Cyberalliancen repræsentere Green Power Denmark, Danske Rederier, Finans Danmark, Teleindustrien og F&P

Høringssvar til Europa-Kommissionens handlingsplan for drone- og anti-dronesikkerhed

Resume

Cyberalliancen støtter handlingsplanen som et vigtigt skridt mod en mere koordineret europæisk indsats mod dronetrusler mod kritisk infrastruktur. Den operative bekæmpelse af fjendtlige droner bør være et myndighedsansvar, mens private aktører bidrager med sektorspecifik viden. Der er behov for klare og harmoniserede EU-regler samt etablering af digitale geografiske zoner i dialog med berørte infrastrukturejere.

Høringssvar

Cyberalliancen takker for muligheden for at afgive høringssvar til Europa-Kommissionens handlingsplan for drone- og anti-dronesikkerhed. Alliancen repræsenterer Green Power Denmark, Danske Rederier, Finans Danmark, Teleindustrien og F&P.

Vi er en række samfundskritiske sektorer, hvor sikker og stabil drift er afgørende både for borgere, erhvervsliv og Danmarks samlede modstandskraft. Vi hilser derfor initiativet velkommen og ser det som et vigtigt skridt mod en mere robust og koordineret europæisk tilgang til håndtering af dronetrusler.

Vi deler vurderingen af, at fjendtlige droner udgør en stigende risiko for kritisk infrastruktur. Droneoverflyvninger kan både true forsyningssikkerheden direkte og anvendes til overvågning og kortlægning af anlæg, som i forvejen er udsatte for komplekse trusler. Handlingsplanens ambition om at styrke EU's mulighed for at identificere, forebygge og håndtere sådanne trusler er derfor både rettidig og nødvendig.

Cyberalliancen støtter behovet for en fælles europæisk afklaring af roller og ansvar i håndteringen af dronetrusler. Et harmoniseret regelsæt vil styrke retssikkerheden, skabe ensartede rammer på tværs af medlemslandene og sikre, at kritiske sektorer ikke møder forskellige eller modstridende krav afhængigt af nationale fortolkninger.

Det er Cyberalliancens opfattelse, at bekæmpelse af fjendtlige droner er et myndighedsansvar. Dronebekæmpelse kræver operative beføjelser, specialiserede kompetencer, efterretningsmæssig kontekst og adgang til teknologier, der kan være både sensitivt og sikkerhedsklassificeret materiale. Det er derfor vigtigt, at politi, forsvar og relevante myndigheder fortsat bærer hovedansvaret for den operative håndtering.

Private ejere og operatører af kritisk infrastruktur kan supplere med viden om anlæg, risici og driftsforhold, men de bør ikke forventes at udføre indgreb, der potentielt kompromitterer myndighedernes efterforskningsmuligheder eller indebærer betydelige ansvarsmæssige risici. Opgaven er forbundet med betydelig kompleksitet, og private aktører sjældent vil være i en position, hvor det er hensigtsmæssigt eller sikkerhedsmæssigt forsvarligt at gennemføre sådanne indgreb.

Vi ser positivt på initiativet om etablering af digitale geografiske zoner omkring kritisk infrastruktur. Sådanne zoner kan bidrage til at forebygge uautoriserede flyvninger og skabe mere forudsigelighed i områder, hvor det er afgørende at undgå forstyrrelser af sikkerhed, drift eller kommunikation. Det er vigtigt, at disse zoner udformes i tæt dialog med de berørte infrastrukturejere og at de tænkes ind i udpegningen. Cyberalliancen lægger vægt på, at fremtidig regulering og implementering sker i et tæt samspil med erhvervslivet og de organisationer, der repræsenterer kritisk infrastruktur.

Cyberalliancen ser frem til det videre arbejde og står gerne til rådighed for faglige bidrag og dialog i processen. Vi deler Kommissionens ambition om at styrke Europas modstandskraft mod dronetrusler og ser handlingsplanen som et vigtigt element i at sikre robuste og sammenhængende rammer for beskyttelsen af kritisk infrastruktur i de kommende år.

Venlig hilsen

Cyberalliancen

Cyberalliancen repræsentere Green Power Denmark, Danske Rederier, Finans Danmark, Teleindustrien og F&P