Kriser kommer aldrig belejligt

DI's beredskabspolitiske udspil

Dansk Industri

Forsidefoto: Getty Images

Indhold

Kriser kommer aldrig belejligt – DI's beredskabspolitiske udspil

I de seneste 30 år har vi levet i fredstid og med relativt få, alvorlige klimahændelser. Men verden er ikke længere som i de foregående årtier. Den er mere foranderlig og usikker.

Forskellige begivenheder de seneste år fra Ruslands ulovlige angrebskrig mod Ukraine, forsyningskriser og COVID-19 har tegnet en helt ny geopolitisk virkelighed. Nye trusler er kommet til. Hybride strategier er nu en del af både Ruslands og Kinas militære doktriner, og Danmark står sammen med resten af Europa foran et nyt trusselsbillede med cyberangreb og informations- og påvirkningsoperationer. Samtidig betyder klimaforandringerne mere og mere ekstremt vejr med store konsekvenser til følge, når ulykkerne rammer.

Kriser i dag er mere grænseoverskridende og vedrører i større og større grad flere sektorer. COVID-19 var en sundhedskrise, men fik lynhurtigt konsekvenser for globale forsyningskæder. Ukraine-krigen er en militær og sikkerhedspolitisk krise, men har også haft enorm indflydelse på både forsyning af fødevarer og energi globalt og med meget høj inflation til følge.

Strategisk Beredskabsforum bygger bro mellem erhvervslivet og det politiske system

DI har taget initiativ til Strategisk Beredskabsforum, der består af topledere fra udvalgte virksomheder, der alle har ekspertise og viden inden for forskellige sektorer.

Strategisk Beredskabsforum udvikler og kvalificerer politiske anbefalinger sammen med DI med det formål at styrke den samlede nationale beredskabsindsats, så Danmark i langt højere grad er forberedt på at håndtere de trusler, som vi står over for i dag.

Medlemmerne i Strategisk Beredskabsforum er:

- Marianne Dahl, Managing Director and Partner, BCG
- Søren Krogh Knudsen, CEO, Columbus
- Flemming Jensen, administrerende direktør, DSB
- Thomas Egebo, CEO, Energinet
- Jakob Riis, President and Group CEO, Falck
- Troels Bjerg, CEO Asia Pacific/Americas/Germany & Global Business Performance, ISS
- Christian Poulsen, CEO, Københavns Lufthavne
- Caroline Pontoppidan, Chief Corporate Affairs Officer, Mærsk
- Claus Fibiger, CEO, Securitas
- Michael Holm, arbejdende formand for bestyrelsen og tidligere CEO, Systematic
- John Henriksen, CEO, TDC Erhverv.

De usikre tider betyder, at udfordringer og behov hele tiden ændres. Det skal vi kunne navigere efter. Herhjemme har vi stadig meget at lære, både hos myndigheder, i civilbefolkningen og i virksomhederne – ikke mindst af vores nordiske naboer, som er langt foran.

Virkeligheden i dag er også, at den offentlige sektor og private virksomheder er vævet ind i hinanden i langt højere grad end for blot få årtier siden. De er hinandens forudsætninger for, at samfundet fungerer.

Håndteringen af COVID-19 viste, at nok kunne vi håndtere en stor uforudset krise, men det blev også tydeligt, at beredskabet ikke var tilstrækkeligt, og at virksomhederne blev involveret for tilfældigt, for uko-ordineret og i nogle tilfælde alt for sent. Oplevelsen fra erhvervslivets side var, at der var for stor berøringsangst over for at bruge private leverandørers løsninger, hvilket virkede kontraproduktivt overfor pandemibekæmpelsen, når det var tydeligt, at det offentlige ikke havde viden eller kapacitet til selv at levere løsningerne. Derfor skal det private og offentlige arbejde bedre sammen i en situation, hvor mere og mere komplekse kriser banker på døren. Danmark skal have et stærkere beredskab, der går på tværs af sektorer, aktører og offentligt og privat.

DI's ambition er at sikre, at Danmark har et robust og effektivt beredskab, der kan håndtere både nationale og internationale kriser, herunder naturkatastrofer, pandemier, cyberangreb og andre trusler. Det skal skabe de bedst mulige betingelser for borgernes hverdag og for virksomhedernes betingelser for at drive forretning.

I dette første beredskabspolitiske udspil præsenterer DI 11 konkrete anbefalinger til at styrke det nationale beredskab, særligt ved at inddrage det private erhvervslivs enorme ekspertise og kapacitet inden for alt fra forsyning af energi og vand, logistik og transport, cyber- og IT-sikkerhed, produktion af medicin, fødevarer, værnemidler osv. Listen er lang.

Det skal ske ved at:

- Inddrage private virksomheders enorme ekspertise i beredskabet
- Øge det nationale forsvar mod hybride trusler
- Styrke organiseringen af beredskabsindsatsen

Det danske beredskab skal op i gear nu - for hvis krisen først indtræffer, er det for sent. ■

Forsyningssikkerhed og hybride trusler er usikkerhedsfaktorer i virksomhederne

26 pct. af virksomhederne svarer, at **forstyrrelser i forsyningssikkerhed** er den største usikkerhedsfaktor de kommende år.

12 pct. af virksomhederne svarer, at **hybride trusler** er den største usikkerhedsfaktor de kommende år.

DI's Virksomhedspanel, efteråret 2024.

DI's anbefalinger til et stærkere, nationalt beredskab

1. Erhvervslivet skal være centralt i beredskabet

- **1.1 Model for erhvervslivets bidrag i beredskabet** Ministeriet for Samfundssikkerhed og Beredskab udarbejder i samarbejde med erhvervslivet konkrete løsninger på, hvordan private virksomheder kan indtænkes i beredskabet, på både nationalt og lokalt niveau.

- **1.2 Standby-kontrakter med private virksomhede** Standby-kontrakter skal indgås i alle dimensioner af det danske beredskab, og det skal ske så hurtigt som muligt, så vi er bedst muligt forberedt på kommende kriser. Inden 2026 skal offentlige myndigheder have sendt standby-kontrakter i udbud.

- **1.3 Etablering af Erhvervslivets Beredskabsstab** Regeringen skal etablere et samarbejds- og beslutningsforum ved siden af NOST'en – Erhvervslivet Beredskabsstab – hvor man forbereder og aftaler, hvordan offentlige og private aktører samles og agerer i forskellige krisesituationer.

- **1.4 Kriseøvelser med private virksomheder** Krisestyringsøvelserne skal fremover igen gennemføres hvert andet år og skal fokusere på krisesituationer, der går på tværs af sektorer, og hvor samarbejde mellem offentlige og private aktører er helt afgørende.

- **1.5 Nemmere og hurtigere proces for sikkerhedsgodkendelser** Sagsbehandlingstider skal nedbringes, medarbejdere bør kun godkendes én gang, hvis den første godkendelse er på højeste niveau, og sikkerhedsgodkendelser skal gælde på tværs af myndigheder.

- **1.6 Myndighederne skal systematisk dele mere information om trusselsbilledet og evt. hændelser med virksomhederne** Myndighederne skal systematisk dele mere information offentligt for at skabe klarhed og undgå spekulationer. Desuden skal strategisk udvalgte virksomheder og efterretningstjenesterne dele fortrolig, sektorspecifik information om trusselsbilledet og hændelser for at udnytte viden og efterretninger på tværs af det offentlige og private.

2. Forsvaret mod hybride trusler skal øges

- **2.1 Stærkere og mere aktivt psykologisk forsvar i samfundet** Efterretningstjenesterne kan – under hensyn til fortrolighed – udgive mere offentligt tilgængelig information om aktuelle påvirkningskampagner og misinformation fra fremmede magter, der er rettet mod Danmark og danske interesser, og bør rådgive virksomheder i at håndtere denne type trusler.

- **2.2 Public service-institutionerne kan bekæmpe mis- og desinformation** Public service-virksomhederne kan via public service-kontrakterne bl.a. pålægges at udvikle indhold, der har til formål at oplyse om aktuelle mis- og desinformationskampagner, uddanne befolkningen i at navigere i nyheder og information og informerer virksomheder om konkrete og aktuelle kampagner.

3. Stærkere organisering af det danske beredskab

3.1 Hvad kan det samlede beredskab? Ministeriet for Samfundssikkerhed og Beredskab udarbejder en kapacitetsanalyse på både nationalt og lokalt niveau, der kortlægger mandskab, materiel og resiliens i alle dele af samfundet.

3.2 En samlet beredskabsplan for Danmark Ministeriet for Samfundssikkerhed og Beredskab skal udarbejde en samlet beredskabsplan, der går på tværs af sektorplanerne. Planen skal tage udgangspunkt i det aktuelle trussels- og risikobillede og sikre forberedelse af tværgående krisescenarier, der kan ramme flere sektorer i landet på én gang.

3.3 Nationalt Risikobillede bør opdateres oftere og være samlende og virksomhedsrettet Centrale emner opdateres årligt, publikationen skal indeholde anbefalinger til virksomhederne, og den skal samle andre myndigheders trussels- og risikovurderinger for at skabe bedre overblik.

Hvad vi taler om, når vi taler om beredskab

Kriser, ulykker og katastrofer kan medføre tab af liv, skader på infrastruktur, bygninger og materiel samt skader på miljøet og naturen. Alt sammen hændelser, der kan true samfundssikkerheden. De kan både være aktørdrevne i form af destruktive handlinger og angreb fra fjendtlige magter og ikke-aktørdrevne som klimahændelser og ekstremt vejr.

Beredskab omhandler samfundets evne til at forberede sig på og håndtere denne slags uforudsete hændelser. Er der nok nødgeneratorer i tilfælde af strømsvigt? Hvad gør vi, hvis betalingssystemer eller kritisk digital infrastruktur afbrydes? Hvordan sætter vi ind ved stormfloder og oversvømmelser?

Det er altså summen af de evner og kapaciteter, som et samfund råder over til at modgå disse situationer.

Det altoverskyggende mål for et lands beredskab er, at virksomheder og borgere kan føle sig trygge, uanset hvilke udfordringer og kriser der opstår. Centrale funktioner i samfundet skal fungere – eller hurtigst muligt vende tilbage til normalen.

Det kræver både planlægning, forberedelse, uddannelse, overblik over ressourcer og øvelser.

1. Erhvervslivet skal være centralt i beredskabet

Danske virksomheder har kompetencer, ekspertise og produkter, som kan bidrage til at styrke beredskabsindsatsen. Det gælder både inden for håndtering af naturhændelser (oversvømmelser, følger af ekstremt vejr mv.) og aktørdrevne trusler (cybersikkerhed, beskyttelse af data og netværk, fysisk overvågning og beskyttelse af materiel og bygninger mv.).

Der er en lang række ressourcer til rådighed rundt omkring i landets virksomheder, som det offentlige kan trække på – i stedet for selv at skulle stå klar til at løse alle tænkelige situationer på alle tænkelige tidspunkter.

Det kan være lastbiler til fragt af fødevarer, medicin eller personer, patruljebiler til hjælp med afspærring af veje eller områder ved oversvømmelser eller store ulykker, eller lagerplads og lignende, som kan stilles til rådighed.

Hvis det skal lykkes, skal det offentlige være langt mere åbent over for at indgå formelle samarbejder med private aktører, end de har været hidtil.

En helt oplagt løsning er at indgå standby-kontrakter, hvor virksomheder skriver under på at levere bestemte varer eller services, når en krise opstår. På den måde kan virksomheder bidrage med kort aftræk og sikre, at alle ressourcer kommer på dæk, når tid er en luksus, man ikke har.

En forudsætning herfor er adgang til nødvendig information og vejledning fra myndigheder. Både før en krise indtræffer, så rettidig forberedelse er mulig, og i real tid, hvis en sikkerhedshændelse opstår. Og så skal der ryddes op i processen omkring sikkerhedsgodkendelser af private virksomheder og deres medarbejdere.

Virksomhedernes bidrag under COVID-19

Under COVID-19-pandemien spillede private virksomheder en afgørende rolle i produktion af værnemidler og andre fornødenheder.

Eksempelvis var det vigtigt for den samlede krisehåndtering, at alkoholproducenter begyndte at fremstille håndsprit, og at producenter af festtelte kunne levere faciliteter til etableringen af testcentre.

Evnen til hurtigt og effektivt at kunne omstille sin produktion til at møde nye behov under en krise er en vigtig evne i den sammenhæng – og en afgørende komponent i samfundets samlede resiliens.

Kilde: Beredt på fremtiden?, Rasmus Dahlberg og Andreas Hagedorn, 2024

Forslag 1.1 Model for erhvervslivets bidrag i beredskabet

Der findes i dag ingen model for, hvordan virksomhederne kan inddrages i beredskabet. Det er til trods for, at den private sektor uomgængeligt spiller en afgørende rolle i det danske beredskab og er central for samfundssikkerheden i Danmark. Det gælder f.eks. i forbindelse med sikring af kritisk infrastruktur, distribution og produktion af fødevarer, energi, medicin og værnemidler, transport mv.

Private virksomheder vil også udgøre en helt afgørende brik i ethvert forsøg på at forhindre eller

Foto: Colourbox

afværge en krise som følge af strømnedbrud, sammenbrud i centrale IT-systemer, hackerangreb på betalingssystemer og lignende.

DI anbefaler:

- Ministeriet for Samfundssikkerhed og Beredskab udarbejder i samarbejde med erhvervslivet i forbindelse med beredskabsplanlægningen konkrete løsninger på, hvordan private virksomheder kan indtænkes i beredskabet, på både nationalt og lokalt niveau.

  Det skal bl.a. indeholde:
  - Et samlet overblik over, hvor i samfundet der er størst risici og konsekvenser ved både aktørdrevne og ikke-aktørdrevne hændelser. Det kan f.eks. være ekstremt vejr, der medfører miljøhændelser, oversvømmelser, strømnedbrud og ødelagt transportinfrastruktur eller trusler fra fjendtlige magter som cyberangreb, sabotage eller spredning af fake news.
  - En afdækning af, hvordan private virksomheders ekspertise kan komme i spil for hver type sikkerhedshændelse – enten ved at forebygge eller håndtere den, hvis en situation skulle opstå.
  - Modeller for hvordan samarbejder mellem myndigheder og virksomheder kan formaliseres på en hurtig og ubureaukratisk måde, samt afklare evt. cost-plus kompensation.

Forslag 1.2 Standby-kontrakter med private virksomheder

Læringen fra COVID-19 har vist, at tidlig involvering af virksomhederne er en helt afgørende forudsætning for, at vi kommer godt igennem kriser. Hvis vi først skal opfinde løsninger fra bunden og derefter kæmpe

Opfordring: Falcks Virksomhedsberedskab samler frivillige kræfter fra den private sektor – kan din virksomhed bidrage?

Falck har med støtte fra blandt andre Dansk Industri lanceret Virksomhedsberedskabet, der skal styrke det danske kriseberedskab.

Virksomhedsberedskabet organiserer de frivillige kræfter i dansk erhvervsliv, der vil og kan træde til i de første timer og døgn efter en krise opstår, for at støtte myndighederne.

Virksomhedsberedskabet vil i første omgang fokusere på at beskytte de svageste borgere i samfundet – dem, som ikke selv nødvendigvis kan ruste sig eller agere handlekraftigt i en krisesituation, men som har brug for ekstra støtte og hjælp. Det er f.eks. beboere på plejehjem, hospices og bosteder.

Dansk Industri opfordrer regeringen til at understøtte udviklingen og udbredelsen af Virksomhedsberedskabet.

Læs mere og tilmeld din virksomhed her:

Virksomhedsberedskabet | Danmarks samlede kriseberedskab

med langsommelige udbudsprocesser, går der dyrebar tid til spilde.

Med standby-kontrakter kan private virksomheder sætte det offentlige "forrest i køen", f.eks. ved levering af værnemidler og lignende under en sundhedskrise.

Der er et enormt samfundsøkonomisk potentiale ved at indrette beredskabet på denne måde, da det offentlige slipper for at skulle opbygge store lagre af nødvendigheder, som risikerer at blive for gamle, ligesom man heller ikke skal have mandskab til rådighed, som kun aktiveres i krisesituationer.

Virksomhederne kan derimod sørge for altid at have tilstrækkelig lagerkapacitet og mulighed for at omprioritere vagter, servicemedarbejdere, chauffører osv. til nationale sikkerhedsopgaver, hvis det bliver nødvendigt – og til en langt lavere omkostning, end hvis staten skulle stå for det hele alene.

Brugen af standby-kontrakter er allerede udbredt i bl.a. USA og Finland, men bruges kun i mindre grad i Danmark på teleområdet og i Forsvaret.

DI anbefaler:

- Standby-kontrakter skal indgås i alle dimensioner af det danske beredskab, og det skal ske så hurtigt som muligt, så vi er bedst muligt forberedt på kommende kriser.

- Inden 2026 skal offentlige myndigheder have sendt standby-kontrakter i udbud inden for produktion og forsyning af:
  - Energi og vand
  - Fødevarer, foder og gødning
  - Medicin, værnemidler og andre sundhedsydelser
  - Transport- og logistikservice (transportmidler og personale)
  - Vagt og sikkerhed (personale, udstyr og brug af bygninger mv.)
  - IT-og cybereksperter
  - Klima- og kystsikring

- Kontrakterne indrettes efter cost plus-metoden, hvor virksomhederne afregnes efter deres direkte omkostninger ved levering af en vare eller service til beredskabet plus en ekstrabetaling, der dækker virksomhedens risiko og eventuelle ekstraomkostninger ved at skulle omstille produktion og levering med kort varsel.

- For at sikre åben og lige konkurrence skal kontrakterne udbydes på samme måde som andre offentlige udbud.

Forslag 1.3 Etablering af Erhvervslivets Beredskabsstab

Større kriser og hændelser i Danmark vil ikke kun berøre myndighedsområder, men vil også i høj grad både påvirke og involvere erhvervslivet. Under COVID-19 blev virksomheder uformelt inddraget på både lokalt og regionalt niveau i NOST'en, hvilket gjorde en betydelig forskel for håndteringen af krisen. Men der er brug for, at involveringen i fremtiden ikke hviler på en uformel og ad hoc inddragelse. Og at det sker meget hurtigere.

Mange globale virksomheder har i deres egne forretninger opbygget beredskaber med klar rollefordeling og et beslutningsdygtigt og operationelt governance setup, som bliver aktiveret i krisesituationer. Den erfaring er uvurderlig, også i håndteringen af samfundskriser. Hvis ikke vi trækker på den viden og erfaring, bliver den nationale beredskabsindsats ringere.

Det samarbejde, der blev opbygget undervejs under COVID-19, skal vi tage ved lære af, så håndtering af fremtidige kriser bliver strømlinet.

DI anbefaler:

- Regeringen skal etablere et samarbejds- og beslutningsforum ved siden af NOST'en – Erhvervslivet Beredskabsstab – hvor man forbereder og aftaler, hvordan offentlige og private aktører samles og agerer i forskellige krisesituationer.

- Erhvervslivets Beredskabsstab med repræsentanter fra de største erhvervsorganisationer skal fungere som koordinerende enhed ift. erhvervslivets bidrag til en krise.

- Erhvervslivets Beredskabsstab kan, hvis den finder det nødvendigt, involvere enkeltvirksomheder i det koordinerende arbejde.

Inddragelse af erhvervslivet i NOST'en under COVID-19

Den tværgående koordinering af den operative indsats på nationalt plan foregår i den Internationale Operative Stab (IOS) og den Nationale Operative Stab (NOST), mens det på regionalt plan finder sted i de 12 Lokale Beredskabsstabe (LBS).

Håndteringen af COVID-19 viste det danske krisestyringssystems effektivitet og fleksibilitet, bl.a. qua den hurtige involvering af private aktører på flere niveauer samt en faktisk, men ikke formel inddragelse af det kommunale og regionale niveau i NOST'en.

Kilde: Beredt på fremtiden?, Rasmus Dahlberg og Andreas Hagedorn, 2024

Forslag 1.4 Kriseøvelser med private virksomheder

De seneste fem år er de såkaldte krisestyringsøvelser, der i henhold til National Beredskabsplan skal afholdes hvert andet år, gledet i baggrunden for håndtering af faktiske kriser (COVID-19 og invasionen af Ukraine).

Der er dog vigtig, systemisk læring ved kontinuerligt at øve scenarier, der tester samfundets samlede evne til at håndtere og styre kriser. Samtidig kan der være afgørende læring ved at lave kriseøvelser på tværs af offentlige myndigheder og det private erhvervsliv, da forskellige sektorer har forskellige ekspertiseområder, og private virksomheder naturligt vil være involveret i løsningen af en lang række sikkerhedshændelser.

DI anbefaler:

- Krisestyringsøvelserne skal fremover igen gennemføres hvert andet år og skal fokusere på krisesituationer, der går på tværs af sektorer, og hvor samarbejde mellem offentlige og private aktører er helt afgørende.

- I øvelserne bør der være fokus på inddragelse af ny teknologi og udstyr, erfaringer fra kriser de seneste år samt integration af forskning inden for sikkerhed og beredskab.

- Øvelserne bør tilrettelægges efter de mest presserende scenarier i myndighedernes trussels- og risikovurderinger.

- Øvelserne bør endvidere invitere alle relevante beredskabsaktører og krisestyringsniveauer. Virksomheder og civilsamfundsorganisationer kan således bidrage i øvelser inden for områder, hvor de har ekspertise.

Forslag 1.5 Nemmere og hurtigere proces for sikkerhedsgodkendelser

Virksomheder eller deres medarbejdere skal være sikkerhedsgodkendt for at kunne udføre opgaver, der kræver adgang til klassificerede oplysninger i Danmark, EU og NATO.

Virksomhederne oplever en række udfordringer i forbindelse med at få sikkerhedsgodkendelser. Sagsbehandlingstider på minimum fire måneder og helt op til et år. En medarbejder med den højeste sikkerhedsgodkendelse kan i forbindelse med andre opgaver blive krævet en ny sikkerhedsgodkendelse – selvom den er på et lavere niveau. Og sikkerhedsgodkendelser gælder ikke på tværs af offentlige myndigheder.

Det er ressourcespild både i virksomhederne og i offentlige myndigheder.

Nationale krisestyringsøvelser

Det nationale krisestyringssystem skal iht. National Beredskabsplan minimum hvert andet år øves ved en krisestyringsøvelse (KRISØV), hvis scenarier siden 2013 har taget udgangspunkt i Nationalt Risikobillede. Denne øvelsesserie har kørt regelmæssigt i perioden 2003-2019 under Kriseberedskabsgruppens ansvar. Det vurderes problematisk, at samfundets samlede evne til at styre kriser ikke længere regelmæssigt øves op mod relevante scenarier, da vigtig organisatorisk læring og identifikation af systemiske svagheder hermed kan gå tabt. Generelt savnes en stærkere og sundere dansk øvelseskultur, som inddrager ny teknologi, integreres tæt med forskning og involverer alle relevante beredskabsaktører og krisestyringsniveauer.

Kilde: Beredt på fremtiden?, Rasmus Dahlberg og Andreas Hagedorn, 2024

DI anbefaler:

- En medarbejder med højeste niveau af sikkerhedsgodkendelse skal ikke sikkerhedsgodkendes igen i forbindelse med andre opgaver, der kræver tilsvarende eller lavere sikkerhedsgodkendelse. Det højeste niveau af sikkerhedsgodkendelse skal dække de lavere niveauer.

- Sikkerhedsgodkendelser skal gælde på tværs af de offentlige myndigheder, og sektorprincippet for sikkerhedsgodkendelser ophæves.

- Ansøgning om sikkerhedsgodkendelser hos PET automatiseres efter samme model som FE, hvor virksomheden får ansøgningsmaterialet i Digital Post og kan underskrive via MitID.

Forslag 1.6 Myndighederne skal systematisk dele mere information om trusselsbilledet og evt. hændelser med virksomhederne

Politiets Efterretningstjenesten (PET) og Forsvarets Efterretningstjeneste (FE) arbejder hver dag for at sikre Danmark. Derigennem får myndighederne adgang til efterretninger og viden om nye trusler, som kan være uvurderlige for samfundets robusthed.

Denne viden er en værdifuld ressource, vi slet ikke får nok ud af i dag, da den ikke kommer ud til de virksomheder, der er med til at sikre, at samfundet kører rundt. Derfor bør klassificeret information i langt højere grad deles med private aktører. Derigennem kan forbedrende tiltag igangsættes i tide, og hvis uheldet skulle være ude, kan erhvervslivet bidrage til at samfundet hurtigere kommer på fode igen.

Når virksomhederne nu spiller en så central rolle i samfundet, kan de opdage sårbarheder og angreb, som myndighederne måske ikke er klar over. Ved at bygge et fortroligt samarbejde op og bruge den viden, der ligger hos begge parter, kan myndighederne bedre hjælpe virksomheder, og virksomhederne kan bedre hjælpe myndighederne.

DI anbefaler:

- Myndighederne bør dele mere information om trusselsbilledet og konkrete hændelser bredt i samfundet for at skabe klarhed og undgå spekulationer.

- For strategiske sektorer udpeges der nøglevirksomheder, der systematisk skal modtage konkret mere fortrolig information om trusselsbilledet generelt og specifikt for deres sektorer.
  - Virksomhederne har en forpligtigelse til at behandle informationen fortroligt, samt at dele relevant information de måtte have med myndighederne. ■

2. Forsvaret mod hybride trusler skal øges

Hybride trusler refererer til en kombination af forskellige metoder og teknikker, der anvendes alene eller sammen for at skabe forvirring, usikkerhed og skade i et samfund.

Truslerne kan både omfatte militære og ikke-militære midler, og de opererer ofte i gråzonen mellem krig og fred. Hybride hændelser er på den måde så subtile, at de ikke kalder på direkte militær respons, mens de samtidig er virkningsfulde nok til at svække eller gøre skade på en modstander. Denne taktik gør det svært at opdage både hændelserne, motivet og aktøren bag – og den uklarhed gør det også vanskeligt at forberede sig mod dem.

F.eks. kan sabotagehandlinger, der har til formål at forhindre en virksomhed i at løse en bestemt type opgave, "forklædes" som ulykker, uheld eller kriminalitet. Det kan være som almindeligt hærværk eller ildspåsættelse.

Ifølge FE bør særligt virksomheder, der har bidraget til støtten af den militære indsats i Ukraine, være opmærksomme på hybride trusler.

De seneste år har der været et større fokus på russisk spionage mod, og formodede forberedelser til sabotage af, kritisk infrastruktur samt påvirkningskampagner, forceret migration og andre hybride virkemidler.

Virksomheder, der leverer energi, producerer eller distribuerer fødevarer og andre kritiske nødvendigheder, spiller en nøglerolle for den danske samfundssikkerhed, og deres resiliens over for hybride angreb som sabotage, cybertrusler- og spionage er derfor væsentligt for hele samfundet.

I foråret 2023 blev mere end 20 energi- og varmeselskaber ramt af det hidtil mest omfangsrige cyberangreb mod dansk kritisk infrastruktur nogensinde. Angrebet nåede kun at have begrænset effekt, men i værste tilfælde kunne det have betydet afbrudt strøm og varme for mere end 100.000 danskere.

Hybride virkemidler kan være:

- Cyberangreb og hacking målrettet, f.eks. kritisk infrastruktur, betalingssystemer eller tele- og internet.
- Misinformation hvor en afsender utilsigtet deler ukorrekte oplysninger og nyheder.
- Desinformation og spredning af fake news, hvor en afsender overlagt deler vildledende oplysninger med henblik på at opnå en effekt, f.eks. politisk eller økonomisk.
- Sabotage og chikanehandlinger som ødelæggelse af udstyr, materiel eller faciliteter.
- Politisk påvirkning gennem støtte til udvalgte politiske grupper eller kandidater.

Virksomhederne forbereder sig på hybride trusler

62 pct. af virksomhederne har taget specifikke forholdsregler eller øget deres beredskab for at **sikre sig mod hybride trusler.**

For virksomheder med mere end 100 ansatte gælder det for ni ud af ti.

70 pct. af virksomhederne er i enten høj eller nogen grad bekymrede for, at deres forretningssituation kan blive **negativt påvirket af hybride trusler** indenfor de kommende år.

De store virksomheder er i lidt højere grad bekymrede end de mindre.

Kilde: DI's Virksomhedspanel, efterår 2024.

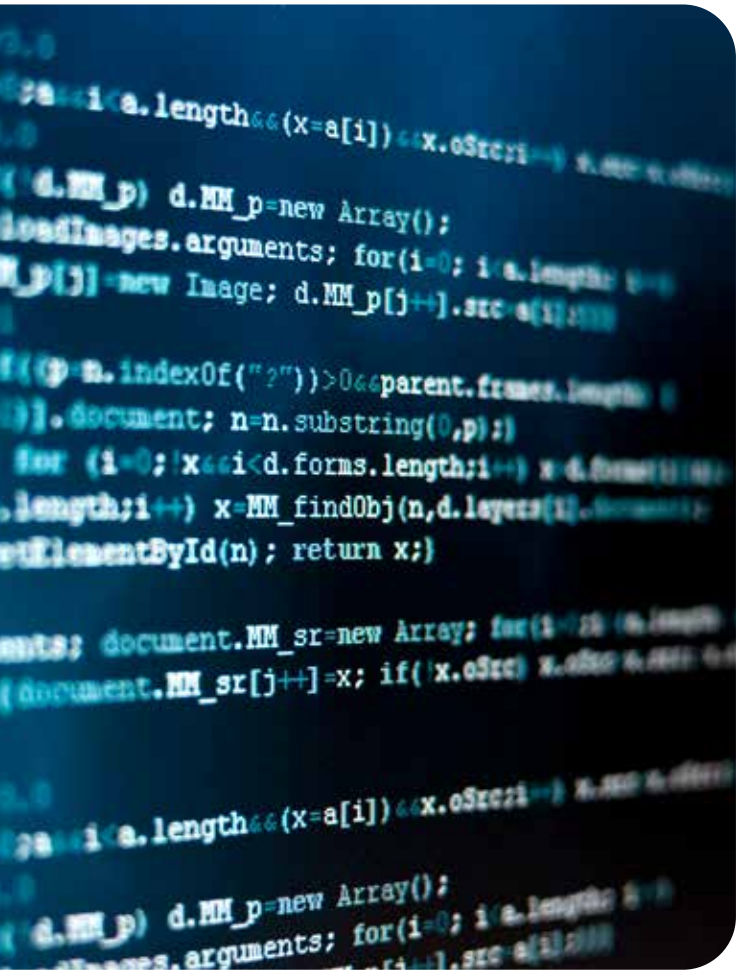

Foto: Getty Images

Forslag 2.1 Stærkere og mere aktivt psykologisk forsvar i samfundet

Misinformation, desinformation og påvirkningskampagner er hybride virkemidler, der forsøger at svække samfundets resiliens og en befolknings villighed til at forsvare sig selv eller at påvirke folks opfattelser, adfærd og beslutninger. Målet med at anvende hybride virkemidler er det samme som ved at anvende klassisk militær magt, navnlig at tvinge sin vilje igennem og opnå noget, som modparten ikke selv ville have gjort eller accepteret.

Psykologisk forsvar omhandler et samfunds samlede evne til at opdage og modstå misinformation fra fjendtlige magter, der har til hensigt at skade et land og dets interesser.

I Sverige har man nedsat Myndigheten för psykologiskt försvar, som har til opgave at identificere, analysere og udøve rådgivning for at modgå påvirkningskampagner og misinformation. Indsatsen omfatter både rådgivning af offentlige myndigheder og borgere. Der er altså tale om en mere åben indsats, der ikke alene handler om efterretningstjenesternes fortrolige oplysning af regeringen og de politiske partier.

DI anbefaler:

- PET og FE skal bidrage til et stærkt dansk psykologisk forsvar, så vi bedst muligt kan imødegå hybride trusler. Det er afgørende, at vurderingen af hvornår informationsstrømme mv. har karakter af at være påvirkningsoperationer eller desinformationskampagner baseres på objektive og transparente kriterier, så det psykologiske forsvar hverken bliver tilfældigt eller politisk bestemt.

  Et stærkt psykologisk forsvar indebærer bl.a., at efterretningstjenesterne skal:
  - Udgive mere offentlig tilgængelig oplysning om aktuelle påvirkningskampagner og misinformation fra fremmede magter, der er rettet mod Danmark og danske interesser.

- Rådgive virksomheder om aktuelle operationer og vejlede i, hvordan man som virksomhed skal forberede sig på og håndtere aktuelle trusler.
- Gennem offentlige informationskampagner oplyse borgere om aktuelle operationer og misinformationskampagner, som man bør være opmærksom på både i det fysiske og digitale rum.

Det skal selvfølgelig altid ske under hensyn til, at nogle oplysninger må forblive fortrolige af hensyn til rigets sikkerhed.

Forslag 2.2 Public service-institutionerne kan bekæmpe mis- og desinformation

Public service-medierne (DR, TV 2 Danmark og de regionale TV 2-virksomheder) har bl.a. til opgave at sikre den danske befolkning nyhedsformidling, oplysning og undervisning. I det lys kan de også spille en afgørende rolle i at bekæmpe mis- og desinformation og påvirkningskampagner. Det handler eksempelvis om at tilgå og opsøge officielle nyhedskilder og kunne evaluere troværdighed af indhold og afsendere.

DI anbefaler:

- Public service-virksomhederne kan via public service-kontrakterne pålægges at udvikle indhold, der har til formål at:
  - Oplyse borgere om aktuelle mis- og desinformationskampagner fra fremmede aktører.
  - Uddanne befolkningen i at navigere i nyheder og information i medier og på internettet, herunder kritisk stillingtagen til kilder, afsendere og mulige intentioner i indhold.
  - Uddanne befolkningen i at genkende indhold, der er genereret af AI og særligt med det formål at udbrede fake news eller andet vildledende indhold.
  - Informerer virksomheder om konkrete og aktuelle kampagner, der kan have betydning for deres forretningsmæssige sikkerhed. ■

Russiske påvirkningskampagner i EU

I sommer kunne DR afsløre, at en russisk statsfond ved navn Pravfond, der hører under det russiske udenrigsministerium, har sendt millioner af kroner ind i EU til finansiering af påvirkningskampagner. Der er bl.a. blevet delt indhold på flere sprog i en række medier, herunder onlinemediet EuroMore, som blev lanceret kort efter Ruslands invasion af Ukraine, som eksperter har betegnet som propaganda. EuroMore har bl.a. publiceret indhold om "den særlige operation i Ukraine", "russofobi i Europa" og "beskyttelse af det russiske sprog".

Debatten om bokseren Imane Khelif under sommerens OL er et andet eksempel på en russisk desinformationskampagne. "Informationen" om at bokseren både skulle have et X- og et Y-kromosom viste sig udelukkende at stamme fra det russiske, statsejede medie ITAR-TASS. ITAR-TASS bruges ifølge et forskningsstudie som et strategisk middel af den russiske stat til international propaganda som en del af Ruslands hybridkrig.

Kilder: Hemmelig operation afsløret: Russisk spionfond har betalt millionbeløb for kampagner i Danmark og EU | Mørklagt | DR

EU indfører sanktioner mod de statsejede medieforetagender RT/Russia Todays og Sputniks udsendelsesaktiviteter i EU - Consilium

Watanabe (2017), Measuring news bias: Russia's official news agency ITAR-TASS' coverage of the Ukraine crisis, European Journal of Communication, vol. 32, Issue 3

3. Stærkere organisering af det danske beredskab

Det nationale beredskab er indrettet efter sektoransvarsprincippet, hvor de enkelte sektorer har ansvaret for deres eget beredskab. Ansvaret er altså placeret der, hvor ekspertisen er størst. Det er et princip, der siden begyndelsen af 1990'erne har fungeret effektivt til at håndtere kortvarige og afgrænsede kriser.

Men stillet over for en moderne verden med cyberangreb og hybride trusler som sabotagehandlinger og påvirkningskampagner, hvor mange sektorer skal koordinere på tværs, og hvor der ikke altid er placeret et entydigt ansvar, er et siloopdelt beredskab sårbart.

Med oprettelsen af Ministeriet for Samfundssikkerhed og Beredskab er der nu en tættere koordinering af myndighedsopgaver i beredskabet end tidligere. Nu har man bl.a. samlet Beredskabsstyrelsen, Styrelsen for Forsyningssikkerhed, dele af Center for Cybersikkerhed, Den Nationale Operative Stab (NOST'en), Det Centrale Operative Kommunikationsberedskab, havmiljø- og stormflodsberedskab samt implementering af NIS2- og CER-direktiverne under ét tag. Dermed er der et tydeligere, overordnet ansvar for det danske beredskab, og vi er kommet noget af vejen.

En af de vigtigste opgaver for det nye ministerium er at skabe et samlet overblik over beredskabets tilstand. Ikke kun i de enkelte sektorer, men på tværs af hele samfundet. Den seneste Nationale Sårbarhedsudredning om samfundets sårbarheder og behov for beredskabsmæssige forbedringer er fra 2004. Vidensgrundlaget er altså 20 år gammelt.

Virksomhederne understøtter det nationale beredskab, både ved at sikre sikkerheden i deres egen forretning og ved at bidrage direkte med ekspertise og kapaciteter i den nationale indsats. Men det kræver dybere indblik i sikkerhedsbilledet og adgang til information, som er overskuelig og opdateret.

For at understrege hvor lidt horisontalt samarbejde der er i Danmark om beredskabet, så er der ikke mindre end fire myndigheder, der udarbejder risiko- og trusselsvurderinger, herunder Beredskabsstyrelsen, Politiets Efterretningstjeneste (PET), Forsvarets Efterretningstjeneste (FE) og Center for Cybersikkerhed. Desuden laver en række sektormyndigheder deres egne trusselsvurderinger. De mange forskellige vurderinger gør det vanskeligt at få et overblik for både for borgere og virksomheder, og det kan besværliggøre at træffe de rette foranstaltninger.

Det er samtidig utilstrækkeligt, at noget information kun opdateres hvert fjerde år, når man tænker på, hvor hurtigt trusselsbilledet ændrer sig – og i mere og mere alvorlig retning.

Myndighedernes trusselsvurderinger

Aktørdrevne trusler

PET – Vurdering af terror–truslen mod Danmark 2023

Fokuspunkter:

Aktørdrevne trusler som:
- Terror
- Terrorfinansiering
- Militant islamisme
- Politisk ekstremisme
- Radikalisering

Vurderingsskala:

Meget alvorlig - Specifik trussel
Alvorlig - Erkendt trussel
General - Kapacitet og hensigt
Begrænset - Potentiel trussel
Minimal - Ingen indikationer på en trussel

FE – UNDSYN 2023

Fokuspunkter:
- Udefrakommende aktørdrevende trusler
- Hybride trusler
- Cybertrusler fra statslige aktører som Rusland og Kina

Vurderingsskala:

Meget høj - Kendskab til kontinuerlige eller iværksatte angreb
Høj - Specifik planlægning eller forsøg på angreb
Middel - Kapacitet/intention, dog ingen specifik planlægning af angreb
Lav - Begrænset kapacitet eller Intention til udførsel af angreb
Ingen - Ingen tegn på trussel

Beredskabsstyrelsen – Nationalt Risikobillede 2022

Fokuspunkter:

14 forskellige hændelsestyper, som kan have samfundsmæssig risici indenfor:
- Naturskabte hændelser
- Aktørdrevne trusler
- Ulykker

Vurderingsskala:

Hændelsestypen bliver delt op i forskellige kendetegn, der bliver vurderet som **alvorlige**, og eller **ekstreme**

Øvrige myndigheder, som udarbejder trusselsvurderinger

- Sundhedsstyrelsen
- Center for Biosikring og Bioberedskab(CBB)

Cybersikkerhed

Center for Cybersikkerhed (CFCS) – Cybertruslen mod Danmark

Fokuspunkter:
- Cyberspionage
- Cyberkriminalitet
- Cyberaktivisme
- Cyberterror

Vurderingsskala:

Meget høj - Kendskab til kontinuerlige eller iværksatte angreb
Høj - Specifik planlægning eller forsøg på angreb
Middel - Kapacitet/intention, dog ingen specifik planlægning af angreb
Lav - Begrænset kapacitet eller intention til udførsel af angreb
Ingen - Ingen tegn på trussel

SektorCERT – Trusselsvurdering

Fokuspunkter:
- Cybertruslen mod dansk kritisk infrastruktur

Vurderingsskala:

Trusselsniveauet opdeles i en farveskala:

Grøn - Ingen usædvanlig aktivitet
Blå - Generel risiko, ingen kritisk påvirkning
Gul - Konkret trussel, potentiale for påvirkning
Orange - Høj risiko, målrettede angreb
Rød- Meget høj risiko, national krise

Forslag 3.1 Hvad kan det samlede beredskab?

Første skridt på vejen mod et samlet og stærkere beredskab er, at vi får et reelt overblik over kapaciteterne.

DI anbefaler:

- Ministeriet for Samfundssikkerhed og Beredskab udarbejder en kapacitetsanalyse på både nationalt og lokalt niveau, der kortlægger mandskab, materiel og resiliens i alle dele af samfundet.

- Kapacitetsanalysen skal sammenholdes med de aktuelle trussels- og risikovurderinger i en samlet vurdering af, hvilke trusler samfundet aktuelt er mest sårbart overfor, og hvor der er størst behov for at styrke beredskabet.

Forslag 3.2 En samlet beredskabsplan for Danmark

Beredskabet i Danmark er diffust, og ingen har i dag det formelle horisontale ansvar. Det er derfor vi oplever, at hver gang en hændelse går på tværs af sektorer, så er beredskabet utilstrækkeligt. I dag har Beredskabsstyrelsen til opgave at føre tilsyn med de forskellige sektorers beredskabsplaner. Men der findes ikke en samlet, national beredskabsplan, der tænker i tværgående scenarier, og som rækker ud over enkelthændelser og i adskilte sektorer.

Hertil kommer, at Beredskabsstyrelsen ikke har til opgave at kvalitetssikre eller godkende sektorplanerne, men blot sikre, at de er lavet. Styrelsen har dermed reelt meget begrænset indflydelse, selv hvis de finder beredskabsplanerne utilstrækkelige.

I elsektoren er der eksempelvis krav om, at de enkelte virksomheder skal have det nødvendige beredskab (f.eks. i form af olielagre) til at opretholde forsyningen i tilfælde af en krise. Men forestiller man sig et større, koordineret hybridangreb, som både rammer strøm- og vandforsyningen, samtidig med at der udføres sabotagehandlinger mod transportinfrastrukturen, kommer de enkelte sektorplaner til kort.

DI anbefaler:

- Ministeriet for Samfundssikkerhed og Beredskab skal udarbejde en samlet beredskabsplan, der går på tværs af sektorplanerne. Planen skal tage udgangspunkt i det aktuelle trussels- og risikobillede og sikre forberedelse af tværgående krisescenarier, der kan ramme flere sektorer i landet på én gang.

- Ministeriet for Samfundssikkerhed og Beredskab skal i fremtiden både sikre sammenhæng på tværs af alle beredskabsplaner samt kvalitetssikre samtlige myndigheders beredskabsplaner.

Forslag 3.3 Nationalt Risikobillede bør opdateres oftere og være samlende og virksomhedsrettet

De relativt sjældne opdateringer af Nationalt Risikobillede betyder, at informationen hurtigt bliver overhalet af virkeligheden. Samtidig er rapporten blottet for anbefalinger til, hvad den private sektor skal gøre.

DI anbefaler:

- Centrale temaer i Nationalt Risikobillede som cyberhændelser, hybride virkemidler og forstyrrelser i forsyningskæder skal opdateres fremover årligt. De kan opdateres uden for almindelig kadence af den trykte publikation og i stedet publiceres på ministeriets hjemmeside.
- Trussels- og risikovurderingerne skal i langt højere grad omhandle, hvordan virksomhederne kan omsætte de nationale vurderinger til egne beredskabsplaner.
- Alle myndigheders risiko- og trusselsvurderinger bør samles med vejledninger og anbefalinger på Ministeriet for Samfundssikkerhed og Beredskabs hjemmeside, så al den nyeste viden altid er samlet og tilgængelig ét sted. På den måde kan borgere og virksomheder nemmere danne sig et overblik over den aktuelle sikkerhedssituation. ■

Foto: Getty Images

Dansk Industri