KAPITTEL 9

Droners mørke side

Knut Torbjørn Moe

I militæret er droner blitt brukt til alt fra øvelser for antiluftskyts til spionasje i fremmede territorier. Siden årtusenskiftet er droner i økende grad blitt brukt til sivile formål, med akselererende teknologisk utvikling fra sivile systemer for profesjonelle formål til dagens rimelige, men avanserte, hobbydroner. Når hvem som helst kan anskaffe en drone, lære seg å fly den på noen timer, og utstyre den med den nyttelasten han eller hun ønsker – hvilke konsekvenser har dette for samfunnets sikkerhet? Har samfunnet skaffet seg en ny risikofaktor som ikke er vurdert grundig nok? Beskyttelse mot droner er et ferskt fagfelt som er i rivende utvikling. Vi skal i dette kapitlet gi et oversiktsbilde over hvilken risiko droner kan utgjøre, hva som kan gjøres for å planlegge egen sikkerhet, og hvilke tiltak man kan treffe for å redusere faren for uønskede konsekvenser.

Med unntak av den historiske gjennomgangen så er dronene det refereres til i dette kapitlet, små, kommersielle, allment tilgjengelige systemer. De befinner seg innenfor den militære klassifiseringen «Group 1», kjennetegnet av at de veier mindre enn ti kilo, flyr lavere enn 1200 fot og saktere enn 100 knop. I tillegg har vi definert at de i hovedsak koster fra 5000 til 15 000 kroner.

Når teknologi blir allment tilgjengelig, betyr det at alle som ønsker det, får tak i produktet. Alle kjøpere bruker produktet til å dekke eget behov og interessefelt. Mødre og fedre, barn og unge, profesjonelle, forskere, myndigheter og kunstnere, men også kriminelle og terrorister, har tilgang til droner. Det er mange eksempler på at ny teknologi brukes destruktivt: Kryptering som sikrer trygg kommunikasjon for alle, brukes av IS til å skjule egen kommunikasjon for politi og forsvar. YouTube, som gjør det

mulig å spre videoinnhold til hele verden, brukes som kringkastingskanal for høyreekstreme. Facebook, som lar deg holde kontakten med venner og kjente, brukes av pedofile til å finne bilder av barn.

Droner har eksistert siden før andre verdenskrig, men da for militær bruk. En nødvendig komponent i ethvert dronesystem er systemets evne til å forstå nøyaktig hvor det er til enhver tid. Den amerikanske visepresidenten Al Gore annonserte i 1998 at deres militære GPS-system også måtte kunne gi presise posisjonsdata til sivile systemer. Frem til denne endringen ble implementert 2. mai 2000, hadde GPS-satellittene kun gitt en presisjon på cirka 100 meter. Denne endringen gjorde presis tredimensjonal posisjonering mulig, og dette ble startskuddet for den sivile dronebransjen. I løpet av 2000-tallet utviklet det seg en sub-industri som jobbet med å utvikle droner til industrielle nytteformål. I 2012 skjedde en revolusjon da det kinesiske selskapet DJI kom med sine «folkedroner», DJI Phantom – og etter hvert DJI Inspire, DJI Mavic og DJI Spark. I løpet av 18 måneder gikk droner fra å være en nærmest ukjent teknologi til å bli folkeprodukter. Det var kun en liten gruppe mennesker som så konturene av sikkerhetsproblemene dette ville skape. I 2017 selges det flere hundre tusen droner på verdensbasis hver måned. Det vil være naivt å tro at ingen av disse ender opp hos mennesker som har destruktive mål med teknologien.

Reguleringene blir hengende etter

Alle produkter som lanseres, må forholde seg til gjeldende lovverk. Bruk av droner må rette seg etter luftfartens omfattende, internasjonale lovverk. I Norge er det Luftfartstilsynet som forvalter regelverket. Lovene som regulerer luftfarten, har vokst frem siden brødrene Wright først fløy langs stranden i Kitty Hawk i 1903. Siden ulykker innen luftfarten har svært store konsekvenser, har formålet siden den gang vært å skape en høyest mulig grad av sikkerhet for alle som flyr. Hvis man ser på antall flyulykker med dødelig utgang, var det i 1950 mer enn 100 hendelser, i 1990 50 hendelser, og i 2016 18 hendelser. Dette viser hvor kraftig nedgangen i uønskede hendelser har vært. Det markerer også hvor viktig det er med reguleringer som eksempelvis sier noe om hvor ofte et fly skal vedlikeholdes, hvor stor

avstand det må være mellom fly i luften, og teknologiske nyvinninger som GPS, lette materialer og dataassisterte kontrollsystemer.

Siden droner er flyvende fartøy, vil de samme reglene i utgangspunktet gjelde for droner som for en BOEING 747 jumbojet. Og det er her konflikter oppstår: Privatpersoner med drone som hobby forstår ikke hvorfor de trenger å utarbeide 100 sider lange risikomanualer og prosedyrebeskrivelser for å ta bilder av hus eller natur. I hovedsak blir det derfor til at kun de som skal jobbe med kommersielle droneoperasjoner, gjør jobben med å etablere en grundig metodikk for sitt arbeid. Det er Luftfartstilsynet som godkjenner og fører tilsyn med virksomheter som utfører RPAS (Remotely Piloted Aircraft System) / droneoperasjoner i Norge. Det foreligger 3 RPAS Operator (RO)-klasser for selskaper som ønsker å jobbe kommersielt: RO-1, RO-2, RO-3. RO-1 er en kortfattet registrering på tilsynets nettsider, mens RO-1 og RO-2 krever innsending og godkjenning av risikoanalyser, operasjonsmanualer med videre.

Det er per juni 2017 så mange som 2 779 bedrifter og personer som har registrert seg hos Luftfartstilsynet, men bare 281 av disse er blitt godkjent RO2/RO3, resten har deklarert seg gjennom en prosess som tar mindre enn tre minutter å gjennomføre (RO1).

Bransjeorganisasjonen UAS Norway opplyser at det anslagsvis er solgt mer enn 50 000 droner i Norge. Tallet er noe upresist, grunnet omfattende parallellimport og innførsel fra utenlandske nettsteder. Så lenge bare 281 virksomheter har gjennomført den omfattende søknadsprosessen, kan det utledes at kun en brøkdel av 50 000 droneeiere har satt seg grundig inn i regelverket. Med all flyvningen som foregår, kan man forstå at en stor del av dette utføres av hobbyflyvere, eller av personer som jobber kommersielt uten de påkrevde godkjenninger. Det betyr også at en stor del av dagens droneoperatører flyr i et luftrom de ikke har forutsetninger for å forstå. Det samme luftrommet trafikkeres av rutefly, legehelikoptre, småfly, politihelikoptre og militære farkoster med piloter som forventer at andre farende følger reglene slik de er opplært til.

Dette er bakgrunnen for at norske myndigheter forsøker å implementere et regelverk som skal gjøre ferdsel i luftrommet trygt for alle. Dette er et svært detaljert og omfattende arbeid. Det er derfor naturlig at det tar lang tid. Nye reguleringer vil ventelig kun bli fulgt av godkjente RO1/2/3-

virksomheter, og dette tallet vokser også langsomt. På den annen side forventes det at salgstallene for droner øker ytterligere de neste årene.

Bare i løpet av høsten 2017 har tre flyplasser måttet stenge fordi droner befant seg i det kontrollerte luftrommet, konserter er overflydd av entusiastiske fotografer, og uønskede hendelser har funnet sted over kjente steder som Preikestolen i Rogaland. Disse hendelsene er ikke utført av godkjente virksomheter som har gjort feil. Det er all grunn til å tro at uvitenhet om gjeldende lover og regler har vært en viktig faktor.

Vi har med andre ord å gjøre med en teknologi der andelen brukere som er profesjonelle, har vært liten og amatørandelen er helt dominerende. Amatørene er lite interessert i luftfart og reguleringer, de er derimot svært interessert i å fly og ta fete bilder. Det er med andre ord stor risiko for at vi vil oppleve en økning i uønskede dronehendelser de kommende årene.

Kjente hendelser

Mediene har de siste årene dekket en lang rekke dronerelaterte hendelser. For å bedre forstå trusselen er det klokt å se nærmere på hva som kjennetegner noen av disse hendelsene. Den 15. september 2013 deltok Tysklands forbundskansler Angela Merkel på et valgkamparrangement i Dresden, sammen med blant andre daværende forsvarsminister Thomas De Maiziere. På arrangementet brukte en aktivist en Parrot AR-drone, og fløy den rett foran scenen for å protestere mot det militære Euro-Hawk-programmet.

Selv om dette var en fredelig demonstrasjon, var det et åpenbart brudd på sikkerheten rundt landets statssjef og forsvarsminister. Dronen kunne båret eksplosiver, eller kjemiske/biologiske våpen, og det ble i ettertid åpenbart at dette var en risiko som måtte analyseres nærmere. Hendelsen blir av mange sett på som starten på den delen av droneindustrien som jobber med motmidler.

Under den store forsvarsøvelsen i Nord-Norge vinteren 2017 observerte styrkene i området en større mengde droner gjennom hele øvelsen. Det ble rapportert om et «to-sifret antall ukjente droner». Det er en kjent sak at militære styrker ser alvorlig på denne typen hendelser, da de øver på reelle situasjoner der det er viktig å ta vare på sikkerheten og kunne bevare hemmelighold rundt ressurser og materiell.

I asynkron krigføring er droner tatt i bruk for geotagging. Det er flere kjente eksempler i Afghanistan, Jemen og Ukraina på at droner er brukt til å finne nøyaktig geolokasjon for forsvarsstillinger. Dette gjøres ved å fly dronen rett over objektet man ønsker å lokalisere, peke kameraet rett ned, og lese av GPS-posisjonen. Dette gjør det mye enklere å treffe målet med raketter og granater. Enda enklere blir det naturligvis hvis man utstyrer dronen med en hjemmelaget bombe. Eksemplene over har hatt bred mediedekning. Terrorister, geriljakrigere og oppviglergrupper har fått en ny metode for å drive krigføring med redusert egenrisiko mot en overlegen makt.

I juli 2017 spilte bandet The Weeekend på Koengen i Bergen foran mer enn 15 000 unge tilskuere.
En fersk dronepilot brukte tiden til å fly over folkemassen på søken etter bilder og video. Piloten glemte å tenke på at droner tidvis faller ned. Det ville ha vært nærmest umulig å unngå å treffe mennesker på bakken hvis noe slikt hadde skjedd. Med en vekt på cirka et kilo og en flyhøyde på 100 meter ville en slik styrt tilsvare at noen ble truffet av en hard litersflaske med en fart på 160 km/t (målt i energi: 980 joules). Det er mer enn nok til å forårsake skade.

Selv om ingen droner falt ned ved dette arrangementet, var mangelen på sikkerhetsdisiplin åpenbar. De som var til stede, oppfattet raskt at farlige situasjoner kunne oppstå. Politiet slo ned på hendelsen i form av bot og inndragning. De siste årene er droner blitt operert på måter som bryter med regler og sikkerhetsforskrifter under flere festivaler og konserter i Norge. Noen ganger har det resultert i bøter, andre ganger har det ikke vært mulig å finne ut hvem operatøren har vært. Dette viser tydelig hvor vanskelig det er å oppdage at en drone er på vei (detektering), avsløre operatøren og eventuelt uskadeliggjøre dronen. Dette er ikke enkelt selv for militære styrker.

I januar 2015 fløy en ansatt i National Geospatial Intelligence Agency i USA en DJI FC40-drone fra leiligheten sin i Chinatown i Washington D.C., beklageligvis med det resultat at den krasjet på en av de best bevoktede plenene i byen – foran Det hvite hus. Selv om operatøren meldte sitt eget tokt til myndighetene, hjalp det ikke saken hans at promillen nok var litt høyere enn hva som er tillatt for bilkjøring. Atskillig mer tankevekkende var det likevel at ingen alarmer ble utløst, eller at dronen ble stoppet før den styrtet. Det tok også lang tid før vaktene fra Secret Service lokaliserte

dronen, selv om de hadde observasjoner av den over området. Selv ved verdens best bevoktede bolig kunne altså små, kommersielle droner entre området uten å bli oppdaget i tide eller bli stoppet.

Droneflyvning kan ha mange mål. I 2012 fløy en norsk kunstner over Det kongelige slott i Oslo for å lage et poeng av trusselen droner utgjør. Dronen svevde over et av de mest kjente og bevoktede objektene i landet i mer enn sju minutter. Likevel ble det ikke reagert mot dronen, uten at det er redegjort nærmere for grunnen til dette. Droner er vanskelige å oppdage, selv for trent sikkerhetspersonell. Det utgjør et problem som det er vanskelig å finne en enkel løsning på.

Risiko og eksempler

Risikofaktorene ved bruk av droner er mange, og her følger eksempler på dette.

Uvitenhet: Den første og største trusselen er operatører som på grunn av uvitenhet flyr droner i, over, eller i nærheten av lokasjoner hvor droner ikke skal benyttes. Flyplasser, fengsler, havner, militærbaser og store ulykker er alle steder hvor droner ikke har noe å gjøre uten grundig planlegging. Steder som dette har etablert regler for droner allerede, og utgangspunktet er at reglene følges.

I Norge alene selges titusenvis av droner i året. Man kan trygt anta at det finnes svært mange hobby- og semiprofesjonelle droneflyvere. Mange av disse har liten eller ingen kunnskap om reglene som styrer droneflyvning i Norge i dag. De skaper også trøbbel for alle som jobber med å avverge at droner brukes til alvorlig kriminalitet. Risikoanalyser omkring dronebruk må derfor være innrettet på måter som gjør at oppdaget droneaktivitet i strid med regelverket kan avskrives som uvitenhet og håndteres deretter.

Overvåkning: Kommersielle droner som selges i butikk, har bare i femårsperioden fra 2012 til 2017 redusert vekten fra tre kilo til 290 gram. Oppløsningen på bildene har gått fra VGA til ultra HD (4K), og rekkevidden er økt fra 100 meter til fem kilometer. En drone til 10 000 kroner kan i dag utføre svært avansert overvåkning. Alt fra personforfølgelse til bankran og spionasje er velegnede oppdrag for denne typen systemer. En DJI Mavic kan holde seg flyvende i 30 minutter og overføre HD-bilder i sanntid til en lukket YouTube-kanal, tilgjengelig for alle med passord og internettilgang.

Hvis man tar på seg spådomsbrillene, vel vitende om at droner bare fra 2011 til 2017 har utviklet seg fra fem kilos sværinger med dårlige kameraer og rekkevidde til dagens fjærlette systemer med 4K og flere kilometers rekkevidde, er det lite som tyder på at vi ikke i løpet av de neste årene vil se enda mindre og bedre systemer på markedet. Om ti-femten år er det ikke usannsynlig at en gruppe autonome droner bedriver ansiktsgjenkjenning og leverer sin nyttelast til rette vedkommende – hvor nyttelast kan være alt fra Amazon-varer, vedkommendes GPS-posisjon, eller nervegift. Det er heller ikke urealistisk å se for seg droner på størrelse med sommerfugler. Hvor går utviklingen etter 2017? I fremtidslitteratur leser man om droner mindre enn fluer, som agerer som insekter (og derfor ikke vekker mistanke) og som kan tilføre mennesker dødelige giftdoser. Realisme om få år, eller fri fantasi?

Smugling: Smugling har eksistert i flere tusen år. Så lenge det finnes varer som enten er ulovlige å flytte over visse grenser eller gjerder, eller varer som belastes med store avgifter – så vil det finnes smuglere som er villig til å risikere fengselsstraff for å tjene penger på flytting og salg av disse varene. Smugling innebærer risiko så lenge man er i besittelse av varene, og spesielt når man forserer kontrollerte soner som grenser, gjerder og så videre. Det er derfor ikke vanskelig å forstå at det må være fristende for smuglere å overlate besittelsen til maskiner som hverken skal ha betalt eller løper noen risiko for å bli arrestert og avhørt.

Droner har en løfteevne fra noen gram til hundrevis av kilo, og vi ser allerede nå utbredt narkotikasmugling mellom Mexico og USA. Det er grunn til å tro at denne aktiviteten vil vokse de kommende år.

Mapping: Mapping er et enkelt ord for fotogrammetrisk kartproduksjon. Kort fortalt er dette vitenskapen bak det å sette sammen mange bilder til å danne ett stort bilde. Dette kan brukes fra for eksempel fly. Man har gjennom flere tiår vært i stand til å ta en lang serie bilder fra luften, for å sette dette sammen til svært detaljerte tredimensjonale satellittbilder.

Droner har tilført muligheten til å lage denne typen bilder lokalt, enkelt og billig. Kartene er så presise at man kan beregne volumet på en jordhaug eller se registreringsnummeret på biler. Operatører kan til og med gjenta akkurat samme flyvning hver dag, og beregne masseforflytninger, ressursutvikling og lignende.

Terrorisme: Det tok kort tid fra droner ble allemannseie fra 2012 til terrorister så potensialet. Terrorister kan anvende droner på mange forskjellige måter. Poenget er at terroristene nå har tilgang til et mini-luftvåpen som er billig i drift og enkelt å sende ut. Vi skal ikke her gå i detaljer om hvordan dette kan gjøres, men det finnes flere generelle beskrivelser i mediene:

- Oversikt: Droner gir terroristen full oversikt over et område i sanntid. Denne informasjonen kan brukes til å skaffe informasjon om når et område er maksimalt fylt med mennesker, når et tog ankommer en bro, eller for samordning av koordinerte angrep.
- Geo-lokalisering: Når en drone befinner seg loddrett over et mål, vil den også kunne rapportere nøyaktige GPS-data for målet. Denne informasjonen kan brukes for å sende inn granater og raketter med stor nøyaktighet.
- Våpen-dropp: Små, potente våpen som granater, biovåpen, kjemiske våpen, til og med radioaktive «skitne bomber» er blitt festet til droner. De kan flys til ønsket mål med svært stor nøyaktighet.
- Avledning: En stor mengde droner kan avlede oppmerksomheten til sikkerhetsstyrker, og åpne opp for andre angrep.

Medier har rapportert om at terrorister og geriljagrupper har brukt droner til sine formål i land som Ukraina, Syria og Irak. Med en allestedsnærværende teknologi som droner er det nærliggende å tro at kriminelle elementer/terrorister i stor grad vil velge å benytte seg av de mulighetene som teknologien gir – også for angrep utenfor krigsområder.

Hacking: Alle virksomheter med et snev av bevissthet rundt egne, konfidensielle data, servere og maskinpark ønsker at bedriftsintern informasjon aldri skal komme på avveie. En kombinasjon av fysisk sikring, logisk sikring og menneskelig kunnskap skal hindre at dette skjer. Det er lite kjent at droner har vært brukt av hackere for å skaffe seg tilgang til data som skulle være beskyttet. Flere metoder er brukt:

- Såkalte sårbarhetsrutere som er i stand til å skanne et stort antall nettverkspunkter, teste for svake punkter, og gi illegitim tilgang til nettverket.

- Falske nettverk: Gjennom å sette opp et nettverk som gir seg ut for å tilhøre en bedrift og lure ansatte til å koble seg til dette, kan operatører avlytte all ukryptert datatrafikk på det falske nettverket.
- Falsk mobildekning: Gjennom å sette opp en falsk basestasjon kan operatører omgå iboende kryptering i GSM-nettet, og tilegne seg full tilgang til samtaler, meldinger og ukryptert datatrafikk.

Dette er et område med svært store mørketall, da bedrifter og virksomheter i svært liten grad rapporterer sikkerhetsbrudd innenfor IT, jamfør Mørketallsundersøkelsen fra Næringslivets Sikkerhetsråd for 2017. Kun fire prosent av alle IT-sikkerhetshendelser får dekning i mediene, og seks prosent offentliggjøres. Samme undersøkelse lister opp de viktigste årsakene til at sikkerhetsavvik oppstår. På toppen av denne listen finner vi «tilfeldigheter/uflaks» og «menneskelig feil» som medvirkende faktor i henholdsvis 74 prosent og 60 prosent av hendelsene. Dette er tall som vitner om at sterkere bevissthet om sikkerhet i stor grad ville kunne redusere antall uønskede hendelser. Disse tallene reflekterer trolig hendelser knyttet til droner.

Aktivisme: Politisk aktivisme kan skape store problemer i følsomme områder. Muligheter til å bringe inn budskap, flagg og symboler til store folkemengder er en uønsket utvikling. Det har allerede skjedd at demonstranter har flydd kontroversielle flagg over idrettsarrangementer på Balkan. Som en parallell kan man eksempelvis se for seg at høyreekstreme aktivister fester et stort hakekorsflagg til to droner, og flyr disse inn over Slottsplassen i Oslo på 17. mai. En handling som selvsagt ville skape store reaksjoner og avsky, men også frykt og panikk ettersom vi lever i et samfunn hvor terrorisme og følgene av den er noe folk tenker mye på.

Det finnes et utall av mer eller mindre organiserte sammenslutninger som kunne tenkes å bruke virkemidler som dette for å fremme sin sak.

Risikoanalyse: Vaktstyrker, politi og forsvar må gjøre seg kjent med hvilke kapasiteter droner besitter. Analysen bør inneholde kunnskap om hva som er mulig, hvordan man skal gå frem for å detektere tilstedeværelse, og hvilke tiltak som kan treffes hvis noe skjer.

Slike risikoanalyser kan gjøres på flere måter, primært sannsynlighetsbasert eller verdibasert. Sannsynlighetsbasert risikoanalyse tar utgangspunkt i sannsynligheten for at noe skjer i relasjon til hvor alvorlig en hen-

delse vil være. Verdibasert risikoanalyse tar utgangspunkt i en hendelses skadepotensial. Førstnevnte er å foretrekke, men forutsetter at man har god statistikk på det man søker å analysere. Gode eksempler kan være flom, brann, svindel og så videre.

Når det gjelder dronehendelser, finnes det ikke nok statistikk. Det er både fordi det er en ny teknologi, og, kanskje hovedsakelig, fordi det er store mørketall for dronehendelser. I likhet med cyberkriminalitet er det underrapportering av hendelser fordi offeret ikke ønsker å tilkjennegi sårbarhet. Verdibasert risikoanalyse vil derfor være å foretrekke inntil bedre statistikk foreligger. De fleste virksomheter har godt etablerte planverk og tiltaksplaner som er basert på gode risikoanalyser. All den tid et slikt rammeverk foreligger, bør også dronerisiko håndteres i det samme rammeverket. Sekundært finnes det en rekke gode tilgjengelige metoder for risikoanalyse.

Droner, risiko og fremtiden

Som vi har gått gjennom i dette kapitlet, har dronerevolusjonen brakt med seg en rekke nye risikoelementer som må håndteres ansvarlig. Det er tre primære komponenter som inngår: Forstå hva droner er i stand til, forstå hvilke trusler de utgjør og forstå hvordan dette kan true egen virksomhet. Siden fagområdet er ungt og med utilstrekkelige data for bred analyse, vil det være nødvendig å ha et våkent øye mot bransjen og gjøre egne vurderinger om hvor langt man skal gå for å sikre egen virksomhet.

Samfunnssikkerhet

En viktig komponent i samfunnssikkerhet bygger på risikoforståelse og -analyse. For at man skal kunne håndtere en gitt trussel, må man søke å forstå denne på en best mulig måte – deretter systematisk analysere denne informasjonen opp mot annen type risiko og bygge opp midler til mottiltak. For at risikoanalyser skal gi mening, må man være villig til å diskutere en faktors faktiske risikoprofil. Når det gjelder droner, så har diskusjonen i samfunnet i all hovedsak vært delt i to: En gruppe er, med rette, svært opptatt av hvordan man unngår at droner og fly kolliderer. Dette er en meget kompleks diskusjon som er godt beskrevet andre steder i boka. Den

andre gruppen er primært opptatt å pushe grenser for hva som er mulig med droner, og skape vakre prosjekter, bilder og filmer. Bransjen har i liten grad gitt oppmerksomhet til hvilke muligheter teknologien åpner opp for personer og grupperinger med onde hensikter. Dermed er disse faktorene i noen grad underkommunisert til de som utarbeider risikoanalyser.

Det første steget mot å løse et problem er å erkjenne at man har et. Dernest følger en analyse av behovet for å treffe tiltak som skal ta hånd om problemet. Dette ansvaret hviler på alle nivåer i samfunnet: politisk ledelse, de statlige og kommunale etater, privat næringsvirksomhet og hver enkelt av oss som individer.

Kriminell virksomhet

Alle virksomheter låser dørene sine. Om natten lukkes vinduene, man har en avansert alarm som sier fra til en nattevakt som passer på at ingen har sneket seg inn for å stjele eiendeler.

Det samme skjedde med cyberkriminalitet, etter hvert som internett ble allestedsnærværende. Virksomheter forstod raskt at de måtte skaffe seg forsvarsverker i form av sikkerhetsoppdateringer, kryptering og brannmurer, adgangsbegrensninger og så videre.

Droner åpner opp for en rekke typer kriminell virksomhet, både i det offentlige rom, i næringslivet og i privatsfæren. Man kan lett se for seg eksempler som:

- Noen som ønsker å smugle ulovlige varer inn i et fengsel
- Narkotikasmuglere som flytter varer over landegrenser
- Statsmakter som henter ut bildeinformasjon fra områder hvor de ikke har adgang
- Industrispionasje som utføres ved hjelp av falske nettverk på hustak

Man må som leder kunne identifisere disse nye truslene, forstå hvordan virksomheten er sårbar overfor truslene, og planlegge slik at man kan forsvare seg mot nye trusler på en planlagt og kontrollert måte. I det minste må man kjenne til truslene, for så å gjøre en vurdering om de er relevante for egen virksomhet.

Risikoanalyser må utvides

Fenomenet droner belyser et problem som er større enn droner alene. Samfunnet eksponeres stadig for nye teknologier som kan utgjøre en risiko for det offentlige rom og næringslivet. Hvor store disse problemene blir, er i stor grad avhengig av med hvilket bevissthetsnivå man velger å tilnærme seg problemet. Lavere bevissthet gir som regel et større problem etter hvert som teknologien får fotfeste.

For droner alene er det sentralt å tilegne seg kunnskap om hva de er i stand til. Da kan man vurdere risikoen og utvikle egne analyser så langt at man har en strategi og et planverk for hvordan egen virksomhet skal ruste seg og motstå eventuelle trusler.

Risikoreduserende tiltak

Norge har et meget godt og profesjonelt statlig tilsyn for luftfarten. Luftfartstilsynet identifiserte tidlig hvilken utfordring droner ville utgjøre, og har i flere omganger utarbeidet gode regler og rutiner for droneferdsel. Med en stor gruppe profesjonelle droneoperatører som følger reglene, så er bekymringene knyttet til denne gruppen relativt små. Disse aktørene har registrert seg, utarbeidet prosedyrebeskrivelser, satt seg inn i regelverk, skaffet forsikring og vet følgelig hva de begir seg ut på når de opererer i norsk luftrom. Reguleringer virker alltid på de lovlydige.

Det er allikevel solgt anslagsvis mer enn 230 000 droner i Norge. De som ikke er kjøpt av profesjonelle operatører, er kjøpt av privatpersoner med ukjent motiv for anskaffelsen. Ettersom dette markedet ikke er regulert, kan hvem som helst kjøpe hva som helst i hvilken som helst forretning. Hvis man følger etablerte amatørfora for droner på Facebook, vil man raskt forstå at en del av disse brukerne ikke har den nødvendige risikoforståelsen for å kunne utføre droneflyvning på en sikker måte, og at de heller ikke vil skaffe seg kunnskap om gjeldende lover og regler.

Dette betyr at det offisielle Norges kommunikasjon ikke når frem til disse operatørene, og at kunnskapsmangelen er en konstant faktor i dette segmentet. Når det observeres uønskede hendelser, ropes det ofte på innstramminger og presiseringer i lovverket. Men dette vil i hovedsak ramme den delen av bransjen som allerede følger regelverket – og mest sannsynlig

ikke de som faktisk er opphavet til den uønskede hendelsen. Man kan være helt sikker på at kriminelle og terrorister ikke har til hensikt å følge lover og regler, uansett.

Dette betyr også at man ikke kan stole på at samfunnet kan regulere seg vekk fra droneproblemer. Man må gjøre en selvstendig vurdering av hva den reelle risikoen er.

Når man skal vurdere risikoreduserende tiltak, må man ta utgangspunkt i hva som er teknisk mulig å få til, hvilke konsekvenser dette vil ha for det man ønsker å verne, og hva kostnaden er for å oppnå et tilfredsstillende nivå av sikkerhet. Normalt sett vil preventive tiltak ha en stor kost/nytte-effekt.

Forstå trusselen

Gjennom å skaffe seg god kompetanse om droner og forstå hvordan de kan anvendes til kriminelle handlinger, står man bedre rustet til å ivareta sikkerheten til sin egen virksomhet.

Uten meget god forståelse for egen virksomhet, og hvor sårbar den er for forskjellige droners egenskaper, vil en komplett risikoanalyse være vanskelig å lage. Gjennom kunnskap om egen bygningsmasse, IT-nettverkstopologi, omkringliggende områder og det øvrige samfunns interesse for virksomheten, kan man tegne opp en fysisk og logisk risikoprofil. Man må vurdere sannsynligheten for industrispionasje, tyveri, protestaksjoner og annet.

Preventive tiltak

Straks man har en forståelse av hvordan droner kan påvirke egen virksomhet, danner det utgangspunkt for omfattende, preventive tiltak som må implementeres.

- Instrukser er det laveste nivået. Man utarbeider prosedyrer for å håndtere dronehendelser. Eksempler kan være å skjule viktige elementer for foto fra luften, å skilte at dronetrafikk er uønsket og anmeldes, og at alt personell er kurset i håndtering av slike hendelser.
- Passive sikringstiltak: På dette nivået beslutter man eksempelvis å slå av trådløse nettverk, sjekke taket av bygninger regelmessig, og raskt kunne lukke alle persienner ved en hendelse.

- Aktive sikringstiltak: På dette nivået implementerer man sikringssystemer som deteksjon og automatisering av mottiltak – helt opp til manipulering av innkommende droner.

Iverksettelse av en tiltaksplan handler primært om kommunikasjon med relevant personell, og oppfølging av tiltakene over tid. Tiltaksplanen bør harmoniseres med øvrig sikkerhetsarbeid i virksomheten, og basere seg på samme metodikk.

Forsvarstiltak

Fra tidlige tider har de primære truslene mot mennesket kommet langs bakken og i vannet. Vi bruker ørene og et ganske godt utviklet syn til å høre og se bevegelse rundt oss. Men vi har til nå ikke hatt noe særlig å frykte fra himmelen. Mennesket er ikke trent til å oppfatte trusler fra himmelen. Når man jobber med å avsløre droner, er man fokusert i noen minutter og klarer å oppdage dem på litt langt hold, så mye som 100–200 meter ved normale optiske/akustiske forhold. Problemet er at det kan gå uker, måneder eller år mellom hver gang en uautorisert drone dukker opp på et gitt sted. Som tidligere beskrevet er trusselen umiddelbar og krever svært hurtig handling.

Erfaring viser at det er slitsomt, monotont og vanskelig å se eller lytte etter droner på himmelen. En person som er trent på vakthold, men som ikke vet når en drone skal komme, klarer å holde fokus på oppgaven i 15 til 30 minutter. Personer som ikke er fokusert på oppgaven, vil i de fleste tilfeller ikke oppdage en normal drone før den er i umiddelbar nærhet, eller at dronen av en eller annen grunn blir unormalt synlig (solrefleks eller lignende). Dette blir enda mer vanskelig dersom flyvningen finner sted om natten. Dette er grunner til at det er utfordrende å gi sikkerhetspersonell oppgaven med å oppdage droner 24 timer i døgnet. Dersom virksomheten, etter risikoanalyser, blir vurdert som sårbar, finnes det flere metoder som kan tas i bruk.

Detektere droner

Prinsippet med å erkjenne et problem for å kunne løse det har en logisk videreføring: Man må kunne iaktta problemet når det er til stede for å kunne reagere på det. Ettersom man ikke kan regne med at mennesker

uten videre vil kunne oppdage droner, vil første steg være å benytte seg av et system for å utløse alarmer og følge med hvor droner flyr. Det finnes flere fysiske egenskaper ved en drone som man kan benytte seg av for varsling.

- De fleste droner har et stort nok tverrsnitt til å gi ekko på en radar. Dette betyr at radarer vil kunne se droner.
- Droner vil utgjøre en kontrast på himmelen, hvilket betyr at et kamerasystem vil kunne oppdage dem som en prikk på himmelen. Om natten kan man oppnå noe av det samme med termiske kameraer.
- Droner flytter luft for å kunne fly, dette lager en karakteristisk lyd som egnede systemer vil kunne oppfatte og ved hjelp av avansert programvare identifisere som en truende drone.
- For å kontrollere dronesystemer benyttes radiosendere, både i kontrolleren og i dronen. Disse radiosenderne sender ut gjenkjennbare radiosignaler, som igjen kan brukes til å identifisere droner.

Det er en allmenn oppfatning blant dem som jobber med slike tiltak at det ikke finnes noen enkelt-teknologier som løser hele problemet. Det finnes i dag en rekke selskap som jobber med integrerte løsninger. Nøkkelen ligger i integrasjon og samhandling på tvers av deteksjonsteknologier:

Radar

Radarer fungerer godt når det gjelder å følge droner på ganske lang avstand, men trenger fri sikt til objektet. Radar kan identifisere og kan tegne en 3D (posisjon, høyde)-visning av objektet og dets flukt. Radarer må kunne skille fugler og annet på himmelen fra droner, og presentere en alarm med stor grad av sikkerhet. Samtidig er radaren mindre egnet til å dekke nærområdet man ønsker å beskytte.

Video

Video er godt egnet til tracking og identifikasjon, når man har avdekket hvor objektet befinner seg. Systemer som dette klarer å tracke og vise objektet på en skjerm for identifikasjon – men får selvsagt problemer om objektet blir borte bak trær og bygninger, og om natten.

Termisk

De fleste droner blir godt synlige på et termisk system, altså kamera som oppfatter varme objekter også i mørket. Disse kan oppdage innkommende droner på god avstand, men objektivene må rettes i korrekt retning først.

Akustisk

Akustisk deteksjon av droner har to primære grener, omni-direktive systemer og retningsbestemte systemer. De omni-direktive systemene preget bransjen tidlig, men rekkevidden var svært kort. Etter hvert har systemer som er retningsbestemte, og som gjennom avansert signalbehandling øker rekkevidden til flere hundre meter, kommet på markedet.

Akustiske systemer som detekterer droner, kan varsle om trusler i nærområdet. Disse systemene har vist seg effektive alene eller som del av et større system.

Frekvensdeteksjon

Det finnes en rekke systemer som fanger opp radiosignaler fra drone og kontroller, som oftest skjer på kjente frekvensbånd. Så lenge dronene sender på disse kjente båndene, og ikke flyr autonomt eller på mobil-modem, fungerer dette bra, selv om man får liten grad av posisjonering.

Andre metoder

Det utvikles stadig nye metoder for deteksjon, og erfaringen så langt viser at også denne utviklingen går raskt. Nye teknologier dukker opp stadig. Det er likevel nærliggende å tro at fremtidige løsninger kommer til å være variasjoner og/eller forbedringer av teknologiene nevnt ovenfor.

Tiltak ved dronehendelser

I det øyeblikket man griper inn overfor en drone, prøver man å manipulere et flyvende objekt i et veldefinert luftrom. Utfallet kan være at dronen kommer på avveie, krasjer eller kommer inn i luftrom den ikke hører hjemme i, med dertil hørende kollisjonsfare.

Luftfarten er styrt av en rekke lover og regler, og man kan ikke uten videre begynne å manipulere flyvende droner i Norge – og ikke forvente

straffeforfølgelse ved en eventuell ulykke. For det sivile samfunnet foreligger det derfor en rekke begrensninger på hva man kan gjøre med droner, for eksempel å manipulere dem. Det finnes allikevel en rekke ting man kan gjøre, uten å skape ytterligere fare overfor tredjepart.

En drone kan foreta seg en hel rekke ting når den befinner seg i nærområdet. Fra enkel overvåkning via smugling til aggressive handlinger. For sikkerhetspersonell er evnen til å følge med og vite hva dronen foretar, seg viktig. I et fengsel vil man kunne gjennomsøke berørte områder og celler. Andre ganger er det nok å vite at noen flyr en drone og reagere på grunn av det, eksempelvis fjerne VIP-er eller andre fra ubeskyttet område.

Passive tiltak

Ved objektbeskyttelse kan man treffe en lang rekke tiltak. På en bygning kan man koble sammen deteksjon av drone med en rekke smarthusfunksjoner:

- Straks senke utendørs persienner for å minimere innsyn
- Automatisk stenge luftevinduer, garasjer, dører og andre åpninger slik at ingenting kan fly inn, eller slippe last inn
- Stenge inntak for luftkondisjonering og/eller skru av inntaksvifter slik at eventuelle biokjemiske laster ikke kan trenge inn i luftesystemet
- Sende alarmer til sikkerhetspersonell, annet personell eller generell alarm, avhengig av risikonivå

Aktive tiltak

Dersom situasjonen tilsier det, vil det i enkelte tilfelle måtte vurderes om aktive tiltak skal tas i bruk. Det finnes mange mulige grep. Man kan for eksempel blokkere radiofrekvenser («jamming»), eller benytte kinetiske metoder (nett, kuler og sprenglegemer). Det understrekes at det i Norge ikke er tillatt å benytte seg av denne typen tiltak uten særlig tillatelse.

Andre muligheter kan være å benytte tett røyk, kraftige lys og lignende som gjør det svært vanskelig å gjennomføre kamerabaserte droneoperasjoner.

Uansett hvilke aktive tiltak man vurderer å implementere, er det svært viktig å innhente informasjon om hva som er lovlig fra Politiet, Luftfartstilsynet, Nasjonal Kommunikasjonsmyndighet, Nasjonal Sikkerhetsmyndighet og andre relevante parter, all den tid det ikke foreligger et eget lovverk for dette.

Vet lite ennå

Det foreligger i dag tilnærmet ingen forskning på omfanget av dronerelatert kriminalitet. Ettersom dronebransjen er så fersk, har kriminelle bare ganske nylig rukket å ta i bruk dette verktøyet til sine formål. Riktignok har vi allerede sett både omfattende smugling, overvåkning og krigføring. Det vil likevel måtte gå noe tid før man ser de faktiske konsekvensene av teknologien på samfunnet vårt. Ettersom det foreligger flere eksempler på dronerelatert kriminalitet, er det ikke overraskende at forsvar, politi og sikkerhetsbransjen følger dette nye fagområdet med argusøyne. Selv om det er for tidlig å konkludere om hvordan trusselen kan håndteres, viser erfaring at man med fordel kan tilegne seg informasjon knyttet til kapasiteter, risiko og tiltak. Det vil være naturlig å inkludere dronetrusselen i interne risikovurderinger og -analyser, og det bør jobbes mer med å dokumentere det faktiske omfanget på hendelser.