

Forsvarsministeriet
e-mail:fmn@fmn.dk og alg@fmn.dk

Sagsnummer 2025/000462.

07.03.2025

Høringsbidrag til udkastet til lovforslag om ændring af lov om forswarets formål, opgaver og organisation m.v. (bekæmpelse af ulovlig droneaktivitet over militære områder m.v.)

Teleindustrien i Danmark takker for muligheden for at afgive hørings-svar vedrørende udkastet til lovforslag om ændring af lov om forswarets formål, opgaver og organisation m.v. (bekæmpelse af ulovlig droneaktivitet over militære områder m.v.).

Vi anerkender fuldt ud behovet for at kunne neutralisere ulovlig droneaktivitet over militære anlæg og særligt beskyttede områder. Droner kan udgøre en alvorlig sikkerhedstrussel mod forswarets installationer, flyvesikkerhed og samfundsvigtige mål, og det er forståeligt, at Forsvaret ønsker effektive midler til at imødegå denne trussel.

Teleindustrien støtter således intentionen om at styrke mulighederne for at neutralisere ulovlige droner på en hurtig og sikker måde. Vi finder imidlertid, at visse telekommunikationsmæssige hensyn ikke er tilstrækkeligt adresseret i det foreliggende lovforslag, hvilket uddybes nedenfor.

Risiko for forstyrrelse af kritisk mobilkommunikation

Lovforslaget giver Forsvaret hjemmel til at anvende "elektroniske modforanstaltninger" mod droner, herunder jamming (forstyrrelse af radiosignaler). Teleindustrien vil understrege, at mange samfundskritiske tjenester i dag er afhængige af mobilkommunikation. Nødopkald, beredskabskommunikation, sundheds-IT, transport- og energisektoren samt betalings- og datasystemer benytter alle de kommercielle mobilnet. Enhver forstyrrelse af mobilnetværkene kan derfor have direkte indvirkning på borgernes sikkerhed og vitale samfundsinteresser. Vi finder det bekymrende, at lovforslaget ikke behandler risikoen for, at neutraliseringsmetoderne kan forstyrre denne kritiske mobilkommunikation.

Det foreslåede § 15 a, stk. 3 i forsvarsloven fritager Forswarets dronebekæmpelsesaktiviteter fra at overholde lov om radioudstyr og

elektromagnetiske forhold (radioudstysloven) og lov om radiofrekvenser (frekvensloven). Disse love har netop til formål at sikre, at radioudstyr og frekvensanvendelse ikke forstyrrer anden lovlig radio-kommunikation i samfundet. Når lovforslaget lægger op til at se bort fra disse beskyttelseslove, åbnes der for, at forsvarets modforanstaltninger kan involvere brug af frekvenser og udstyr på en måde, som normalt ville være ulovlig på grund af risikoen for interferens.

Påvirkning af mobilnet og økonomiske konsekvenser for erhvervslivet

Det fremgår af bemærkningerne, at Forsvaret med den foreslåede fravigelse af frekvensloven vil kunne anvende radiofrekvenser, som andre har tilladelse til at benytte, eller anvende frekvenser uden tilladelse i strid med de normale rammer for disse frekvenser. Konkret betyder det, at Forsvaret ved neutralisering af droner kan komme til at sende på frekvensbånd, der bruges af mobiloperatørerne (eller af andre trådløse tjenester), hvilket i værste fald kan forstyrre mobiltrafikken i området. Allerede en kortvarig forstyrrelse af et mobilnetværk kan medføre tab af forbindelse for mange brugere. For samfundskritiske enheder, der er afhængige af konstant forbindelse, kan dette skabe farlige situationer – eksempelvis hvis ambulancepersonale mister forbindelsen til et hospitals datasystem, eller hvis borgeres 112-opkald ikke går igennem i de pågældende sekunder.

Det anføres i lovforslaget, at det ingen økonomiske konsekvenser har for erhvervslivet. Teleindustrien er uenig i denne antagelse. Mobilnettene udgør en central del af erhvervslivets infrastruktur, og selv små forstyrrelser kan have betydelige afledte omkostninger. Hvis en drone-neutraliseringsindsats forårsager udfald på mobilnettet, kan det ramme virksomheder økonomisk – f.eks. ved at betalingstransaktioner fejler, produktion eller logistik forsinkes, eller kritiske IoT-systemer midlertidigt går offline. Disse indirekte konsekvenser bør anerkendes.

Utsigtede negative effekter på teleinfrastruktur i tætbefolkede områder

De foreslåede neutraliseringsmetoder kan have indflydelse på den samfundskritiske teleinfrastruktur. Dette er især relevant i tætbefolkede områder som København. Lovforslaget omfatter bl.a. droner ved "civiliste slotte, som er under Forsvarets bevogtning" – det vil sige f.eks. kongelige residenser midt i bymæssig bebyggelse. Her vil brugen af jamming kunne påvirke et betydeligt antal mennesker og tjenester i nærheden. Radiobølger respekterer ikke ejendomsskel, og en jammer udsendt ved f.eks. Amalienborg Slotsplads kan potentielt påvirke frekvenserne i et større område end tiltænkt – herunder naboers mobiltelefoner, Wi-Fi-forbindelser, GPS-modtagere m.v. Selv om Forsvarsministeriet i bemærkningerne anfører, at neutralisering skal tilrettelægges sådan, at der kun er lav risiko for at påvirke udenforstående, er der ingen konkrete retningslinjer i lovforslaget for, hvordan denne lave risiko sikres i praksis. Teleindustrien finder, at der bør opstilles klare procedurer for, hvordan der må jammes i nærheden af

teleinstallationer for at undgå uforvarende udfald på f.eks. mobilmaster eller internetforbindelser.

3

Inddragelse af mobiludbydere i implementeringen

I det vi anerkender, at det kan være vanskeligt at arbejde med indhentning af retskendelser i forbindelse med et pludseligt opstået behov for nedtagning af en drone, anbefaler Teleindustrien, at mobiloperatørerne inddrages tæt i processen vedr. dronebekæmpelse. Et formaliseret samarbejde mellem Forsvaret og teleudbydere bør etableres således, at teleselskaberne får adgang til oplysninger om, hvor og hvornår jamming er sket, og således at eventuelle forstyrrelser i telenettene kan identificeres som forårsaget af "lovlig jamming". Alternativt risikerer teleselskaberne at bruge unødige ressourcer og tid på at identificere kilden til forstyrrelser i nettene.

Alternative og mindre forstyrrende neutraliseringsmetoder

Teleindustrien anerkender, at elektroniske modforanstaltninger ofte kan være den mest effektive måde til at uskadeliggøre en drone på afstand. Vi skal dog opfordre til, at mere målrettede teknologier foretrækkes frem for bredbåndet jamming, hvor det er muligt. Lovforslagets bemærkninger nævner selv metoder som "spoofing" af GPS-signaler og "cyber-takeover", hvor dronen omdirigeres eller tvinges til at lande kontrolleret. Sådanne tilgange påvirker primært dronen selv frem for at forstyrre alle signaler på frekvensen, og de kan dermed reducere risikoen for forstyrrelser. Vi foreslår, at Forsvaret – når teknologien og situationen tillader det – benytter spoofing eller overtagelse af dronesignaler frem for generel jamming, alternativt fysisk nedskydning eller retningsbestemt jamming overvejes.

Afslutningsvis vil Teleindustrien i Danmark gerne fremhæve, at vi deler ønsket om at beskytte militære områder og kritiske lokaliteter mod ulovlig droneaktivitet. Vores ovenstående bemærkninger har til formål at sikre, at denne beskyttelse sker uden utilsigtet at kompromittere den teleinfrastruktur, som borgerne og erhvervslivet er dybt afhængige af i det daglige. Vi anbefaler derfor en balanceret tilgang, hvor Forsvaret får de nødvendige beføjelser til at handle mod droner, men hvor der samtidig indbygges garantier og samarbejdsprocedurer, som varetager hensynet til mobilnetværkene og kommunikationssikkerheden.

Teleindustrien står naturligvis til rådighed for yderligere dialog og samarbejde om disse emner.

Med venlig hilsen



Jakob Willer
Direktør