Danmarks digitale totalforsvar og -beredskab

De nødvendige trin til resiliens og sikkerhed

NAVIGATING 360

IT-BRANCHEN

1 Danmark er ikke tilstrækkeligt rustet til at imødegå hybride og digitale trusler

Cybertruslen er blevet et permanent grundvilkår, vi skal forholde os til i Danmark, og det gør vi ikke i tilstrækkelig grad. Danmark er med andre ord ikke godt nok rustet til at imødegå det mest alvorlige og komplekse, hybride risiko- og trusselbillede siden anden verdenskrig.

Vores kritiske digitale infrastruktur er for sårbar over for både digitale og fysiske angreb.

Det skyldes til dels, at ansvaret for at imødegå hybride trusler – og særligt cybertruslen – falder mellem det militære og civile og mellem eksisterende ressortområder og myndighedsansvar. Det nuværende sektoransvarsprincip fungerer dårligt i et trusselsbillede, der går på tværs af sektorer og domæner.

I Danmark tænker vi fortsat for vertikalt og sektoropdelt, mens de hybride trusler er horisontale og sammenvævede. Her kan vi lære af fx Finland og senest Ukraine, der er eksempler på lande med en stærkere horisontal koordinering og mere robuste samfundsmekanismer.

2 Der mangler mandat, koordinering og fælles styring af vores digitale forsvar og beredskab

Danmark mangler i dag en stærk national organisering af det digitale forsvar og beredskab. Ministeriet for Samfundssikkerhed og Beredskab har fået det overordnede ansvar for at styrke og koordinere Danmarks cyberforsvar, men mangler det nødvendige mandat, den politiske tyngde og de operative beføjelser til reelt at drive koordineringen på tværs af myndigheder, sektorer og kritisk infrastruktur.

En løsning kunne være at etablere en overordnet "paraplystruktur" for digital sikkerhed og beredskab med tydeligere ansvar, beslutningskraft og prioritering på tværs af ressortområder. En organisering der samtidig forholder sig til, at vi ikke befinder os i en fredstid, som vi kender den, men at trusselsbilledet i stigende grad er præget af vedvarende digitale angreb og hybride påvirkningsoperationer.

Samtidig er manglede informationsdeling fortsat en stor udfordring for vores digitale modstandskraft. I dag er der begrænset mulighed for at dele viden om trusler, risici og hændelser på tværs af sektorer, bl.a. på grund af regler, manglende sikkerhedsgodkendelser og uklare ansvarsforhold. Her er der behov for en arkitektur for videndeling og en platform, der kan understøtte videndeling både før, under og efter hændelser, hvis vi for alvor skal etablere et digitalt totalforvar og -beredskab i Danmark.

3 Digital oprustning halter markant efter den klassiske militære oprustning

Danmark tænker fortsat sikkerhedspolitik meget fysisk og militært – og i langt mindre grad digitalt. Mens der investeres massivt i klassiske forsvarskapaciteter som fregatter, kampvogne og ammunition, fylder cyber- og dataområdet relativt lidt i både den offentlige debat og de konkrete investeringer.

Konsekvensen er, at data, software, digital infrastruktur og teknologisk suverænitet endnu ikke behandles som strategiske sikkerhedsressourcer på linje med traditionelle militære kapaciteter.

Samtidig er der store efterslæb i den offentlige it-infrastruktur – herunder i Forsvaret – og behov for langt større investeringer i både cyberforsvar, datakapacitet og digital robusthed.

Cybertruslen er vanskelig at forstå og forholde sig til politisk, fordi den er usynlig, teknisk og konstant til stede. Det er lettere at forstå og mobilisere opmærksomhed omkring et droneangreb eller et fysisk angreb end omkring manipulation af data, kompromitterede systemer og kontinuerlige cyberangreb. Dermed er cybertruslen blevet en stærkt undervurderet del af det hybride trusselsbillede, som vi er nødt til at tage mere alvorligt.

4 Offentlig-privat samarbejde er nøglen til et digitalt totalforsvar

Et digitalt totalforsvar kan ikke bygges af staten alene. Det kræver et langt tættere, mere strategisk og mere forpligtende samarbejde mellem myndigheder, Forsvaret, kritisk infrastruktur og den digitale sikkerhedsindustri.

Danmark har allerede vist, at tæt offentlig-privat samarbejde kan drive både digital innovation og opbygning af stærke digitale kapaciteter. Den samme tilgang bør nu bruges til at udvikle et digitalt totalforsvar, hvor staten og virksomhederne i fællesskab opbygger de sikkerheds- og beredskabskapaciteter, som samfundet er afhængigt af.

Sikkerhed har traditionelt været en klassisk statslig kerneopgave, men på det digitale område er staten samtidig afhængig af teknologivirksomhederne og den digitale sikkerhedsindustri. Statens opgave bliver derfor i højere grad at sætte strategisk retning, definere rammer og prioriteter samt skabe de rette incitamenter og samarbejdsmodeller, mens markedet i praksis kommer til at spille en central rolle i udviklingen og leveringen af de konkrete digitale sikkerhedskapaciteter.

Samtidig kræver et digitalt totalforsvar en langt tydeligere prioritering af, hvad der er mest kritisk at beskytte. Vi kan ikke beskytte alle systemer, data og infrastrukturer lige godt, og derfor er der behov for en fælles forståelse af, hvilke funktioner og kapaciteter der er vigtigst for samfundets robusthed og handleevne under kriser.

Et digitalt totalforsvar forudsætter samtidig mere genkendelige og transparente sikkerhedskrav på tværs af sektorer, bedre deling af data og trusselsinformationer, fælles øvelser og nationale beredskabsplaner. Samtidig er der behov for en mere klart defineret og sammenhængende sikkerhedsarkitektur, så samfundskritiske systemer og infrastrukturer i højere grad kan fungere og samarbejde på tværs under kriser.

Samarbejdsformerne skal desuden være langt mere agile end i dag. Trusselsbilledet ændrer sig hurtigt, og derfor er lange udviklingsforløb og tunge processer ofte utilstrækkelige. Der er behov for hurtigere feedbackloops, løbende tilpasning og tættere samspil mellem stat, forsvar og industri.

5 Tillid til data og systemer er en kritisk sikkerhedsfaktor

Truslen mod samfundet handler ikke kun om at lamme systemer, men også om at underminere tilliden til dem. Danmark er et samfund med høj digitalisering og stor tillid til institutioner, data og digitale systemer, og netop derfor er samfundet også sårbart over for manipulation og påvirkning.

Korrumpering af data, misinformation og påvirkningskampagner kan underminere borgernes tillid til både myndigheder, demokratiske institutioner og samfundets digitale infrastruktur. Tillid til data og digitale systemer bliver dermed i stigende grad et sikkerhedspolitisk spørgsmål.

Moderne hybridkrig handler i høj grad om at skabe usikkerhed, mistillid og polarisering i samfundet. Derfor handler digital robusthed ikke alene om at beskytte systemer og data gennem teknologi og cybersikkerhed, men også om at beskytte den tillid og sociale sammenhængskraft, som det danske samfund bygger på.

6 Samfundsberedskab handler også om kultur og mental robusthed

Danmark skal som samfund blive bedre til at leve med kriser og til at operere under usikkerhed og forstyrrelser uden at gå i panik. Robusthed handler ikke alene om teknologi, cybersikkerhed og beskyttelse af kritisk infrastruktur, men også om samfundets evne til at bevare overblik, handlekraft og sammenhængskraft, når kriser rammer.

Borgerne skal i højere grad forberedes både mentalt og praktisk på situationer med digitale nedbrud, strømudfald eller længerevarende forstyrrelser af samfundskritiske systemer. Samtidig bør civilsamfund, frivillighed og lokale fællesskaber tænkes langt mere aktivt ind i det samlede beredskab.

Danmark har stærke forudsætninger i kraft af høj samfundstillid, et stærkt foreningsliv og en stor frivilligkultur. Disse styrker kan blive centrale elementer i et mere robust samfundsberedskab. Det kræver samtidig mere træning, flere scenariebaserede øvelser og en bredere samfundsmæssig bevidsthed om, hvordan man håndterer kriser og forstyrrelser i praksis.