt erstattes (fx er vådservietter en mulig substitut for brugsvand, mens flaskevand kan erstatte vandforsyning i nogle døgn)?
- **Involvér** relevante forsyningsselskaber, leverandører og andre samarbejdspartnere gennem dialog, øvelser og fælles planlægning samt åben og ærlig erfaringsopsamling.

8. Styrelsen for Forsyningssikkerhed og Epinion: Forsyningssikkerhed for samfundets vigtigste funktioner. August 2024.
9. https://samsik.dk/wp-content/uploads/2025/04/forberedt-paa-kriser.pdf

## 4. Forøg krisestyringskapaciteten

Kommunale krisestabe bør sammensættes meget bredt på tværs af forvaltninger og med en robusthed, således at de kan fungere i døgndrift over længere tid, evt. uger. Ofte er krisestabe dimensioneret efter at kunne håndtere én krise, fx en storbrand eller oversvømmelse, som varer kort tid, hvorefter man vender tilbage til en normaltilstand. Hybridtrusler, klimaforandringsdrevne naturskabte risici og komplekse teknologiske hændelser kan imidlertid presse kommunens beredskab til det yderste ved at påvirke mere end én sektor, ramme flere steder på én gang, kræve en indsats fra flere fagområder og foregå over længere tid. Den formelle kriseorganisation i de lokale beredskabsstabe, under politiets overordnede koordinering, spænder ofte over flere eller adskillige kommuner, og de kan derfor ikke forventes at varetage indsættelse og ledelse lokalt på kommunalt niveau, hvilket peger på, at kommunens stab selv bør opbygge en vis kapacitet, både i kompetencer, men også udholdenhed.

Erfaringerne fra COVID-19 er, at langvarige kriser er udmattende for de ramte organisationer, hvorfor den aktuelle situation fordrer en dimensionering af kommunens normalberedskab, som muliggør mere smidig skalering. Ved større kriser skal der endvidere tages højde for de dilemmaer, som nøglemedarbejdere kan stå i, når det professionelle og personlige ansvar skal afvejes. Er der udpeget stedfortrædere, som kan tage over, hvis nøglemedarbejdere ikke er i stand til at udføre deres opgaver i krisestyringen?

Krisestabe sammensættes bedst generisk med tilknytning af fagspecifikke ressourcepersoner under konkrete kriser. Robusthed i krisestyring kræver standardprocedurer for aktivering, skabelse af overblik og beslutningsprocesser og udholdenhed – og ikke mindst masser af øvelse, som dækker hele spektret fra simple dilemmaøvelser til komplekse fuldskalaøvelser.[10] Planer skal "motioneres" jævnligt for at være nyttige. "Hvis barren for aktivering af kommunens krisestyringsorganisation er sat for højt, bliver man aldrig dygtig", som en beredskabschef udtrykker det i et interview til denne rapport. Det handler om hellere at aktivere krisestyringen en gang for meget end for lidt samt at se de potentielle konsekvenser for kommunen i hver eneste hændelse.

Kommunens krisestyring skal kunne foregå på sikre, online platforme eller i dertil indrettede fysiske faciliteter, hvor der på forhånd er taget højde for sikkerhed, kommunikation, forplejning mv. Der bør endvidere udpeges sekundære lokaliteter, sådan at krisestaben kan samles og fungere, selv om den primære lokalitet er utilgængelig. Stillet over for hybridtrusler bør den kommunale krisestyringskapacitet endvidere udvides med akut analysekapacitet, som kan sikre, at situationsopfattelsen modsvarer en virkelighed, hvor risici og trusler konstant kombineres på nye måder.

Konkrete tiltag:

- **Dimensionér** kommunens krisestyringskapacitet, så alle dele af forvaltningen involveres og opfatter sig som en del af det samlede beredskab. Skab en god beredskabskultur ved at involvere så mange som muligt i debriefinger, evalueringer og erfaringsopsamlinger efter øvelser og hændelser.
- **Opbyg** de nødvendige fysiske rammer for kommunal krisestyring i form af mindst én lokalitet med nødstrømsanlæg, SINE-kommunikationsudstyr, satellittelefoni, borgervendt kommunikation mv. og gennemfør øvelser så realistisk som muligt i de korrekte omgivelser ("train as you fight").
- **Træn** organisationens evne til at styre kriser gennem jævnlige øvelser, både på papir og i praksis, og uddan nøglepersonel i stabsledelse, før det er for sent. Aktivér hellere krisestyringsorganisationen en gang for meget end en gang for lidt.

10. Den norske beredskabsmyndigheds kommuneundersøgelse fra 2025 viste eksempelvis, at mens 79 procent af kommunerne havde en plan for nødvandforsyning, så havde kun 37 procent rent faktisk øvet dette i relevante scenarier. www.dsb.no/ros-og-beredskap/kommuner/kommuneundersokelsen/kommuneundersokelsen-2025/

# 5. Skab kontakt til erhvervsliv og civilsamfund

Samfundets samlede beredskab består naturligvis af myndighederne, men også af erhvervslivet, civilsamfundet og borgerne. Civilsamfundet kan fungere både som ekstra hænder og med ekspertise inden for eget felt samt udgøre en vigtig kommunikationskanal til borgerne, særligt sårbare, svage og udsatte, som et supplement til kommunens egne medier. Derfor bør kommunerne have et tæt koordineret samarbejde med relevante foreninger i kommunen for at opbygge kendskab og kontakt forud for kriser.

Civilsamfundet rummer organisationer med forskellige kompetencer, som kan aktiveres, hvis naturskabte farer eller hybride virkemidler rammer kommunen. Eksempelvis har Dansk Røde Kors 200 lokale afdelinger samt et egentligt nationalt beredskab og har tidligere bidraget med blandt andet rådgivning i forbindelse med COVID-vaccination, flygtningekrise og flere. Beredskabsforbundet er også repræsenteret med organiserede frivillige mange steder, og de fleste kommuner har et lokalt hjemmeværnskompagni, som nok er en militær organisation, men som med fordel kan inddrages i netværket og planlægningen. Typiske barrierer for involvering af utraditionelle aktører i beredskabet er ofte bekymringer omkring juridiske forhold, som måske kunne være afklaret på forhånd, fx forsikring og arbejdstidsregler samt bekymringen for, om "de nu også kommer, når det gælder".

I beredskabsaftalen fra januar 2025 annoncerede ministeren for samfundssikkerhed og beredskab nedsættelsen på nationalt plan af fora for både civilsamfund og erhvervsliv.[11] Falck har taget initiativ til Virksomhedsberedskabet,[12] som hjælper med at koordinere bidrag fra private virksomheder under kriser.

Brancheforeninger som Dansk Industri, Dansk Erhverv og SMV Danmark har et styrket fokus på erhvervslivets rolle i samfundets samlede beredskab. Der er således mange muligheder for at involvere private virksomheder proaktivt i beredskabet. Disse nationale initiativer bør afspejles på kommunalt niveau, så der skabes kontakt forud for kriser. Forudsætningen for god involvering er opbygning af et tillidsfuldt samarbejde gennem blandt andet øvelser.

Konkrete tiltag:

- **Gå i dialog** og aftal i regi af kommunesamarbejdet i de lokale beredskaber, hvordan man vil samarbejde og inddrage civilsamfundsorganisationer og private virksomheder i beredskabsplanlægningen. Kan det lokale erhvervsliv træde til i krisesituationer med fx midlertidige kommunikationsløsninger og opstilling af nød-IT-infrastruktur? Og er der frivillige kræfter, som vil kunne bidrage?
- **Involvér** kommunens samarbejdspartnere bredt i planlægnings- og øvelsesaktivitet, sådan at der opbygges relationer og skabes gensidig forståelse for kompetencer og kvalifikationer.
- **Afklar** retningslinjer for samarbejdet på forhånd, sådan at der ikke opstår unødig usikkerhed om eksempelvis hjemmel, ansvar og økonomisk godtgørelse godtgørelse under kriser. Husk at der ikke kan stilles de samme krav til frivillige samarbejdspartnere som til leverandører og ansatte.

11. https://mssb.dk/nyheder/2025/april/nyt-erhvervsforum-for-samfundssikkerhed-og-beredskab-ser-dagens-lys/ https://mssb.dk/nyheder/2025/marts/minister-for-samfundssikkerhed-og-beredskab-civilsamfundsorganisationer-skal-faa-beredskab-ind-i-hjemmene-og-ud-i-lokalsamfundet/
12. www.falck.dk/om-falck/nyheder-og-presse/virksomhedsberedskab/virksomhedsberedskab/

# Hvis hybridkrigen rammer kommunen

*Nationalt Risikobillede 2025* medtager for første gang truslerne fra hybridkrig i analysen af de risici, som det danske samfund står over for, og anvender en god og beskrivende definition, nemlig at hybride virkemidler omfatter "metoder og kapaciteter, som fremmede stater anvender for at opnå strategiske fordele eller mål, uden at det direkte kan kategoriseres som konventionel militær magt". I praksis betyder det, at et IT-nedbrud kan skyldes et cyberangreb med en statslig aktør i ryggen, at en brand i en transformatorstation kan skyldes sabotage rettet mod kritisk infrastruktur, eller at spredning af rygter om valgsvindel eller pludselige folkestrømme ind over kommunegrænsen kan være igangsat af fremmede magter som et led i at destabilisere Danmark.

**Påvirkningsoperationer**
Spredning af *desinformation* (bevidst spredning af fejlagtige oplysninger) kræver opmærksomhed, fordi det ofte foregår online på sociale medier og har potentiale til at undergrave tilliden til myndighederne og skabe utryghed i befolkningen. Ved en effektiv kampagne vil påvirkning være selvforstærkende via uoplyste og bange borgere, som uforvarende spreder *misinformation* (ubevidst spredning af fejlagtige oplysninger).[13]

De bagvedliggende årsager til kriser er måske mindre relevante i et kommunalt perspektiv, hvor konsekvenserne er i fokus, men en vigtig pointe er, at hybridtrusler forøger den samlede usikkerhed. En kilde beskriver eksempelvis, hvordan TDC-nedbruddet i november 2024 gav anledning til overvejelser om et angreb, selv om årsagen blev angivet som værende en fejl i en softwareopdatering: "I princippet og i praksis har årsagen ingen betydning, men man finder alligevel en større tryghed i visheden om, at fejl skyldes os selv og ikke angreb." Desuden kan hybride virkemidler i yderste konsekvens få lige så store konsekvenser som traditionel land- og luftkrig for et moderne gennemdigitaliseret, strømafhængigt og højeffektivt samfund som det danske – ikke mindst ved at undergrave tilliden til digitale løsninger, hvilket på sigt kan få uoverskuelige konsekvenser for sammenhængskraften i det danske velfærdssamfund.

Sandsynligheden for, at hybride virkemidler vil ramme en dansk kommune, er vanskelig at fastslå. Energistyrelsen hævede i maj 2025 beredskabsniveauet for olie- og fjernvamesektoren til GUL (middel) ligesom for den øvrige energisektor, og FE's overordnede vurdering i *Udsyn 2024* er, at det er *sandsynligt,* at Rusland løbende planlægger og forbereder sabotageaktioner mod infrastruktur i Danmark og Europa. Når Forsvarets Efterretningstjeneste bruger sandsynligheden *sandsynligt,* som er næsthøjeste trin, dækker det over en vurderet sandsynlighedsgrad på 60-90%. Det betyder, at der er både en kapacitet og en hensigt – altså at det rent faktisk foregår.[14]

13. Jeanette Serritzlev fra Forsvarsakademiet giver fem gode råd til kildekritik i denne artikel: https://issuu.com/hjemmevaernskommandoen/docs/hjemmev_rnet_2_2022_1_/s/16823323

14. www.fe-ddis.dk/globalassets/fe/dokumenter/2024/-fe-udsyn2024-.pdf

**Hybridtruslers karakteristika**

- Kombination af både militære og (primært) ikke-militære virkemidler
- Vanskeligt at fastslå hvem der står bag, og hvad det konkrete formål er
- Konsekvensen er forvirring, usikkerhed og erosion af tillid i samfundet

Under præsentationen af *Nationalt Risikobillede 2025* blev der lagt vægt på at identificere egne sårbarheder, men også dette må ses i sammenhæng. Kommuner, hvor der er andre myndigheder eller større kritisk infrastruktur, kan blive påvirket af angreb mod disse, selv om kommunen i sig selv ikke er målet. Det kan være nationale færdselsårer, samfundsvigtige installationer, det nationale elnet eller kaserner, fly og flådestationer. Truslen er blandt andet beskrevet som brandstiftelse mod virksomheder, sabotage af broer og transmissionslinjer, og det vil have en umiddelbart afsmittende effekt i kommunen, hvor det sker.

Hybride aktiviteter skal altid ses i en større sammenhæng. Ligesom med terror er det ofte et kendetegn for hybride virkemidler, at formålet med dem er at skabe en større påvirkning af samfundet, end hvad selve angrebet indeholder. Fx kan sabotage af vandforsyningen anvendes sammen med falske påstande om, at myndighederne skjuler en forgiftning af vandet, hvilket nævnes som eksempel i *Nationalt Risikobillede 2025*. Dermed er det undermineringen af tilliden til myndighederne, der er formålet, mens selve sabotagen af vandforsyningen er midlet.

**Styrk opmærksomheden**

Selv i et gennemdigitaliseret samfund kræver sabotageaktioner nogle gange fysisk adgang til objektet, fx et vandværk, en transformatorstation eller et serverrum. I de tilfælde kan der være tale om forudgående spionage med henblik på at finde ud af, hvordan man kan få adgang, og hvad sikkerhedsniveauet er. Ansatte bør derfor være ekstra opmærksomme på tegn på fx indbrud, uden at noget er stjålet, eller uforklarlige hændelser eller mystiske besøg. Sikkerhedsbevidstheden hos medarbejdere kan relativt nemt øges ved at sætte fokus på området gennem korte orienteringer. Det væsentlige er, at hvis noget er anderledes, end det plejer at være, så meldes det til kommunens ledelse.

# Centrale begreber i *Nationalt Risikobillede 2025*

*Nationalt Risikobillede 2025* anvender begreberne risiko, trusler, hændelser og sårbarheder:

- **Risiko** forstås som produktet af sandsynligheden og konsekvensen af et faremoment. Det er eksempelvis forekomsten af en snestorm, som lukker en motorvej i en længere periode, sådan at trafikken forstyrres, eller et nedbrud på et vandværk, hvilket afbryder forsyningen til forbrugerne. Risici kan mitigeres ved at nedbringe enten sandsynligheden for forekomsten eller afbøde de potentielle konsekvenser af identificerede faremomenter gennem mitigerende tiltag.
- **Trusler** er bevidste hensigter eller handlinger med det formål at påføre andre skade, eksempelvis sabotage mod kritisk infrastruktur, hvilket kan medføre konsekvenser på linje med naturskabte og teknologiske farer, nemlig afbrydelser i samfundsvigtige funktioner. Da trusler er intentionelle (drevet af menneskelige motiver og vilje) og responsive (ændrer sig efter forebyggende tiltag), kan sandsynligheden ikke beregnes kvantitativt ligesom for risici, men vurderes kvalitativt, fx som lav, middel eller høj ud fra nærmere angivne forudsætninger.
- **Hændelser** har i 2025-udgaven af Nationalt Risikobillede afløst "ulykker" som betegnelse for konkret manifestation af konsekvenser af risici, hvilket afspejler den skærpede sabotagetrussel. Scenarier konstrueres ud fra hændelsestypers konsekvensprofiler, altså muligheden for tab af liv og værdier, varighed, udbredelse med videre.
- **Sårbarheder** dækker over et socialt eller teknologisk systems modtagelighed for skadepåvirkning, eksempelvis en forældet firewall i et IT-netværk eller en bestemt gruppe borgere, som er afhængige af omsorgsydelser fra kommunen.

Forståelsen af *faremomenter* (eksempelvis storm, sne, oversvømmelse, uventet migration, terrorangreb og cybertrusler) beror på de relevante myndigheders risiko- og trusselsvurderinger og styrkes ved inddragelse af perspektiver fra relevante interessenter og viden fra eksperter med indsigt i kommunens særlige forhold. Det kan eksempelvis være sabotagetruslen mod lokal kritisk infrastruktur, trusselsbilledet ved militære installationer, specifikke cybertrusler og lokale naturskabte/klimaforandringsdrevne farer.

Kommunens *sårbarhed* kan kortlægges gennem blandt andet analyser af afhængigheder, flaskehalse, afledte konsekvenser. Der er tale om en metodisk gennemgang af alle erkendte sårbarheder, eksempelvis afhængigheden af opladningsmulighed for elbiler til det personale, som skal levere sundheds- og omsorgsydelser til plejekrævende borgere i eget hjem. En nyttig tilgang er at undersøge *forudsætningerne* for alle kommunens funktioner, prioriteret efter hvor kritiske de er. Her spørger man simpelthen, hvilke services og ressourcer, der skal være tilgængelige, for at en given funktion kan videreføres.

Graden af *eksponering* afhænger af det konkrete faremoment, fx geografisk placering eller farens specifikke karakter på tidspunktet for forekomsten. Eksempelvis har alle byer i en kommune en grad af sårbarhed over for skybrud, men eksponeringen kan være meget forskellig afhængig af den specifikke vejrsituation. En forudsætning for at vurdere eksponeringen af en fare er, at sårbarhederne på forhånd er identificeret og erkendt. Et detaljeret, opdateret og tilgængeligt overblik over kommunens sårbare borgere kan eksempelvis anvendes til under en krise at vurdere disses individuelle eksponering over for et strømnedbrud eller en afbrydelse af vandforsyningen.

*Kapaciteter* består af dels de hårde (fx fysisk udstyr, politikker, procedurer, organisation) og de bløde (beredskabskultur, lederskab og flere) og forstås bedst i en beredskabssammenhæng som "mangel herpå", altså den negative effekt af fraværet af kapacitet. Risiko reduceres dels gennem konkret tilstedeværelse af kapaciteter, hvilket tilstræbes gennem beredskabsplanlægning, dels ved tilvejebringelse af detaljeret, opdateret og tilgængelig viden om disse kapaciteter, således at de kan anvendes mest effektivt i en krisesituation. Kapacitetsoverblik understøttes af effektive og sikre teknologier såsom databaser og GIS, hvor et antal sektorer og eksempelvis leverandører hver har ansvar for at holde informationer opdateret.

Beredskabsstyrelsen stiller på brs.dk et antal konkrete redskaber og vejledninger til rådighed inden for risiko- og sårbarhedsanalyse og beredskabs- og kontinuitetsplanlægning, mens Styrelsen for Samfundssikkerhed publicerer risiko- og trusselsvurderinger på samsik.dk. Forsvarets Efterretningstjenestes situations- og trusselsvurderinger findes på fe-ddis.dk, mens Politiets Efterretningstjenestes vurderinger af trusler mod Danmark offentliggøres på pet.dk.

KL
Weidekampsgade 10
2300 København S

+45 3370 3370
kl@kl.dk
www.kl.dk

Produktionsnr. 831068
ISBN: 978-87-94514-73-6-pdf