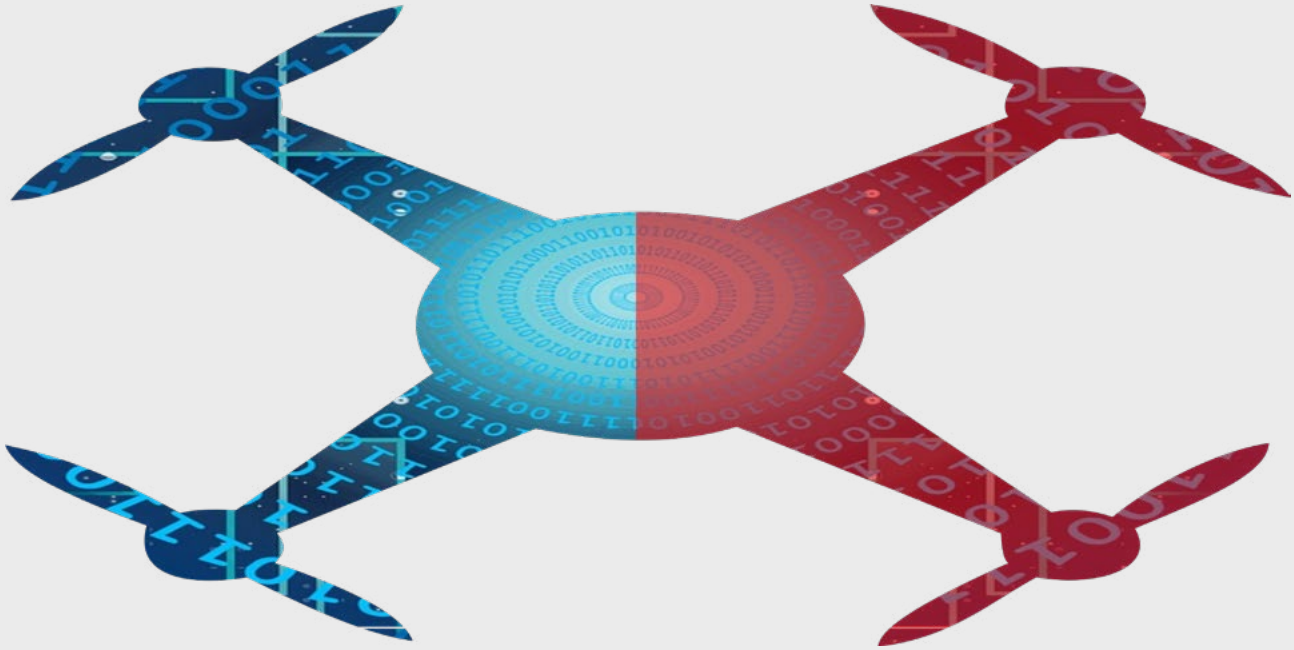
Myndigheten för samhällsskydd och beredskap

STUDIE

Artificiell intelligens för obemannade luftfartyg vid samhällsstörningar

Tillämpningar och sårbarheter



Artificiell intelligens för obemannade luftfartyg vid samhällsstörningar: Tillämpningar och sårbarheter

Artificial intelligence for unmanned aircraft systems in rescue services: Applications and vulnerabilities

Tidsperiod: 2019-2020
Utförare: MSB
Ansvarig forskare/författare: Peter Svenmarck, Maria Wikström, Erik Zouave, Mikael Krona

MSB:s Kontaktperson: Stefan Haggö, tel. 010-240 35 92

Omslag: FOI
Tryck: DanagårdLiTHO
Produktion: Advant

Publikationsnummer: MSB1577 - juni 2020
ISBN: 978-91-7927-041-4

MSB har beställt och finansierat genomförandet av denna forskningsrapport (alt. studierapport). Författarna är ensamma ansvariga för rapportens innehåll.

Sammanfattning

Denna rapport är en litteraturöversikt om artificiell intelligens (AI) med dess möjligheter och utmaningar för obemannade luftfartyg inom svensk verksamhet vid samhällsstörningar. Obemannade luftfartyg kan snabbt inhämta information från potentiellt farliga områden. AI kan bearbeta och analysera heterogena data på ett sätt som vida överstiger mänsklig förmåga. Rapporten riktar sig mot beslutsfattare, tekniker samt metod- och utvecklingsansvariga inom myndigheter och andra aktörer med ansvar för samhällsskydd och beredskap.

Litteraturöversikten visar att AI-tillämpningar för obemannade luftfartyg på flera sätt kan bidra till förmågor som används vid samhällsstörningar. För luftfartygens tekniska funktioner kan AI stödja navigering, beräkningseffektivitet, bildbehandling och koordinering av flera luftfartyg. För specifika fall av samhällsstörningar kan AI stödja detektion av bränder, översvämningar, jordskred, skador, människor, livstecken och ljud samt skapa provisoriska kommunikationsnätverk. Litteraturöversikten visar även att tillämpning av AI kan medföra nya sårbarheter som angripare kan utnyttja. Sårbarheterna innebär att luftfartygens navigering, automatiserade beslut och analyser kan störas eller förvanskas. Angripare kan även använda AI för att utföra cyberattacker mot obemannade luftfartyg. För att omsätta kunskapen i litteraturöversikten inom svensk verksamhet vid samhällsstörningar behövs bland annat utredningar av operativa behov och åtgärder mot AI-sårbarheter.

Summary

The report is a literature review of artificial intelligence (AI) with its possibilities and challenges for unmanned aircraft systems (UAS) in Swedish rescue services. UAS can rapidly gather data from potentially hazardous locations. AI can process and analyse heterogeneous data in ways that significantly exceeds human capabilities. The report is intended for decision makers, engineers, and staff responsible for technology and method development within rescue services and crisis response.

The literature review shows that AI applications for UAS in many ways contributes to capabilities of rescue services. AI can support UAS technical functions for navigation, computational efficiency, image processing and coordination of several UAS. Further, AI can support specific crises by detection of fires, flooding, landslides, humans, life signs, and sounds, as well as create temporary communication networks. The literature review also shows that application of AI creates new vulnerabilities that attackers may utilise. The vulnerabilities means that UAS navigation, automated decisions and analyses may be interfered or distorted. Attackers may also utilise AI for cyberattacks against UAS. Further investigations of operational needs and countermeasures against AI-vulnerabilities are required to utilise the results of the literature review.

Innehåll

1. Inledning

Tillgången till aktuell och korrekt lägesbild kan vara avgörande för hantering av samhällsstörningar. Två tekniker som har potential att bidra till dessa lägesbilder är obemannade luftfartyg (eng. Unmanned Aircraft System, UAS) och artificiell intelligens (AI). Obemannade luftfartyg kan snabbt inhämta information från potentiellt farliga områden. AI kan bearbeta och analysera heterogena data på ett sätt som vida överstiger mänsklig förmåga.

Det beräknas att 14 procent av de kommunala räddningstjänsterna i Sverige använde obemannade luftfartyg i sin verksamhet redan år 2017 och att 11 procent samtidigt höll på att införskaffa obemannade luftfartyg (Olofsson, 2017). Integreringen av obemannade luftfartyg i verksamheten vid samhällsstörningar förväntas ge ökad flexibilitet, uthållighet och kostnadsminimering till verksamheten (Näsström, Hagström, Mårtensson, Nilsson & Woltjer, 2017). Obemannade luftfartyg används bland annat för att identifiera, kartlägga och följa skadliga händelseförlopp (Hovelsrud Oddevald & Falk, 2015; Näsström m.fl., 2017; EDA, 2020). Den tänkta användningen av obemannade luftfartyg är omfattande och inbegriper exempelvis bränder, kemolyckor, oljeolyckor och ras. De obemannade luftfartygen förväntas förstärka den strategiska förmågan genom att bidra till upprätthållandet av aktuell lägesbild och därmed med information av värde för inriktning och samordning vid kriser (Näsström m.fl., 2017; MSB, 2018b).

Användningen av AI för obemannade luftfartyg har uppmärksammats i MSB:s (2018b) vägledning om obemannade luftfartyg i kommunal räddningstjänst. Det finns flera möjliga tillämpningar av AI för hantering av samhällsstörningar. Exempel på sådana tillämpningar är analys av storskalig data från krissituationer (WeRobotics, 2018; Qadir m.fl., 2016), simuleringar för träning av personal (Khalil, Abdel-Aziz, Nazmy & Abdel-Badeeh, 2008), automatiserat och semiautomatiserat beslutsstöd vid samhällsstörningar (Khalil m.fl., 2008; Kejriwal & Zhou, 2019), navigering och framförsel av smarta robotar vid samhällsstörningar (Apvrille, Tanzi & Dugelay, 2014; Khalil m.fl., 2008) och objektigenkänning (Apvrille m.fl., 2014; EDA, 2020). Förhoppningen är även att smart robotteknik kan förbättra verksamhetens ”uthållighet […] robusthet, redundans, effektivitet och flexibilitet” samt öka risktoleransen inom vissa typer av verksamhet i farliga miljöer (Svenmarck & Bengtsson, 2018).

Förutom nya möjligheter innebär utvecklingen av AI utmaningar. Vissa AI-tekniker är sårbara för antagonistisk manipulering som är svår att upptäcka (Svenmarck, Luotsinen, Nilsson & Schubert, 2018). Utvecklingen av AI-modeller förutsätter en god tillgång till träningsdata som kan vara svårt att upprätta (Svenmarck m.fl., 2018). Det finns även en växande farhåga att AI kommer att förstärka hotaktörers förmåga att genomföra digitala, fysiska och politiska angrepp mot samhället (Brundage m.fl., 2018). AI-tekniker skulle således kunna stödja hotaktörers ambitioner genom att bidra till resurseffektiva, skalbara och anpassade angrepp som kan maskeras och förnekas (Brundage m.fl., 2018; Horowitz m.fl., 2018). Förutsatt att utmaningarna med AI kan hanteras, finns förutsättningarna att AI kan öka förmågan hos obemannade luftfartyg inom räddningstjänsten.

1.1 Syfte

Syftet med denna rapport är att presentera resultaten av en litteraturöversikt om möjligheter och utmaningar med AI för obemannade luftfartyg vid hanteringen av samhällsstörningar. Litteraturöversikten baseras på två frågeställningar:

- Vilka aktuella AI-tillämpningar utarbetas inom forskning och utveckling för verksamhet med obemannade luftfartyg?
- Vilka hot och sårbarheter inom obemannade luftfartyg kan exploateras med stöd av AI?

Rapporten riktar sig främst mot beslutsfattare, tekniker, metod- och utvecklingsansvariga inom myndigheter och andra aktörer med ansvar för samhällsskydd och beredskap.

1.2 Metod

Litteraturöversikten omfattar AI-tillämpningar och sårbarheter som kan exploateras med AI relaterat till obemannade luftfartyg inom verksamhet vid samhällsstörningar. I litteraturöversikten ingår vetenskaplig litteratur, försöksverksamhet med obemannade luftfartyg vid samhällsstörningar samt rapporter och vägledningar från MSB på området. Litteratursökningar genomfördes med följande engelska sökord: *adjustable autonomy, artificial intelligence, autonomous technologies/systems, crisis management, rescue drones, UAV, unmanned aerial vehicle, UAS, unmanned aircraft system, threat* och *malicious*. Litteratursökningarna genomfördes med Google Scholar, Scopus och IEEE Explore.

1.3 Avgränsningar

Fokus för litteraturöversikten är tillämpningen av AI-tekniker, exempelvis maskininlärning och djupinlärning, snarare än teoretiska studier om maskinell kognition. Studien var även särskilt fokuserad på tillämpningar med relevans för svensk hantering av samhällsstörningar. Enligt MSB (2018a) omfattar samhällsstörningar ”de företeelser och händelser som hotar och ger skadeverkningar på det som ska skyddas i samhället”. Litteraturöversikten är avsedd att avspegla områdets omfattning snarare än att detaljerat beskriva samtliga studier som har genomförts.

1.4 Disposition

Rapporten inleds med en kort bakgrund om obemannade luftfartyg och de vanligaste AI-teknikerna i Kapitel 2. Resultaten från litteraturöversikten redovisas i Kapitel 3 i form av tekniska funktioner i obemannade luftfartyg som kan stödjas och förstärkas med AI, tillämpningar av AI för obemannade luftfartyg vid samhällsstörningar samt sårbarheter inom obemannade luftfartyg och angreppsvektorer med AI. Kapitel 4 innehåller en analys med diskussion om resultaten från litteraturöversikten. Slutligen redovisas rekommendationer i Kapitel 5 och slutsatser i Kapitel 6.

2. Bakgrund

Kapitlet inleds med en beskrivning av hur svensk räddningstjänst i MSB (2018b) och litteraturen indelar obemannade luftfartyg samt deras delkomponenter och generella förmågor. Exempelvis utifrån storlek, framdrivning, navigering och sensorer (avsnitt 2.1). Därefter beskrivs vad AI innebär och vanliga AI-tekniker (avsnitt 2.2).

2.1 Obemannade luftfartyg

Utformningen av obemannade luftfartyg, deras system och delkomponenter påverkas utav deras tilltänkta syfte och användningsområde. Ytterligare avvägningar och faktorer som påverkar utformningen av obemannade luftfartyg är kostnadseffektivitet, vilken typ av tilltänkt förmågehöjning som systemet syftar till samt vilka typer av risker som ska minimeras eller hanteras vid användningen av systemet (Bethel, Carruth & Garrison, 2012).

I svensk räddningstjänst är storlek på obemannade luftfartyg en övergripande faktor för deras indelning. Enligt MSB:s (2018b) vägledning för kommunal räddningstjänst och Näsström m.fl. (2017) inbegriper storleksklasserna små obemannade luftfartyg (maxvikt 7 kg), medelstora obemannade luftfartyg (vikt 7 till 25 kg) och stora obemannade luftfartyg (vikt överstiger 25 kg). Tekniska faktorer som avgör vilken storlek som väljs omfattar bland annat vilka typer av laster eller sensorer som luftfartyget ska bära, vilken databearbetningskapacitet som behövs och vilka energikrav som ställs (Mastroddi, 2014). Utöver detta påverkar organisatoriska faktorer vilken storlek som är lämplig; exempelvis tillstånd, underhåll och tillgången till utbildad personal för att använda och underhålla olika viktklasser (MSB, 2018b).

Ytterligare en vanlig faktor för indelning av obemannade luftfartyg är framdrivningsmetod. Generellt sett kan luftfartyg ha rotationsbaserad framdrivning (t.ex. propeller), vindbaserad framdrivning (t.ex. glidflygning) eller biomimetisk framdrivning (t.ex. flaxande vingar) även om det sistnämnda är relativt ovanligt (Hambling, 2016; Rifai, Marchand, Poulin & 2008). Ett sätt att skilja på de vanligaste varianterna av obemannade luftfartyg, som är rotationsbaserade, är att dela in dem utifrån om de har roterande vingar, vanligtvis kallade multikoptrar, eller fasta vingar (MSB, 2018b).

Olika typer av obemannade luftfartyg har olika former av rörlighet, robusthet och miljöhållbarhet. Multikoptrar startar och landar vertikalt, vilket är en klar fördel under insatser i exempelvis tätbebyggda områden och skog (MSB, 2018b; Thamm m.fl., 2015). Multikoptrar kan flyga nära hinder och hovra, men eftersom de aktivt måste skapa sin lyftkraft under hela flygningen är de oftast inte lika uthålliga som luftfartyg med fasta vingar som dynamiskt skapar en stor del av lyftkraften med hjälp av vingarna (MSB, 2018b; Thamm m.fl., 2015). Luftfartyg med fasta vingar lämpar sig bättre för övervakning från högre höjd och kan ofta flyga snabbare än multikoptrar (MSB, 2018b). Luftfartyg med fasta vingar behöver däremot oftast en större yta för start och

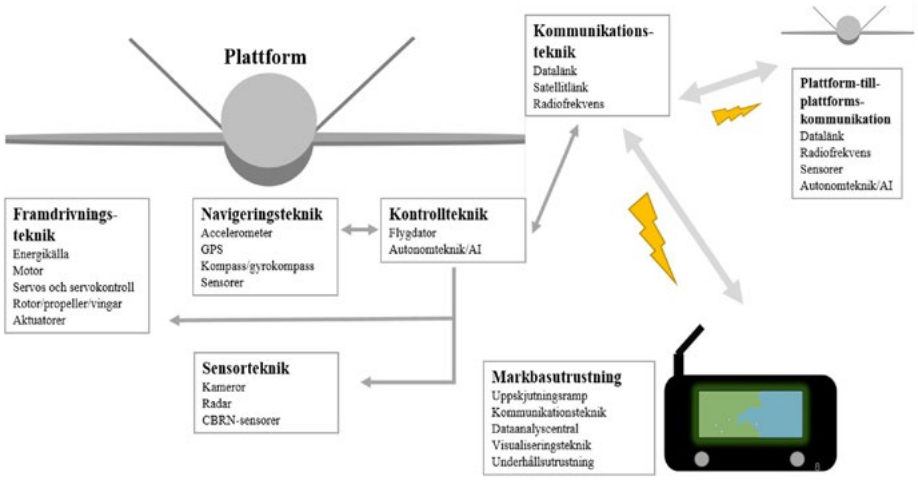
landning då de antingen kastas för hand eller kräver en startramp för att lyfta samt kräver en viss sträcka för att kunna landa (MSB, 2018b). Thamm m.fl. (2015) tillägger också att den högre farten vid landning riskerar att skada både luftfartyget och dess potentiellt dyrbara last. Hybrider beskriver luftfartyg som kombinerar rotorblad med fasta vingar för att möjliggöra vertikal start och landning, hög hastighet och lång uthållighet (Ozdemir m.fl., 2014).

Signalbaserade navigeringsmetoder, som är vanligt förekommande, omfattar radionavigering, radarnavigering och satellitnavigering (Rantakokko, Strömbeck & Marsten-Eklöf, 2016; Rydell, Hulgren & Strömbeck, 2017). I Rydell m.fl. (2017) behandlas även bildbaserad navigering, det vill säga observation av föremål som en sensor rör sig över, landmärkesbaserad navigering (observation av definierade och fasta föremål) samt kartor och terrängmodeller.

Valet av sensorteknik påverkar också systemets förmåga. Sensorer brukar delas in i elektrooptiska sensorer, radar och CBRN-sensorer (MSB, 2018b; Näsström m.fl., 2017). Elektrooptiska sensorer kan skapa bilder baserade på olika ljusvåglängder (ultraviolett, synligt, nära infrarött och infrarött) där vissa våglängder exempelvis kan penetrera dimma och indikera värme. Radar baseras på kortvågiga radiosignaler som kan tränga igenom dåliga väderförhållanden, exempelvis regn och snö. CBRN-sensorer inbegriper indikatorer som bland annat kan detektera kemiska och biologiska ämnen.

Eftersom utformningen av obemannade luftfartyg beror på ett flertal omständigheter är det inte möjligt att göra en heltäckande kartläggning av olika system och deras delkomponenter. Ett normalfall för samhällsstörningar är ett sensorbärande system (MSB, 2018b) utifrån vilket det går att göra en övergripande kartläggning (Pastor, Rubio & Royo, 2006; Park m.fl., 2007; Altawy & Youssef, 2016). I Figur 1 skildras övergripande delkomponenter med exempel.

Figur 1. Delkomponenter hos ett obemannat luftfartyg (Bild av Zouave, Bruce och Svensson).



2.2 Artificiell intelligens

AI handlar om att konstruera datorsystem som uppvisar intelligent beteende (Nationalencyklopedin, 2020). Några av de områden som studeras inom AI är problemlösning, representation av mänskliga kunskaper, planering, lärande, förståelse av naturligt språk, perception och robotars beteende (t.ex. Frankish & Ramsey, 2014). Genom att kombinera flera av dessa förmågor kan intelligenta agenter skapas som känner av och tolkar omgivningen, identifierar och värderar åtgärder samt genomför dessa (Russell & Norvig, 2009). Självkörande bilar är ett exempel på intelligenta agenter.

De senaste årens framgångar inom AI-området har framförallt skett inom maskin- och djupinlärning. Maskininlärning (eng. machine learning) handlar om att med datorer skapa en modell för hur svaret beror av indata utifrån många exempel. Under lång tid begränsades prestationen inom maskininlärning av att de särdrag (utmärkande egenskaper) som särskiljer indata för en viss tillämpning enbart kunde skapas manuellt, vilket krävde omfattande kunskaper och erfarenhet (Goodfellow, Bengio & Courville, 2016). Detta problem har på senare år lösts med djupinlärning (eng. deep learning) där systemet även lär sig hur särdragen ska utformas för att beskriva indata. Djupinlärning förutsätter så kallade neuronnät där miljontals matematiska operationer som multiplikation och addition används för att modellera komplexa funktioner.

Neuronnät kan tränas med övervakad inlärning när det finns ett svar för vad som ska detekteras i indata och med oövervakad inlärning för att detektera strukturer i indata utan att ange dem explicit. Förstärkningsinlärning (eng. reinforcement learning) är en ytterligare typ av inlärning som är särskilt lämpad för att lära strategier för spel mellan två parter. Förstärkningsinlärning kombineras ofta med djupinlärning för att uppskatta hur bra möjliga alternativ är. Ett välkänt exempel är när förstärkningsinlärning användes för att träna AlphaGo som besegrade en professionell Go-spelare (Silver m.fl., 2016).

En stor del av forskningen inom djupinlärning handlar om att konstruera arkitekturer för neuronnät som både har hög prestanda för specifika tillämpningar och samtidigt kan tränas på rimlig tid. Några exempel på arkitekturer för neuronnät är:

- Faltningsnät (eng. convolutional neural networks): Används för att processa spatiala data som till exempel bilder där närliggande pixlar har tydliga relationer till varandra.
- Återkopplade neuronnät (eng. recurrent neural networks): Används för att processa sekventiella data som har temporala beroenden som till exempel text.
- Generative adversarial networks (GAN): Är en metod för att träna ett generativt neuronnät som syntetiserar data utifrån en uppsättning parametrar. GAN ger ofta bra generativa neuronnät eftersom metoden använder maskininlärning för att samtidigt träna det generativa neuronnätet och ett diskriminator neuronnät som särskiljer syntetiska och verkliga data.

Fler arkitekturer beskrivs exempelvis i Goodfellow m.fl. (2016). Eftersom beräkningarna för träningsiterationerna kan ske parallellt kan allt större neuronnät tränas med grafikkort som snabbt får allt högre beräkningskapacitet. En ytterligare faktor som är avgörande för många tillämpningar av neuronnät är den ökade tillgången till annoterade träningsdata med god kvalitet.

3. Resultat

Litteratursökningarna resulterade i totalt 90 publikationer av relevans för uppdragets frågeställningar: (1) AI-tillämpningar för obemannade luftfartyg och (2) sårbarheter som kan exploateras med AI. Litteraturöversikten inleds med AI-tillämpningar för obemannade luftfartyg i de tekniska funktioner i obemannade luftfartyg som kan stödjas eller stärkas genom AI (avsnitt 3.1). Denna del av litteraturöversikten berör förmågor som är grundläggande eller generella för användningen av obemannade luftfartyg i verksamheten som till exempel navigering och beräkning. Därefter beskrivs AI-tillämpningar för obemannade luftfartyg för specifika fall av samhällsstörningar (avsnitt 3.2). Dessa tillämpningar berör främst olika typer av detekteringsförmågor för att till exempel identifiera var och hur samhällsstörningar manifesteras, exempelvis vilka områden som drabbats av brand eller översvämning samt detekteringsförmågor som är mer riktade, exempelvis om det finns människor i ett område och om de är vid liv. Den avslutande delen av litteraturöversikten redovisar sårbarheter inom obemannade luftfartyg och angreppsvektorer som kan exploateras med AI (avsnitt 3.3).

3.1 Tillämpningar av AI för tekniska funktioner i obemannade luftfartyg

Ett övergripande sätt att tillämpa AI på är genom att möjliggöra respektive förstärka funktioner i de obemannade luftfartygen. Avsnittet beskriver även på vilka sätt AI har utvecklats för att stödja dessa funktioner och förmågor samt möjliggjort nya förmågor för obemannade luftfartyg. Dessa AI-teknologier omfattar AI-stödd navigering och hinderdetektering (avsnitt 3.1.1), AI-stödd beräkningskraft (avsnitt 3.1.2), AI-stödd bildbehandling (avsnitt 3.1.3) samt svärmteknik (avsnitt 3.1.4).

3.1.1 AI-stödd navigering och hinderdetektering

För tillfället sker omfattande forskning och utveckling om autonom navigering av obemannade luftfartyg. Det finns ett flertal sensorer och kameror som kan användas för detta syfte, där objektdetektering och objektigenkänning är en viktig del. Devos, Ebeid och Manoonpong (2018) använde sig av två LiDAR-sensorer (eng. Light Detection and Ranging) för upptäckt av hinder med ett återkopplande neuronnät för att på så sätt möjliggöra för luftfartyget att undvika dem. Författarna hävdar att sensorerna kan vara ultraljudssensorer eller LiDAR och att deras fördelar för upptäckt av hinder är att mängden högdimensionell signalbehandling är mindre jämfört med bildbehandlingen för datorseende.

Imanberdiyev, Fu, Kayacan och Chen (2016) beskriver en studie där förstärkningsinlärning har använts för autonom navigering av ett obemannat luftfartyg i en simulerad miljö. I sitt arbete har de tagit fram en algoritm som inte är lika beräkningstung som många andra modellbaserade förstärkningsinlärningsalgoritmer och som därmed lämpar sig för realtidssystem. Pham, La, Feil-Seifer

och Nguyen (2018) menar att förstärkningsinlärning kan möjliggöra att obemannade luftfartyg lär sig att navigera genom föränderliga och okända områden, vilket ofta är fallet vid räddningsaktioner. Obemannade luftfartyg som nyttjar denna algoritm behöver därmed inte förlita sig på en given modell av omgivningen.

Det pågår en omfattande forskning kring autonom navigering för obemannade luftfartyg i nanoklass, det vill säga obemannade luftfartyg som endast är ett par centimeter i diameter och väger några få tiotals gram. Deras storlek medför att de kan användas inomhus och undersöka områden som är svåråtkomliga för människor och större luftfartyg. Många obemannade luftfartyg är utrustade med GPS, men Palossi, Conti och Benini (2019) anser att detta inte inbegrips i begreppet autonom navigering då obemannade luftfartyg i detta fall är beroende av en extern ad-hoc signal/beräkning. GPS-signaler kan inte heller användas effektivt i inomhusmiljö (Apvrille m.fl., 2014). Palossi m.fl. (2019) skriver om de problem som forskning försöker lösa för autonom navigering av obemannade luftfartyg i nanoklass. Traditionell autonom navigering som använder en 3D-karta av omgivningen är väldigt beräkningstung. För väldigt små luftfartyg, med kort batteritid och som inte kan ta mycket last, tillåts inte tillräcklig beräkningskraft ombord. Palossi m.fl. (2019) beskriver istället en visuell navigationsalgoritm som baseras på ett faltningsnät och som inte är lika beräkningstung. I deras experiment kan ett obemannat luftfartyg navigera inomhus i en okänd miljö och undvika plötslig uppkomst av hinder på två meters avstånd vid en hastighet på 1,5 m/s.

3.1.2 Beräkningseffektivitet och beräkningsavlastning

När AI-system ska utföra alltmer komplexa uppgifter krävs större neuronnät som medger högre inlärningskapacitet på bekostnad av krav på högre beräknings- och minneskapacitet (Kouris, Venieris & Bouganis, 2019). Detta är en utmaning för obemannade luftfartyg eftersom ett ökat antal beräkningar ökar energiförbrukningen, vilket förkortar flygtiden. Utmaningen med ökad energiförbrukning blir än påtagligare för tidskritisk bearbetning av sensordata som till exempel autonom navigering (Kyrkou, Plastiras, Theocharides, Venieris och Bouganis, 2018; Kouris m.fl., 2019). För robust autonom navigering krävs att obemannade luftfartyg kan upptäcka hinder i realtid och väja för att undvika kollision (Kyrkou m.fl., 2018). Flera studier görs av mindre beräkningstunga algoritmer för autonom navigering (Imanberdiyev m.fl., 2016; Palossi m.fl., 2019).

Den stora mängden information som tas emot från sensorer och kameror skapar höga krav på att kunna hantera ett högt dataflöde. En vanlig lösning för system med begränsade resurser, såsom obemannade luftfartyg, är att avlasta beräkningar på mer kraftfulla fjärrenheter (Kouris m.fl., 2019). Apvrille m.fl. (2014) och Xu, Ota och Dong (2019) har genomfört studier kring kameror och AI för navigering av obemannade luftfartyg. Deras forskning syftar till att hantera den begränsade beräkningskraften ombord genom att använda en avlastande fjärrenhet. Luftfartyget skickar då bilder till fjärrenheten som analyserar dessa och räknar ut flygkommandon som skickas tillbaka till luftfartyget. Apvrille m.fl. (2014) påpekar dock att detta kräver robusthet mot signallatens och störningar. På senare år har arkitekturen för obemannade

luftfartyg utvecklats mot att undvika beroende av fjärrenheter, dels på grund av att det kan bli en flaskhals när många obemannade luftfartyg eller andra enheter kommunicerar med fjärrenheten och dels på grund av cyberattacker som kan reducera tillgängligheten på fjärrenheter och då förhindra att obemannade luftfartyg fungerar korrekt (Fraga-Lamas, Ramos, Mondéjar-Guerra & Fernández-Caramés, 2019).

3.1.3 Bildbehandling

AI har möjliggjort objektdetektering i realtid med stor noggrannhet. För att med begränsad flygtid hinna söka av och kartlägga ett område är ett alternativ att flyga högre upp (Haris, Watanabe, Fan, Widyanto & Nobuhara, 2017). Stora avstånd och omgivande ljus är dock exempel på faktorer som kan försvåra objektdetektering (Magoulianitis, Ataloglou, Dimou, Zarpalas & Daras, 2019). Med hjälp av AI kan system lära sig att öka bildupplösningen så att korrekt detektering av objekt kan ske (eng. super resolution). Detta har exempelvis påvisats av Magoulianitis m.fl. (2019) som ökade ett systems förmåga att detektera obemannade luftfartyg på långt avstånd, vilket annars kan vara svårt och förväxlas med exempelvis flygplan och fåglar. Haris m.fl. (2017) använde sig också av AI för att uppnå ökad bildupplösning av bilder tagna från ett luftfartyg, vilket då gav högre kvalitet vid 3D-rekonstruktion utifrån bilderna.

Djupinlärningsmetoder baserade på Generative Adversarial Networks (GAN) har visat sig användbara inom många områden, inte minst bildbehandling (Chen m.fl., 2020). GAN har bland annat använts för att omvandla bilder, exempelvis syntetisera flygfoton från kartbilder, rekonstruera objekt från konturer och färglägga svartvita bilder (Isola, Zhu, Zhou & Efros, 2017; Perera, Abavisani & Patel, 2018). Chen m.fl. (2020) använde sig av GAN vid en typ av tomografi (avbildning i skikt) för att minska brus som uppstår när bilderna tas. Bilderna brusreducerades av en tränad generator för att förbättra kvaliteten. Ledig m.fl. (2017) tillämpade GAN för att återskapa fotorealistiska bilder vid övergången från lågupplösta till högupplösta bilder, där texturdetaljer annars kan saknas. Vidare beskriver Li, Li, Wu, Chen och Ngan (2019) hur de högupplösta bilderna kan genereras för att särskilt förbättra klassificeringen av små objekt som ofta är svårare att detektera och klassificera. GAN har också använts för att omvandla termiska IR-bilder, som kan vara svårtolkade för människor, till realistiska bilder inom det synliga spektrumet (Nyberg, Eldesokey, Bergström & Gustafsson, 2018).

3.1.4 Svärmteknik

Svärmteknik är de obemannade luftfartygens förmåga att kunna koordinera, formera och organisera sig gemensamt med andra obemannade luftfartyg (Ruetten, Regis, Feil-Seifer & Sengupta, 2020) och andra smarta robotar (Brodeur, Regis, Feil-Seifer & Sengupta, 2018). AI-baserad svärmteknik för obemannade luftfartyg undersöks till exempel för sökning och räddning (eng. Search and Rescue, SAR) (Ruetten m.fl., 2020; Zuhri, Zahari, Desia, Ismail & Al Haek, 2015) samt objektigenkänning (t.ex. Arola & Akhloufi, 2019). Användning av flera luftfartyg som

autonomt kan koordineras genom svärmteknik är intressant för scenarion där större områden måste avsökas. Svärmteknik kan möjliggöra:

- Styrning och kontroll av flera obemannade luftfartyg på ett sätt som överstiger mänsklig simultanförmåga (Ruetten m.fl., 2020).
- Användning av flera och potentiellt olika typer av sensorsystem i samma område för att öka avskanningsförmågan (Ruetten m.fl., 2020).
- Optimering av färdvägsplanering och avskanning av sökareor för att öka sannolikheten av lyckade detekteringsförsök (Zuhri m.fl., 2015; Brodeur m.fl., 2018; Arola & Akhloufi, 2019).
- Erhållande av en mer detaljerad områdesavskanning per batteritimme (Ruetten m.fl., 2020; Lomonaco, Trotta, Ziosi, Avila & Díaz-Rodríguez, 2018).

Svärmteknik kan anpassas utifrån olika användningsbehov. I centraliserad, hierarkisk styrning kan ett eller flera luftfartyg leda övriga system (Arola & Akhloufi, 2019; Panerati m.fl., 2018; Brodeur m.fl., 2018). De obemannade luftfartygen behöver då någon form av kommunikation med de övriga luftfartygen. Det finns även situationer när det inte är önskvärt att ha centraliserad koordinering eftersom ett fel hos ledaren kan få dess följare att fallera. Det kan också finnas situationer där kommunikation via uppkoppling eller sammankoppling bör undvikas (Arola & Akhloufi, 2019). Då kan styrningen decentraliseras till varje enskilt luftfartyg som baserar sitt eget beteendemönster på sensordata som beskriver de luftfartyg som befinner sig i direkt anslutning till dem (Ruetten m.fl., 2020).

I forskningslitteraturen användes svärmteknik huvudsakligen för att koordinera två typer av beteenden. Dels användes svärmteknik för att optimera de obemannade luftfartygens formation i förhållande till varandra (Ruetten m.fl., 2020; Brodeur m.fl., 2018) och därmed maximera sökområde per flygning i formation. I detta hänseende är en av tillämpningarna för AI och svärmtekniken att möjliggöra kommunikation mellan luftfartygen i en svärm (Lomonaco m.fl., 2018). Dels användes svärmtekniken för att träna och koordinera gruppens flygmönster. Detta tillåter en grupp obemannade luftfartyg att använda ett givet avskanningsmönster över ett område, till exempel utåt expanderande cirkulationsflygning (Zuhri m.fl., 2015) eller testa egna flygmönster för att optimera sökning över oförutsägbara terränger över tiden (Ruetten m.fl., 2020).

Ett antal olika AI-tekniker används för svärmar. Exempelvis kan koordinering mellan obemannade luftfartyg realiseras genom algoritmer som beräknar positionering genom RSSI (eng. Received Signal Strength Indicator) som är ett mått på hur väl utrustning kan motta signaler (Ruetten m.fl., 2020; Brodeur m.fl., 2018). Vidare kan koordineringen baseras på trådlös kommunikation (Di Felice, Trotta, Bedogni, Chowdhury & Bononi, 2014) i maskformiga nätverk (eng. mesh networks). Alternativt kan djupinlärning och faltningsnät tillämpas för bildbaserad koordinering och navigering (Arola & Akhloufi, 2019). Färdvägs- och sökmönsteroptimering kan tränas med simuleringar (Ruetten m.fl., 2020; Brodeur m.fl., 2018; Zuhri m.fl., 2015) och scenariomodellering (Panerati m.fl., 2018; Di Felice m.fl., 2014). Ruetten m.fl. (2020) använder neuronnät och genetiska algoritmer för att förbättra färdvägsplanering under träningen av systemen. Bayesianska eller Gaussbaserade modeller kan exempelvis tillämpas för att göra sannolikhetsberäkningar om terräng, rutt eller trolig placering av objekt eller personer i miljön (Waharte, Trigoni & Julier, 2009).

3.2 Tillämpningar av AI för obemannade luftfartyg vid samhällsstörningar

Vid en samhällsstörning är det viktigt att skapa sig en bild av dess påverkan och omfattning i ett tidigt skede för att kunna planera insatser och minimera risken för ytterligare spridning och därmed begränsa konsekvenserna. Det sker omfattande forskning kring tillämpningar av AI för obemannade luftfartyg. Med hjälp av obemannade luftfartyg, som kan utforska områden som kan vara svåråtkomliga och farliga för människor, kan en bättre lägesbild erhållas snabbt och effektivt. Med hjälp av AI för obemannade luftfartyg kan ytterligare stöd fås vid samhällsstörningar. Forskning som sker berör framförallt autonom detektering av olika slag. Detta avsnitt beskriver dessa tillämpningar.

3.2.1 Branddetektering i skog och mark

Bränder kan få förödande konsekvenser, vilket gör att korrekt och tidig detektering av bränder är av stor vikt (Akhloufi, Castro & Couturier, 2018). Med hjälp av ett obemannat luftfartyg utrustat med kamera och GPS kan högupplösta bilder tas emot tillsammans med information om position (Zhao, Ma, Li & Zhang, 2018). För att möjliggöra en snabbare upptäckt av brand i skog och mark sker en utveckling kring autonom branddetektering i bilder från obemannade luftfartyg. Studier gjorda av bland annat Zhao m.fl. (2018) och Merino, Caballero, Martínez-de-Dios, Maza och Ollero (2012) har resulterat i algoritmer som lokaliserar brand utifrån flygbilder fångade av visuella kameror och infraröda kameror. Det sistnämnda arbetet inkluderade även att uppskatta flammornas maximala höjd och brandens spridning för att ge ytterligare information för bekämpningen.

Det finns dock några svårigheter när det gäller att träna system att identifiera brand utifrån en bild då nedanstående faktorer gällande bränder kan variera stort (Zhao m.fl., 2018):

- färg
- form
- struktur (rök, lågor eller båda)
- bakgrund.

Vidare nämns i litteraturen att GPS inte är tillräckligt för att bestämma exakt position av detekterad brand då höjd och terrängtyp gör det svårt att översätta de identifierade pixlarna som innehåller brand till en exakt position i rummet (Hossain, Zhang & Yuan, 2019). Det finns dock metoder, bland annat användning av en tredimensionell framställning av terrängytan (Hossain m.fl., 2019) och analys med hjälp av flera obemannade luftfartyg (Akhloufi m.fl., 2018), som ger en mer exakt position.

3.2.2 Översvämningsdetektering

Flygbilder från obemannade luftfartyg är viktigt för myndigheter och andra aktörer som behöver kartlägga översvämmade områden för att uppskatta potentiella skador och efterverkningar. Forskning som till exempel Cirneanu

och Popescu (2019) och Ichim och Popescu (2019) visar att bildanalys med neuronnät (t.ex. faltningsnät) och Gabor-filtrering kan förse beslutsfattare med korrekta klassificeringar av översvämmade områden på kort tid och därmed utgöra ett värdefullt beslutsstöd vid dessa samhällsstörningar.

3.2.3 Jordskredsdetektering

Ytterligare ett detekteringsområde där objektigenkänningsteknik applicerats är kartläggning, inventering och riskbedömning av förskjutning av jord, stenar och spillror. Tekniken går ut på geospatial bildanalys av flygbilder för att identifiera och klassificera olika typer av jordskred eller för att prediktera jordskred i områden där de kan leda till skada, exempelvis på liv och egendom (Ghorbanzadeh m.fl., 2019; Thai Pham m.fl., 2019). Tekniken bygger i stort på tillämpning av olika maskininlärningsmetoder och neuronnät. Forskningen antyder att försök med dessa modeller har varit lyckade, men att modellerna måste provas på global skala för att valideras (Ghorbanzadeh m.fl., 2019; Thai Pham m.fl., 2019).

3.2.4 Objektdetektering och bedömning av skador

AI-modeller kan tränas till att i realtid detektera en mängd olika objekt vilket kan förse räddningspersonal med en förbättrad lägesbild (Pi, Nath & Behzadan, 2020). Det finns möjlighet att detektera exempelvis fordon (Kyrkou m.fl, 2018) och att dessutom räkna dem (Li m.fl., 2019). Bedömning av skadeplats kan också göras, exempelvis detektering av antal skadade och oskadade byggnadstak, välta träd och spillror (Pi m.fl., 2020) liksom bedömning av infrastruktur såsom sprickor på broar eller asfalterade vägar (Wu m.fl., 2018). Med hjälp av AI kan system även känna igen flera olika typer av objekt i en och samma bild (Radovic, Adarkwa & Wang, 2017).

3.2.5 Människodetektering

Att snabbt kunna upptäcka människor i fara kan vara livsavgörande (Lygouras m.fl, 2019). Detektering via ett obemannat luftfartyg kan dessutom vara användbart för att bedöma vilka resurser som ska tas med vid en räddningsaktion (Apvrille m.fl., 2014). Med hjälp av datorseende och djupinlärningsmetoder kan människor detekteras i olika situationer, exempelvis i olika kroppspositioner och bilder tagna ovanifrån (Miyazato, Uehara & Nagayama, 2019) samt människor som befinner sig i vatten (Lygouras m.fl, 2019). Med hjälp av AI är det även möjligt att estimera i vilken riktning och med vilken fart en person rör sig (Apvrille m.fl., 2014).

3.2.6 Detektering av livstecken

Undersökning av människor på en olycksplats kan försvåras på grund av bland annat instabila ytor och svår terräng, vilket i sin tur kan utgöra en fara för räddningspersonalen (Al-Naji, Perera, Mohammed & Chahl, 2019). Via ett obemannat luftfartyg som detekterar livstecken genom att analysera kroppsrörelser orsakade av andning är det möjligt att på avstånd avgöra om en person är vid liv eller

ej (Al-Naji m.fl., 2019). Tester har även gjorts med användning av förstoring och förstärkning av video för att upptäcka små rörelser orsakade av andning, men som är osynliga för blotta ögat (Ordóñez, Cabo, Menéndez & Bello, 2018).

3.2.7 Akustisk detektering

Detektering med kameror har en del begränsningar då de inte fungerar lika bra i mörker eller om objektet döljs av något (Sibanyoni, Ramotsoela, Silva & Hancke, 2018). Därför har det genomförts studier kring användandet av ljud från källan för att lokalisera denna. Sibanyoni m.fl. (2018) genomförde en studie där de placerade mikrofoner på undersidan av ett obemannat luftfartyg och utvecklade en algoritm för lokalisering av ljud från visselpipor. Salvati, Drioli, Ferrin och Foresti (2019) gjorde en liknande studie, men de utförde testerna på tre olika ljudkällor: vitt gaussiskt brus, en skrikande röst och ett visslande ljud. Författarna nämner dock att ljud från vind och luftfartygets propellrar och motor kan störa ljudet som ska detekteras. De testade därför att placera mikrofonerna på avstånd, under luftfartyget.

3.2.8 Kommunikationsnätverk

Samhällsstörningar kan slå ut viktiga kommunikationsnätverk som är av extra betydelse för människor i behov av undsättning och för sök- och räddningsteam. Vid sådana tillfällen kan det vara viktigt att snabbt kunna sätta upp ett provisoriskt kommunikationsnätverk. de Paula Parisotto m.fl. (2019) skriver att en möjlig lösning för mobila och flexibla nödkommunikationsnät är utplacering av obemannade luftfartyg utrustade med basstationer, som sänder och tar emot radiovågor, för att skapa tillfälliga täckningsområden, så kallade celler. Förstärkningsinlärning har sedan använts för att skapa en snabb autonom och optimerad utplacering av flera luftfartyg för att uppnå bästa sändningseffekt och maximera antalet användare som kan nå ett kommunikationsnätverk (de Paula Parisotto m.fl., 2019).

3.3 Sårbarheter inom obemannade luftfartyg och angreppsvektorer med AI

Det finns en farhåga bland forskare att AI kommer att förstärka vissa hotaktörers förmåga att genomföra digitala, fysiska och politiska angrepp mot samhället (Brundage m.fl., 2018; Horowitz m.fl., 2018; Scharre & Horowitz, 2018). Brundage m.fl. (2018) beskriver hur digitala angrepp kan ske genom cyberattacker eller genom att utnyttja sårbarheter hos AI-system som gör att de inte fungerar som avsett. Angrepp kan ske genom att till exempel ta över obemannade luftfartyg och krascha dem mot ett mål. Vidare kan angrepp på politisk nivå ske genom till exempel övervakning, riktad propaganda och vilseledning. Den effektiva automationen med AI av uppgifter som tidigare ansetts kräva mänsklig intelligens gör bland annat att fler aktörer har möjlighet att genomföra dessa typer av angrepp och att angreppen kan ske snabbare samt mot fler mål.

Digitala angrepp med cyberattacker kan riktas mot informationens tillgänglighet, integritet eller sekretess. För obemannade luftfartyg kan det handla om att angriparen till exempel slår ut eller förvanskar delar av sensorinformationen eller GPS-positionen i navigeringssystemet (Benkraouda, Barka & Shuaib, 2018). Sådana angrepp kan försvåra eller till och med förhindra effektiv och säker användning av obemannade luftfartyg. Eftersom obemannade luftfartyg består av många delar som kommunicerar via datalänkar kan attacker genomföras på flera olika sätt. Attacker kan dels genomföras mot de markstationer som används för att styra och kommunicera med obemannade luftfartyg och dels mot själva luftfartygen. Det senare kan ske dels i samband med systemunderhåll och informationsöverföring när digitala lagringsmedier eller datornätverk ansluts till obemannade luftfartyg. Angreppen kan till viss del försvåras genom att inte ansluta obemannade luftfartyg till datornätverk, men angriparen kan fortfarande utnyttja sårbarheter hos USB-minnen och andra lagringsmedier för att genomföra cyberattacken.

3.3.1 Sårbarheter inom obemannade luftfartyg

För civil användning av obemannade luftfartyg är datalänkarna särskilt sårbara eftersom de ofta använder okrypterade och icke-autentiserad överföring av GPS-information och transponderdata med positionsinformation (Manesh & Kaabouch, 2019). Manesh och Kaabouch (2019) beskriver tre kategorier av cyberattacker mot datalänkar hos obemannade luftfartyg: dataintrång för att komma över information, datamanipulation som förvanskar information samt störning så att information blir otillgänglig. Ett exempel på datamanipulation är när angriparen förvanskar GPS-informationen så att det obemannade luftfartyget tror att den är på en annan plats och på så sätt påverkar styrningen när systemet kompenserar för den felaktiga positionsinformationen. Ytterligare exempel på datamanipulation är förvanskning av transponderdata med falsk eller felaktig positionsinformation, vilket gör att piloter och flygtrafikledare inte längre får en korrekt lägesbild. Genom att förvanska transponderdata kan angriparen även få automatiska system som ska undvika kollisioner att generera flygbanor som resulterar i kollisioner (Behzadan, 2017). De vanligaste angreppen mot obemannade luftfartyg har hittills varit förvanskning och störning av GPS-positioner (Krishna & Murphy, 2017). Rani, Modares, Sriram, Mikulski och Lewis (2016) beskriver även hur angriparen kan ta över styrningen av ett kommersiell obemannat luftfartyg genom att avlyssna datatrafiken och skicka egna kommandon till styrsystemet.

3.3.2 Cyberattacker med AI

Cyberattacker mot markstationer och obemannade luftfartyg har överlag stora likheter med angrepp mot andra IT-system. Först kartläggs organisationen och systemet som ska angripas. Förståelse av organisationen ger en uppfattning om förväntade mjukvaror, hur många som sköter IT-systemen och säkerhetsnivån (Stanard m.fl., 2004). Därefter skapas en angreppsgraf som beskriver möjliga angreppsvektorer för att utnyttja förväntade sårbarheter och samtidigt minimera risken för upptäckt. Angreppet genomförs sedan delvis eller helt automatiskt med hjälp av befintliga och specialutformade verktyg för cyberattacker.

Med AI blir det enklare för angripare att genomföra kartläggningen inför angreppet, planera angreppet med en attackgraf och att utföra angreppet med effektiva verktyg. AI-verktyg utvecklas till exempel för journalister för att sammanställa stora informationsflöden (Günther & Quandt, 2016), inom medicin för att sammanställa resultat från vetenskapliga publikationer (Moreno & Redondo, 2016), inom juridik för att identifiera trender och prejudikat från tidigare rättsfall (Moreno & Redondo, 2016) samt för att sammanställa information på sociala medier (Dehghani m.fl., 2017). Angripare kan använda liknande AI-verktyg för sin kartläggning av angreppsmål (Zouave m.fl., 2020).

Kartläggningen av angreppsmålet används för att skapa en angreppsgraf som beskriver alla de steg som måste utföras för att lyckas med angreppet (Falco, Viswanathan, Caldera & Shrobe, 2018). Eftersom planering är ett klassiskt AI-område finns flera exempel på automatisk generering av angreppsgrafer. Falco m.fl. (2018) kombinerar planeringsmetoden från Shrobe (2002) med klassificering av när, var och hur möjliga attacker kan genomföras enligt etablerade beskrivningar av cyberhot. Den automatiska genereringen av angreppsgrafer användes för att beskriva möjliga angrepp mot ett system för övervakningskameror. Den automatiska genereringen av angreppsgrafen minskade planeringstiden från en timme med manuell planering till minuter. Den genererade angreppsgrafen var även mer detaljerad och fullständig samt använde fler standardiserade begrepp.

Vidare finns det en farhåga att AI gör själva cyberattacken mer effektiv. Precis som försvarare av IT-system använder AI för att upptäcka sårbarheter och angreppsvektorer, så kan angripare använda samma verktyg för cyberattacker. Två exempel på sådana verktyg där AI används är automatisk skanning av program för att upptäcka sårbarheter, och penetrationstester som simulerar hela angrepp där flera sårbarheter kombineras för att uppnå målet med cyberattacken. Xue, Sun, Venkataramani och Lan (2019) beskriver en litteraturöversikt där maskininlärning används för analys av program. Fördelarna med maskininlärning är att inlärningen av informativa särdrag sker automatiskt och att det går snabbt att analysera stora program. Några av de sårbarheter som kan upptäckas är överskridande av allokerade minnesbuffrar (eng. buffer overflow) och minnespekare som inte är initialiserade (eng. null pointer dereference). Angripare kan utnyttja dessa sårbarheter för att exekvera valfri programkod och få tillgång till säkerhetsskyddsklassificerade uppgifter.

För penetrationstestning kan samspelet mellan försvarare och angripare på en abstrakt nivå ses som ett spel där varje aktör kan utföra ett antal åtgärder och resultatet är att cyberattacken lyckas eller misslyckas. Denna typ av spel kan modelleras med förstärkningsinlärning och flera försök görs för att tillämpa den tekniken för penetrationstester. Exempelvis Niculae, Dichiu, Yang och Bäck (2020) simulerar en nätverksmiljö där angripare, användare och försvarare representeras med agenter som kan utföra olika åtgärder beroende på nätverkets tillstånd. Resultaten visar att algoritmen, som representerar värderingen av lämpliga åtgärder med en tabell, presterar bättre än algoritmen som använder ett neuronnät. Schwartz (2018) fann däremot ingen skillnad mellan dessa algoritmer. Niculae m.fl. (2020) beskriver även att AI-algoritmerna är betydligt bättre än tidigare försök att automatisera penetrationstestning med

mer förutbestämda strategier. Vidare behöver inte de komplexa beräkningar som används för förstärkningsinlärning begränsa tillämpningen till små labbnätverk. Exempelvis beskriver Ghanem och Chen (2020) hur penetrationstestning med förstärkningsinlärning för medelstora nätverk kan upptäcka komplexa och ej uppenbara angreppsvektorer.

3.3.3 Sårbarheter och säkerhet för AI

Liu m.fl. (2018) beskriver hur hot mot säkerheten för AI-system kan riktas mot att ändra eller påverka systemets parametrar, skapa störningar som försämrar AI-systemets prestation och använda det på ett sätt som ger tillgång till säkerhetsskyddsklassificerade uppgifter. Attacker kan både göras mot systemets prestation överlag och mot dess prestation för specifika fall. Hur attackerna genomförs beror på angriparens mål, kunskaper om AI-systemet, förmåga att påverka AI-systemet samt valet av strategi.

Ett sätt att påverka systemets parametrar är att manipulera de träningsdata som används för maskininlärning. Många AI-system använder offentliga databaser som träningsdata eller anpassar befintliga AI-system som använder dessa databaser. Genom att ändra, ta bort eller lägga till träningsdata i databaserna kan en angripare påverka systemets prestation. Yang, Wu, Li och Chen (2017) beskriver till exempel hur förstärkningsinlärning kan används för att generera träningsdata som försämrar systemets prestation. Befintliga AI-system kan dessutom ha bakdörrar som angriparen kan utnyttja. Gu, Dolan-Gavitt och Garg (2017) beskriver till exempel hur ett AI-system kan tränas att felaktigt klassificera vägmärken genom att enbart sätta på en liten klisterlapp.

Liu m.fl. (2018) beskriver även hur attacker kan riktas mot befintliga AI-system med störning av indata som försämrar systemets prestation. Till exempel så att mål inte upptäcks vid klassificering eller att systemet förväxlar olika mål. Störningen kan skapas i form av ett subtilt brus som är omöjligt att upptäcka med blotta ögat när det överlagras på en bild (Goodfellow, Shlens & Szegedy, 2014; Svenmarck m.fl., 2018). En annan metod är att lägga till utvalda särdrag när bilden tas för att försämra systemets prestation. Sharif, Bhagavatula, Bauer och Reiter (2016) beskriver till exempel hur ett system för ansiktsigenkänning felaktig känner igen en person med specialutformade glasögon som en annan valfri person. En begränsning för många av dessa attacker är att de förutsätter kunskaper om AI-systemets parametrar. Dessvärre kan det även räcka med att mäta systemets beteende för ett begränsat antal fall för att få tillräcklig information för att skapa störningar som försämrar systemets prestation (Papernot m.fl., 2017).

Slutligen beskriver Liu m.fl. (2018) hur attacker kan riktas mot att använda AI-system på ett sätt som ger tillgång till säkerhetsskyddsklassificerade uppgifter som till exempel medicinsk information om patienter, enkätundersökningar och personers ansikten. Fredrikson, Jha och Ristenpart (2015) beskriver till exempel hur en persons namn och hur säker ett system för ansiktsigenkänning är på svaret kan användas för att delvis återskapa personens ansikte. Vidare beskriver Shokri, Stronati, Song och Shmatikov (2017) en attack som anger om ett visst fall ingick i AI-systemets träningsdata. Angriparen kan på så sätt få tillgång till säkerhetsskyddsklassificerade uppgifter som användes i träningsdata.

4. Diskussion

Litteraturöversikten visar att AI-tillämpningar för obemannade luftfartyg på flera sätt kan bidra till förmågor som används vid samhällsstörningar. Exempelvis kan AI stödja navigering i delvis okända miljöer samt stödja hinderdetektering, vilket kan öka förmågan att genomföra uppdrag i svåra och delvis okända miljöer. Eftersom bra neuronnät är beräkningstunga handlar en stor del av forskningen om att utveckla mindre beräkningstunga neuronnät samt att utveckla energieffektiv hårdvara för AI-beräkningar. Detta är en förutsättning för möjligheten att genomföra AI-beräkningarna ombord på obemannade luftfartyg där last och batteritid ofta är begränsade. Beräkningsavlastning på mer kraftfulla servrar är också en möjlighet, men det gör att de datalänkar som används för att kommunicera med obemannade luftfartyg blir mer sårbara för angrepp och andra typer av störningar.

AI kan användas för att öka förmåga att detektera. Exempelvis så kan bildupplösningen ökas för att underlätta detektering av små objekt på långa avstånd och reducera brus som försvårar detektering. AI kan även användas för att omvandla IR-bilder, som kan vara svåra att tolka utan specialutbildning, till visuella bilder. Möjligheterna att förbättra bildanalyser har hittills bara delvis studerats för verksamhet vid samhällsstörningar. AI är även en förutsättning för att kunna använda svärmar av obemannade luftfartyg. Med svärmar av obemannade luftfartyg skulle det potentiellt vara möjligt att generera detaljerade översiktsbilder av stora områden utan att ytterligare belasta personal eller behöva fler piloter för fjärrstyrning av obemannade luftfartyg. Obemannade luftfartyg med AI kan också vara till hjälp för att detektera bränder och andra skadeförlopp där det är svårt att få en överblick samt för att detektera människor i nöd.

Den effektiva automationen av uppgifter som AI medger kan även användas av angripare för att attackera obemannade luftfartyg. Vissa sårbarheter uppstår genom de datalänkar som används för att kommunicera med luftfartyget, där datalänkarna dessutom ofta är okrypterade och icke-autentiserade. Angrepp mot dessa datalänkar kan göras för att komma över information, manipulera information eller störa tillgången till information. Angripare kan på så sätt påverka styrningen av obemannade luftfartyg, vilket kan orsaka stora skador. Angripare kan även använda AI för att attackera markstationen för obemannade luftfartyg med bättre angreppsgrafer samt för att genomföra mer effektiva attacker med automatisk upptäckt av sårbarheter och angreppsstrategier. Vidare har AI-tekniker i sig sårbarheter som angriparen kan utnyttja genom att till exempel manipulera träningsdata eller generera störningar som är omöjliga att upptäcka med blotta ögat, men som försämrar systemets prestation.

Gemensamt är att många AI-tekniker i litteraturen visar på vad som är möjligt. Däremot behöver teknikerna fortfarande förbättras för att uppnå ökad tillförlitlighet. Exempelvis, för hinderdetektering på kortare avstånd och i högre hastighet, detektering på större avstånd, detektering av flera typer av ljud samt detektering av människor i flera positioner och vinklar. Flera av möjligheterna med AI skulle dessutom behöva testas i realistiska scenarion utanför en labbmiljö. Vidare är ökad tillförlitlighet i sig inte tillräckligt utan det finns även annat att ta hänsyn till. Exempelvis, hur AI ska inkorporeras i verksamheten och vilken information som kan användas för vilka beslut. Kan ett system som med hjälp av AI anser att en människa inte visar livstecken vara beslutsgrundande för prioriteringar vid en räddningsinsats?

5. Rekommendationer

Denna rapport presenterar en litteraturöversikt av möjligheter och utmaningar som förknippas med användningen av AI för obemannade luftfartyg för verksamhet vid samhällsstörningar. Litteraturöversikten baseras på internationell forskning och tydliggör förmågor i verksamheten som kan stärkas samt bli utsatta för angrepp med AI. Följande rekommendationer är avsedda att stärka möjligheterna och omsätta kunskapen i litteraturöversikt inom svensk verksamhet vid samhällsstörningar.

Rekommendation 1. Utred potentiell inverkan av AI för obemannade luftfartyg på svensk operativ förmåga.

Denna rapport presenterar ett antal konkreta användningsområden och förmågor som stöds eller möjliggörs av AI. Samtliga användningsområden är generellt sett relevanta för verksamhet vid samhällsstörningar. Ytterligare utredning bör fastställa eventuella prioriteringar av AI-stödda förmågor utifrån svenska operativa behov. Exempelvis kan vissa typer av detekteringsförmågor vara mer betydelsefulla för svenska behov än andra detekteringsförmågor.

Rekommendation 2. Utred organisatorisk beredskap och kompetensbehov om AI för obemannade luftfartyg.

Litteraturöversikten påvisar en bred och varierad forskning om AI för obemannade luftfartyg vid samhällsstörningar. Omfattningen på tillämpningarna tyder på att AI kommer att användas alltmer för verksamhet vid samhällsstörningar. För att öka den svenska beredskapen inför en sådan utveckling bör ytterligare utredningar genomföras om samordningen mellan svensk teknisk forskning, industri och räddningstjänst samt upphandling, personalförsörjning, kompetensförsörjning, rättsliga och organisatoriska förutsättningar för AI-användning.

Rekommendation 3. Utred nödvändiga åtgärder mot sårbarheter som kan exploateras med AI.

Litteraturöversikten beskriver ett antal AI-stödda hot mot obemannade luftfartyg för verksamhet vid samhällsstörningar. Angrepp mot obemannade luftfartyg kan dels ske direkt mot luftfartygen och dels mot markstationer och datalänkar. AI kan göra dessa angrepp snabbare och effektivare. AI-tekniker har även i sig sårbarheter som angripare kan utnyttja för att försämra systemens prestation. Det finns ett fortsatt behov av att utreda vilka strategier och åtgärder som kommer att vara effektiva för att skydda, hantera, minimera och bekämpa sådana hot mot verksamheten.

Rekommendation 4. Utred problemet med databrist inom AI för obemannade luftfartyg.

Djupinlärning förutsätter ofta stora datamängder för att träna, testa och validera neuronnät. Eftersom många tillämpningar enbart har tillgång till begränsade datamängder behöver särskilda tekniker användas för att djupinlärning ska vara möjligt. Svenmarck m.fl. (2018) beskriver tre möjliga tekniker: återanvända och träna om befintliga neuronnät på nya indata, använda generative adversarial networks (GAN) eller modellering och simulering för att skapa syntetiska indata. Eventuella problem med databrist för verksamhet vid samhällsstörningar behöver utredas.

Rekommendation 5. Utred behovet av transparens inom AI för obemannade luftfartyg.

Djupa neuronnät kan innehålla miljontals parametrar och det är svårt att veta exakt vilka särdrag som detekteras och hur de används för att beräkna svar. Transparens för djupa neuronnät är därför ett aktivt område för att skapa förtroende för att AI-systemet beter sig som förväntat (t.ex. Luotsinen, Oskarsson, Svenmarck & Wickenberg Bolin, 2019). Behovet av transparens för verksamhet mot samhällsstörningar behöver utredas.

6. Slutsatser

Litteraturöversikten visar att AI-tillämpningar för obemannade luftfartyg på flera sätt kan bidra till förmågor som används vid samhällsstörningar. För luftfartygens tekniska funktioner kan AI stödja navigering, beräkningseffektivitet, bildbehandling och koordinering av flera luftfartyg. För specifika fall av samhällsstörningar kan AI stödja detektion av bränder, översvämningar, jordskred, skador, människor, livstecken och ljud samt skapa provisoriska kommunikationsnätverk. Litteraturöversikten visar även att tillämpning av AI kan medföra nya digitala sårbarheter, potentiellt även i obemannade luftfartyg vid samhällsstörningar. Sårbarheterna innebär att luftfartygens navigering, automatiserade beslut och analyser kan störas eller förvanskas. Angripare kan även använda AI för att utföra cyberattacker mot obemannade luftfartyg. För att omsätta kunskapen i litteraturöversikten inom svensk verksamhet vid samhällsstörningar behövs utredningar av operativa behov, svensk beredskap inom AI, åtgärder mot AI-sårbarheter, eventuella problem med databrist samt behovet av transparent AI.

7. Referenser

Akhloufi, M. A., Castro, N. A. & Couturier, A. (2018). UAVs for wildland fires. I *Autonomous Systems:* Sensors, Vehicles, Security, and the Internet of Everything (Vol. 10643, s. 106430M). International Society for Optics and Photonics.

Al-Naji, A., Perera, A. G., Mohammed, S. L. & Chahl, J. (2019). Life signs detector using a drone in disaster zones. *Remote Sensing*, *11*(20), 2441.

Altawy, R. & Youssef, A. M. (2016). Security, privacy, and safety aspects of civilian drones: A survey. *ACM Transactions on Cyber-Physical Systems*, *1*(2), 1-25.

Apvrille, L., Tanzi, T. & Dugelay, J.-L. (2014). Autonomous drones for assisting rescue services within the context of natural disasters. I *2014 31th URSI General Assembly and Scientific Symposium (URSI GASS)* (s. 1-4).

Arola, S. & Akhloufi, M. A. (2019). Vision-based deep learning for UAVs collaboration. I *Unmanned Systems Technology XXI* (Vol. 11021, s. 1102108). International Society for Optics and Photonics.

Behzadan, V. (2017). Cyber-physical attacks on UAS networks-challenges and open research problems. *arXiv preprint arXiv:1702.01251*.

Benkraouda, H., Barka, E. & Shuaib, K. (2018). Cyber-attacks on the data communication of drones monitoring critical infrastructure. I N. Meghanathan & W. C. Wyld (Red.), *7th International Conference on Signal, Image Processing and Pattern Recognition (SPPR-2018)*, 22-23 december 2018, Sydney, Australia (s. 83-93). Tamil Nadu, India: AIRCC Publishing Corporation.

Bethel, C. L., Carruth, D. & Garrison, T. (2012). Discoveries from integrating robots into SWAT team training exercises. I *2012 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)* (s. 1-8). IEEE.

Brodeur, T., Regis, P., Feil-Seifer, D. & Sengupta, S. (2018). Search and rescue operations with mesh networked robots. I *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 6-12). IEEE.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., hÉigeartaigh, S. Ó., Beard, S., Belfield, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M., Bryson, J., Yampolskiy, R. & Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *arXiv preprint arXiv:1802.07228*.

Chen, Z., Zeng, Z., Shen, H., Zheng, X., Dai, P. & Ouyang, P. (2020). DN-GAN: Denoising generative adversarial networks for speckle noise reduction in optical coherence tomography images. *Biomedical Signal Processing and Control*, *55*, 101632.

Cirneanu, A. L. & Popescu, D. (2019). Flooded area detection by gabor filtering based on convolutional neural network. *University Politehnica of Bucharest Scientific Bulletin Series C-Electrical Engineering and Computer Science*, *81*(1), 69-80.

de Paula Parisotto, R., Klaine, P. V., Nadas, J. P., Souza, R. D., Brante, G. & Imran, M. A. (2019). Drone Base Station Positioning and Power Allocation using Reinforcement Learning. I *2019 16th International Symposium on Wireless Communication Systems (ISWCS)* (s. 213-217). IEEE.

Dehghani, M., Johnson, K. M., Garten, J., Boghrati, R., Hoover, J., Balasubramanian, V., Singh, A., Shankar, Y., Pulickal, L., Rajkumar, A. & Parmar, N. J. (2017). TACIT: An open-source text analysis, crawling, and interpretation tool. *Behavior Research Methods*, *49*(2), 538–547.

Devos, A., Ebeid, E. & Manoonpong, P. (2018). Development of autonomous drones for adaptive obstacle avoidance in real world environments. I *2018 21st Euromicro Conference on Digital System Design (DSD)* (s. 707-710). IEEE.

Di Felice, M., Trotta, A., Bedogni, L., Chowdhury, K. R. & Bononi, L. (2014). Self-organizing aerial mesh networks for emergency communication. I *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)* (s. 1631-1636). IEEE.

EDA (2020). *ESA and EDA joint research: advancing into the unknown*. Hämtad 10 mars 2020 från https://www.eda.europa.eu/info-hub/press-centre/latest-news/2020/01/09/esa-and-eda-joint-research-advancing-into-the-unknown

Falco, G., Viswanathan, A., Caldera, C. & Shrobe, H. (2018). A master attack methodology for an AI-based automated attack planner for smart cities. *IEEE Access*, *6*, 48360-48373.

Fraga-Lamas, P., Ramos, L., Mondéjar-Guerra, V. & Fernández-Caramés, T. M. (2019). A Review on IoT Deep Learning UAV Systems for Autonomous Obstacle Detection and Collision Avoidance. *Remote Sensing*, *11*(18), 2144.

Frankish, K. & Ramsey, W. M. (Red.). (2014). *The Cambridge handbook of artificial intelligence*. Cambridge University Press.

Fredrikson, M., Jha, S. & Ristenpart, T. (2015). Model inversion attacks that exploit confidence information and basic countermeasures. I *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (s. 1322-1333).

Ghanem, M. C. & Chen, T. M. (2020). Reinforcement Learning for Efficient Network Penetration Testing. *Information*, *11*(1), 6.

Ghorbanzadeh, O., Blaschke, T., Gholamnia, K., Meena, S. R., Tiede, D. & Aryal, J. (2019). Evaluation of different machine learning methods and deep-learning convolutional neural networks for landslide detection. *Remote Sensing*, *11*(2), 196.

Goodfellow, I. J., Shlens, J. & Szegedy, C. (2014). Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*.

Goodfellow, I., Bengio, Y. & Courville, A. (2016). *Deep learning*. MIT press.

Gu, T., Dolan-Gavitt, B. & Garg, S. (2017). Badnets: Identifying vulnerabilities in the machine learning model supply chain. *arXiv preprint arXiv:1708.06733*.

Günther, E. & Quandt, T. (2016). Word counts and topic models: Automated text analysis methods for digital journalism research. *Digital Journalism*, *4*(1), 75-88.

Hambling. D. (2016). *Gliding Algorithm Lets Drones Surf The Winds For Hours No fuel needed*. Hämtad 10 mars 2020 från https://www.popsci.com/new-software-lets-drones-surf-winds-for-hours

Haris, M., Watanabe, T., Fan, L., Widyanto, M. R. & Nobuhara, H. (2017). Superresolution for UAV images via adaptive multiple sparse representation and its application to 3-D reconstruction. *IEEE Transactions on Geoscience and Remote Sensing*, *55*(7), 4047-4058.

Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K. & Scharre, P. (2018). *Artificial intelligence and international security*. Washington: Center for a New American Security (CNAS).

Hossain, F. A., Zhang, Y. & Yuan, C. (2019). A Survey on Forest Fire Monitoring Using Unmanned Aerial Vehicles. I *2019 3rd International Symposium on Autonomous Systems (ISAS)* (s. 484-489). IEEE.

Hovelsrud Oddevald, L. & Falk, P (2015). *Egner droner seg som et operativt beslutningsstøtteverktøy i brann- og redningstjenesten? – Våre øyne i luften*. Haugesund: Høgskolen Stord/Haugesund.

Ichim, L. & Popescu, D. (2019). Flooded Areas Evaluation from Aerial Images Based on Convolutional Neural Network. I *IGARSS 2019-2019 IEEE International Geoscience and Remote Sensing Symposium* (s. 9756-9759). IEEE.

Imanberdiyev, N., Fu, C., Kayacan, E. & Chen, I. M. (2016). Autonomous navigation of UAV by using real-time model-based reinforcement learning. I *2016 14th International Conference on Control, Automation, Robotics and Vision (ICARCV)* (s. 1-6). IEEE.

Isola, P., Zhu, J. Y., Zhou, T. & Efros, A. A. (2017). Image-to-image translation with conditional adversarial networks. I *Proceedings of the IEEE conference on computer vision and pattern recognition* (s. 1125-1134).

Kejriwal M. & Zhou P. (2019). SAVIZ: Interactive Exploration and Visualization of Situation Labeling Classifiers over Crisis Social Media Data. I *International Conference on Advances in Social Networks Analysis and Mining, Vancouver (s.* 705-708).

Khalil, K. M., Abdel-Aziz, M., Nazmy, T. T. & Abdel-Badeeh M. S. (2008). The Role of Artificial Intelligence Technologies in Crisis Response. *arXiv preprint arXiv:0806.1280*.

Kouris, A., Venieris, S. I. & Bouganis, C. S. (2019). Towards Efficient On-Board Deployment of DNNs on Intelligent Autonomous Systems. I *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (s. 568-573). IEEE.

Krishna, C. L. & Murphy, R. R. (2017). A review on cybersecurity vulnerabilities for unmanned aerial vehicles. I *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)* (s. 194-199). IEEE.

Kyrkou, C., Plastiras, G., Theocharides, T., Venieris, S. I. & Bouganis, C. S. (2018). DroNet: Efficient convolutional neural network detector for real-time UAV applications. I *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (s. 967-972). IEEE.

Ledig, C., Theis, L., Huszár, F., Caballero, J., Cunningham, A., Acosta, A., ... & Shi, W. (2017). Photo-realistic single image super-resolution using a generative adversarial network. I *Proceedings of the IEEE conference on computer vision and pattern recognition* (s. 4681-4690).

Li, W., Li, H., Wu, Q., Chen, X. & Ngan, K. N. (2019). Simultaneously Detecting and Counting Dense Vehicles From Drone Images. *IEEE Transactions on Industrial Electronics*, *66*(12), 9651-9662.

Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S. & Leung, V. C. (2018). A survey on security threats and defensive techniques of machine learning: A data driven view. IEEE access, 6, 12103-12117.

Lomonaco, V., Trotta, A., Ziosi, M., Avila, J. D. D. Y. & Díaz-Rodríguez, N. (2018). Intelligent drone swarm for search and rescue operations at sea. *arXiv preprint arXiv:1811.05291*.

Luotsinen, L. J., Oskarsson, D., Svenmarck, P. & Wickenberg Bolin, U. (2019). *Explainable Artificial Intelligence: An Introduction to XAI techniques in Military Deep Learning Applications*. FOI-R--4849--SE. Stockholm: Totalförsvarets forskningsinstitut.

Lygouras, E., Santavas, N., Taitzoglou, A., Tarchanidis, K., Mitropoulos, A. & Gasteratos, A. (2019). Unsupervised Human Detection with an Embedded Vision System on a Fully Autonomous UAV for Search and Rescue Operations. *Sensors*, *19*(16), 3542.

Magoulianitis, V., Ataloglou, D., Dimou, A., Zarpalas, D. & Daras, P. (2019). Does Deep Super-Resolution Enhance UAV Detection?. I *2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)* (s. 1-6). IEEE.

Manesh, M. R. & Kaabouch, N. (2019). Cyber Attacks on Unmanned Aerial System Networks: Detection, Countermeasure, and Future Research Directions. *Computers & Security*, *85*, 386-401.

Mastroddi, F. (2014). *Robotics in Horizon 2020 IMPACT and Technology Readiness Levels*. Hämtad 10 mars 2020 från http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4027

Merino, L., Caballero, F., Martínez-De-Dios, J. R., Maza, I. & Ollero, A. (2012). An unmanned aircraft system for automatic forest fire monitoring and measurement. *Journal of Intelligent & Robotic Systems*, *65*(1-4), 533-548.

Miyazato, T., Uehara, W. & Nagayama, I. (2019). Development of a free viewpoint pedestrian recognition system using deep learning for multipurpose flying drone. *Electronics and Communications in Japan*, *102*(11), 16-24.

Moreno, A. & Redondo, T. (2016). Text analytics: the convergence of big data and artificial intelligence. *IJIMAI*, *3*(6), 57-64.

MSB (2018a) *Gemensamma grunder för samverkan och ledning vid samhällsstörningar*. MSB-777. Karlstad, Sverige: Myndigheten för samhällsskydd och beredskap.

MSB (2018b). *Obemannade luftfartyg i kommunal räddningstjänst: Vägledning 1.0*. MSB-1284. Karlstad, Sverige: Myndigheten för samhällsskydd och beredskap.

MSB (2019). *Faktablad: Gemensamma grunder för samverkan och ledning vid samhällsstörningar*. MSB-843. Karlstad, Sverige: Myndigheten för samhällsskydd och beredskap.

Näsström, F., Hagström, M., Mårtensson, T., Nilsson, P. & Woltjer, R. (2017). *RPAS inom ramen för förstärkningsresursen för stöd till samverkan och ledning*. FOR-R--4439--SE. Stockholm: Totalförsvarets forskningsinstitut.

Nationalencyklopedin (2020). *Artificiell intelligens*. Hämtad 10 mars 2020 från https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/artificiell-intelligens

Niculae, S., Dichiu, D., Yang, K. & Bäck, T. (2020). *Automating Penetration Testing using Reinforcement Learning*. Hämtad 10 mars 2020 från http://stefann.eu/files/Automating%20Penetration%20Testing%20using%20Reinforcement%20Learning.pdf

Nyberg, A., Eldesokey, A., Bergstrom, D. & Gustafsson, D. (2018). Unpaired Thermal to Visible Spectrum Transfer using Adversarial Training. I *Proceedings of the European Conference on Computer Vision (ECCV)* (s. 0-0).

Olofsson, A. (2017). *Drönare i räddningstjänst – Juridiska problemområden samt räddningstjänstens användning av drönare i Sverige*. Luleå tekniska universitet.

Ordóñez, C., Cabo, C., Menendez, A. & Bello, A. (2018). Detection of human vital signs in hazardous environments by means of video magnification. *PloS one*, *13*(4).

Ozdemir, U., Aktas, Y. O., Vuruskan, A., Dereli, Y., Tarhan, A. F., Demirbag, K., ... & Inalhan, G. (2014). Design of a commercial hybrid VTOL UAV system. *Journal of Intelligent & Robotic Systems*, *74*(1-2), 371-393.

Palossi, D., Conti, F. & Benini, L. (2019). An Open Source and Open Hardware Deep Learning-powered Visual Navigation Engine for Autonomous Nano-UAVs. I *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (s. 604-611). IEEE.

Panerati, J., Gianoli, L., Pinciroli, C., Shabah, A., Nicolescu, G. & Beltrame, G. (2018). From swarms to stars: Task coverage in robot swarms with connectivity constraints. I *2018 IEEE International Conference on Robotics and Automation (ICRA)* (s. 7674-7681). IEEE.

Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B. & Swami, A. (2017). Practical black-box attacks against machine learning. I *Proceedings of the 2017 ACM on Asia conference on computer and communications security* (s. 506-519).

Park, H., Kim, M. H., Chang, C. H., Kim, K., Kim, J. G. & Kim, D. H. (2007). Design and experimental validation of uav control system software based on the tmo structuring scheme. I *IFIP International Workshop on Software Technolgies for Embedded and Ubiquitous Systems* (s. 192-201). Berlin: Springer.

Pastor, E., Lopez, J. & Royo, P. (2006). A hardware/software architecture for UAV payload and mission control. I *2006 IEEE/AIAA 25TH Digital Avionics Systems Conference* (s. 1-8). IEEE.

Perera, P., Abavisani, M. & Patel, V. M. (2018). In2i: Unsupervised multi-image-to-image translation using generative adversarial networks. I *2018 24th International Conference on Pattern Recognition (ICPR)* (s. 140-146). IEEE.

Pham, H. X., La, H. M., Feil-Seifer, D. & Nguyen, L. V. (2018). Autonomous uav navigation using reinforcement learning. *arXiv preprint arXiv:1801.05086*.

Pi, Y., Nath, N. D. & Behzadan, A. H. (2020). Convolutional neural networks for object detection in aerial imagery for disaster response and recovery. *Advanced Engineering Informatics*, 43, 101009.

Qadir, J., Ali, A., ur Rasool, R., Zwitter, A., Sathiaseelan, A. & Crowcroft, J. (2016). Crisis analytics: big data-driven crisis response. *Journal of International Humanitarian Action*, *1*(1), 12.

Radovic, M., Adarkwa, O. & Wang, Q. (2017). Object recognition in aerial images using convolutional neural networks. *Journal of Imaging*, *3*(2), 21.

Rani, C., Modares, H., Sriram, R., Mikulski, D. & Lewis, F. L. (2016). Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal of Defense Modeling and Simulation*, *13*(3), 331-342.

Rantakokko, J., Strömbäck, P. & Marsten-Eklöf, F. (2016). *GNSS-fri navigering – Ett diskussionsunderlag*. FOI Memo 5958. Stockholm: Totalförsvarets forskningsinstitut.

Rifai, H., Marchand, N. & Poulin, G. (2008). Bounded control of a flapping wing micro drone in three dimensions. I *2008 IEEE International Conference on Robotics and Automation* (s. 164-169). IEEE.

Ruetten, L., Regis, P. A., Feil-Seifer, D. & Sengupta, S. (2020). Area-optimized UAV swarm network for search and rescue operations. I *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)* (s. 0613-0618). IEEE.

Russell, S. & Norvig, P. (2009). *Artificial Intelligence: A Modern Approach (3rd ed.)*. Upper Saddle River, NJ: Prentice Hall.

Rydell, J., Hultgren, K. & Strömbeck, P. (2017). *Bildbaserade navigeringstekniker – en omvärldsbevakning*. FOI-R--4445--SE. Stockholm: Totalförsvarets forskningsinstitut.

Salvati, D., Drioli, C., Ferrin, G. & Foresti, G. L. (2019). Acoustic Source Localization From Multirotor UAVs. *IEEE Transactions on Industrial Electronics* (s. 1-1).

Scharre, P. & Horowitz, M. (2018). *Artificial Intelligence What Every Policymaker Needs to Know*. Hämtad 10 mars 2020 från https://www.cnas.org/publications/reports/artificial-intelligence-what-every-policymaker-needs-to-know

Schwartz, J. (2018). *Autonomous Penetration Testing using Reinforcement Learning*. Bachelor Thesis. Brisbane, Australia: University of Queensland.

Sharif, M., Bhagavatula, S., Bauer, L. & Reiter, M. K. (2016). Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. I *Proceedings of the 2016 acm sigsac conference on computer and communications security* (s. 1528-1540).

Shokri, R., Stronati, M., Song, C. & Shmatikov, V. (2017). Membership inference attacks against machine learning models. I *2017 IEEE Symposium on Security and Privacy (SP)* (s. 3-18). IEEE.

Shrobe, H. (2002). Computational vulnerability analysis for information survivability. *AI Magazine*, *23*(4), 81.

Sibanyoni, S. V., Ramotsoela, D. T., Silva, B. J. & Hancke, G. P. (2018). A 2-D Acoustic Source Localization System for Drones in Search and Rescue Missions. *IEEE Sensors Journal*, *19*(1), 332-341.

Silver, D., Huang, A., Maddison, C. J., Guez, A., Sifre, L., Van Den Driessche, G., ... & Dieleman, S. (2016). Mastering the game of Go with deep neural networks and tree search. *Nature*, *529*(7587), 484.

Stanard, T., Lewis, W. R., Cox, D. A., Malek, D. A., Klein, J. & Matz, R. (2004). An exploratory qualitative study of computer network attacker cognition. *I Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 48, No. 3, s. 401–405). SAGE Publications.

Svenmarck, P. & Bengtsson, K. (2018). *Förmågor hos framtidens intelligenta enheter: Nya förutsättningar för ledning*. FOI-R--4665--SE. Stockholm: Totalförsvarets forskningsinstitut.

Svenmarck, P., Luotsinen, L., Nilsson, M. & Schubert, J. (2018). Possibilities and Challenges for Artificial Intelligence in Military Applications. I Proceedings of *NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting* (2018), Bordeaux, France.

Thai Pham, B., Shirzadi, A., Shahabi, H., Omidvar, E., Singh, S. K., Sahana, M., ... & Lee, S. (2019). Landslide susceptibility assessment by novel hybrid machine learning algorithms. *Sustainability*, *11*(16), 4386.

Thamm, H. P., Brieger, N., Neitzke, K. P., Meyer, M., Jansen, R. & Mönninghof, M. (2015). SONGBIRD-An innovative UAS combining the advantages of fixed wing and multi rotor UAS. *International Archives of the Photogrammetry, Remote Sensing & Spatial Information Sciences*, *40*.

Waharte, S., Trigoni, N. & Julier, S. (2009). Coordinated search with a swarm of UAVs. I *2009 6th IEEE annual communications society conference on sensor, mesh and ad hoc communications and networks workshops* (s. 1-3). IEEE.

WeRobotics. (2018). *Programs*. Hämtad 10 mars 2020 från https://werobotics.org/programs/

Wu, W., Qurishee, M. A., Owino, J., Fomunung, I., Onyango, M. & Atolagbe, B. (2018). Coupling deep learning and UAV for infrastructure condition assessment automation. I *2018 IEEE International Smart Cities Conference (ISC2)* (s. 1-7). IEEE.

Xu, J., Ota, K. & Dong, M. (2019). LUNA: Lightweight UAV Navigation Based on Airborne Vision for Disaster Management. I *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (s. 315-322). IEEE.

Xue, H., Sun, S., Venkataramani, G. & Lan, T. (2019). Machine learning-based analysis of program binaries: A comprehensive study. *IEEE Access*, *7*, 65889-65912.

Yang, C., Wu, Q., Li, H. & Chen, Y. (2017). Generative poisoning attack method against neural networks. *arXiv preprint arXiv:1703.01340*.

Zhao, Y., Ma, J., Li, X. & Zhang, J. (2018). Saliency detection and deep learning-based wildfire identification in UAV imagery. *Sensors*, *18*(3), 712.

Zouave, E., Bruce, M., Colde, K., Jaitner, M., Rodhe, I. & Gustafsson, T. (2020). *Artificially intelligent cyberattacks*. FOI Report. Stockholm: Totalförsvarets forskningsinstitut.

Zuhri, M. F. R., Zahari, A., Desia, R., Ismail, A. R. & Al Haek, M. (2015). The swarm-based exploration algorithm with expanded circle pattern for searching activities. *Jurnal Teknologi*, *77*(20), 61-65.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1577 - juni 2020 ISBN 978-91-7927-041-4