

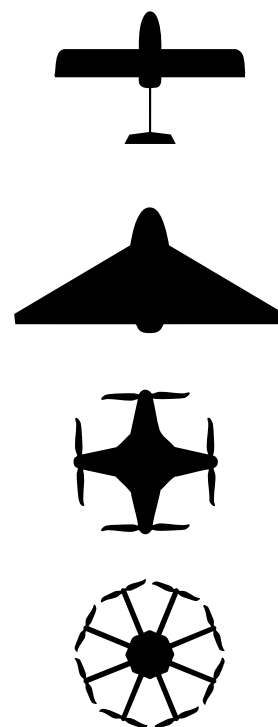
Skydd mot drönare



Drönare (även kallat UAS - **unmanned aircraft system** eller UAV – **unmanned aerial vehicle**) kan användas på olika sätt – ofta för nytta eller nöje men även i brottsligt syfte. Det kan handla om att en drönare flyger över förbjudna områden eller om att drönaren används som verktyg för brott genom att samla information, kartlägga områden, utföra sabotage, begå cyberintrång eller genomföra attentat med explosiva ämnen eller vätskor. Drönarhot innebär att skyddet inte bara kan utgå från vem som tar sig in. En drönare kan användas från avstånd och påverka verksamheten utifrån.

En incident med drönare kan bero på flera olika faktorer, och incidenten kan vara oavsiktlig eller avsiktlig.

Här kan det handla om okunskap om vilka regler som gäller eller vilka konsekvenser en handling kan få, eller oaktsamhet vad gäller att följa reglerna. Men det kan också handla om uppsåt, där syftet är att orsaka skada av något slag.



Figur 1. Incident med UAV – avsikt och konsekvens



Analysera behovet av skydd

En behovsanalys är nödvändig för välgrundade beslut, och analysen bör utgå från de skyddsvärden som kan påverkas av drönare.

En behovsanalys kan göras genom att

- identifiera skyddsvärden och deras sårbarheter för drönare
- identifiera möjliga start-, styr- och observationsplatser utanför området
- bedöma konsekvenser och sårbarheter för skyddsvärden
- bedöma om köer, samlingsplatser, infarter eller andra flöden skapar förutsägbara sårbarheter
- beskriva, och besluta om, möjliga åtgärder för att minska sårbarhet eller konsekvens
- bedöma kvarvarande risk.

Överväg lämpliga skyddsåtgärder

Det finns flera relativt enkla och kostnadseffektiva skyddsåtgärder som kan övervägas. Målet är ofta att göra skyddsvärden svårare att se, svårare att nå eller svårare att förstå.

- Insynsskydd kan monteras runt byggnader, anläggningar och tomtgränser eller vid de mest sårbara platserna för att förhindra eller försvåra insyn. Insynsskydd kan utgöras av växtlighet, fönsterfilm, staket, markiser eller persienner.
- Ytor och flöden kan utformas så att långvariga köer och täta folksamlingar undviks.
- Fysiska barriärer kan prioriteras vid platser där drönare annars kan nå eller observera skyddsvärden ovanifrån, till exempel entréer, köer, teknisk utrustning eller öppna ytor. Sådana barriärer kan t.ex. bestå av växtlighet, linor eller nät.
- Möblering och placering inomhus kan anpassas för att minska sårbarheten. Till exempel ska datorskärmar placeras så att de inte syns utifrån.
- Teknisk utrustning finns av många olika slag och varierar i effektivitet och prisbild. Sådan utrustning kan användas för att upptäcka, följa och klassificera ett objekt.
- Regler och riktlinjer för hur och var drönare får användas kring verksamheten kan användas för att informera allmänheten och som underlag för att utbilda personal. Regler och riktlinjer kompletteras med tydlig skyltning.
- Geografiska UAS-zoner kan användas för att förbjuda, begränsa eller hantera drönare inom skyddsvärda områden. Dessa visualiseras då på digitala kartor och i fjärrpilotens handkontroll.
- Övervakning med hjälp av till exempel kameror eller utbildad säkerhetspersonal som aktivt övervakar, hanterar och dokumenterar drönarverksamhet. Beakta även personer eller fordon som kan styra drönare från närliggande platser.
- Utbildning och beredskap kan omfatta att personal utbildas om hotet, hur drönare eller möjliga operatörer kan upptäckas och vad personalen förväntas göra vid en incident.
- Samverkan med myndigheter kan gälla att man tar fram en gemensam hotbildsanalys, genomför gemensamma övningar och delar information.



Drönare kan nyttjas i olovliga syften, t.ex.

Underrättelse

Insamling av data, skapa kartor.

Störning

Blockera, förhindra, falsklarm, störa radio/GPS.

Distraktion

Avleda säkerhetsresurser.

Cyberangrepp

Leverera skadlig kod eller utrustning.

Propaganda

Sprida känslig information eller desinformation.

Sabotage

Angripa utrustning eller byggnader.

Angrepp

Explosiver, farliga ämnen, skrämman.

Det finns flera kostnadseffektiva åtgärder för att enkelt öka motståndskraften mot olika typer av drönarhot.

Bedöm behovet av tekniska lösningar

Det finns olika tekniska lösningar för att upptäcka och varna för drönare. Dessa består ofta av sensorer (enskilda eller i kombination) och finns i storlekar från bärbara till stationära system.

Sensorer kan registrera olika typer av information:

- bild (visuella kameror eller IR)
- ljud (akustiska sensorer)
- objekt (radar)
- radiovågor (RF-sensorer).

Vissa enkla sensorer upptäcker enbart drönares identifieringssignaler, vilka måste sändas ut enligt lag.

Sensorernas prestanda påverkas av dagsljus, väder, signalmiljö och behov av fri sikt samt av förhållanden i omgivningen. Systemen kräver dessutom ofta uppdaterad mjukvara för att identifiera olika drönartyper.

Vilket system man väljer beror på ett antal parametrar:

- förvarningstid (tid mellan upptäckt och åtgärd)
- detektionsavstånd
- fast eller tillfällig montering
- möjlighet att flytta utrustningen
- möjlighet att indikera förekomst, riktning eller position
- kompetens hos och avsatt tid för den som sköter systemet.

Ofta krävs en avvägning mellan de olika parametrarna.

Läs mer

[Transportstyrelsens regler för drönare](#)

[Transportstyrelsens information om geografiska UAS-zoner](#)

[Luftfartsverkets drönarkarta](#)

[Polisens information om regler för drönare](#)

[Myndigheten för samhällsskydd och beredskaps vägledning om säkerhet i offentlig miljö](#)