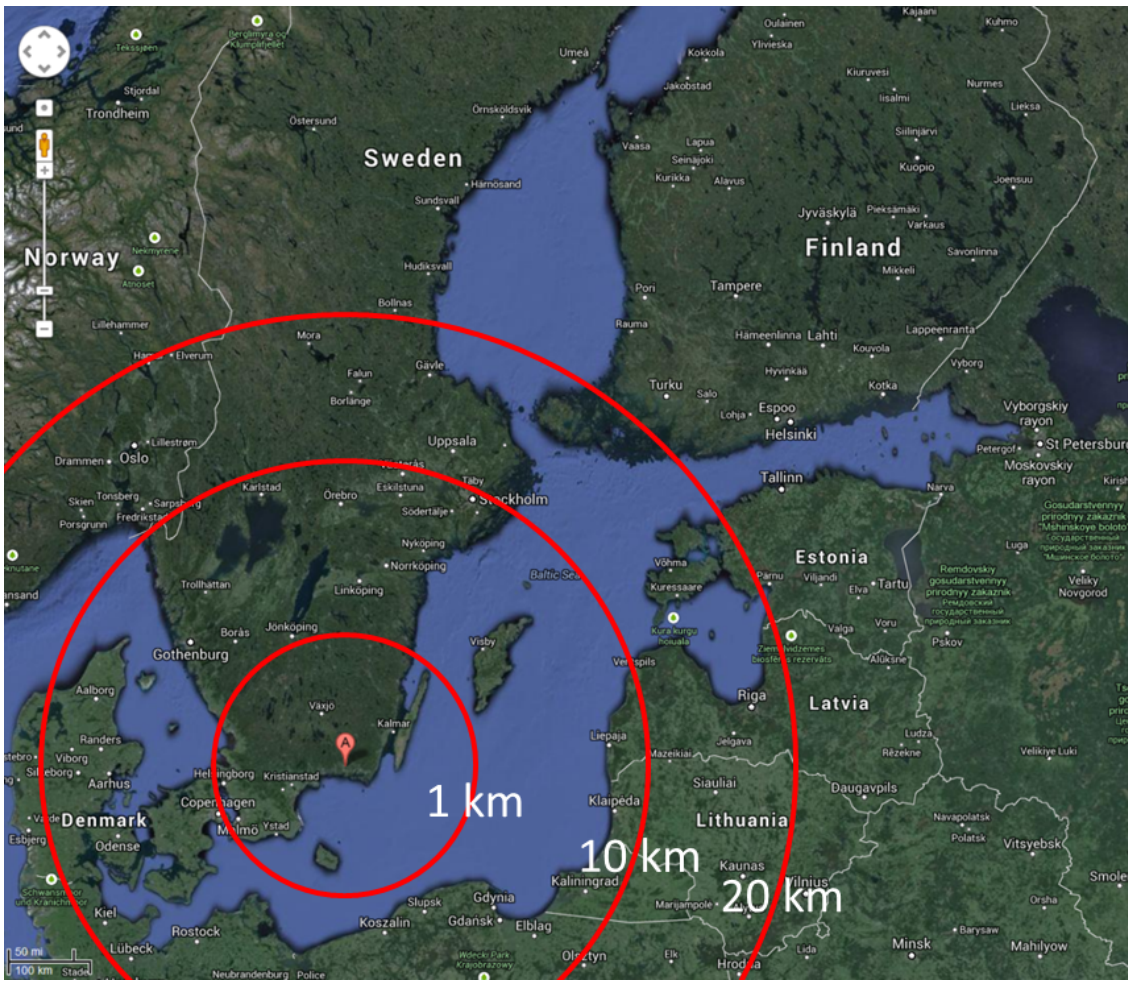
Robust kommunikation, cybersäkerhet och artificiell intelligens för säkerhet i RPAS

ERIK AXELL, MAGNUS JÄNDEL, DAVID LINDAHL,
SARA LINDER, IOANA RODHE OCH LARS WESTERDAHL



FOI-R--3825--SE
ISSN 1650-1942 December 2013

Erik Axell, Magnus Jändel, David Lindahl, Sara Linder, Ioana Rodhe och Lars Westerdahl

Robust kommunikation, cybersäkerhet och artificiell intelligens för säkerhet i RPAS

Titel	Robust kommunikation, cybersäkerhet och artificiell intelligens för säkerhet i RPAS
Title	Robust communication, cyber security and artificial intelligence for security in RPAS
Rapportnr/Report no	FOI-R—3825--SE
Månad/Month	December
Utgivningsår/Year	2013
Antal sidor/Pages	71 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Temaområde
Projektnr/Project no	E34517
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Informations- och areosystem

Sammanfattning

Denna rapport sammanfattar resultatet av det första årets arbete om informationssäkerhet i projektet *Obemannade farkoster och cyberhot* inom FoT temaområde *Autonoma farkoster för territorialövervakning*. Fokus är på fjärrstyrda farkoster för territorialövervakning i ett tjugoårsperspektiv.

Vi analyserar robust kommunikation för styrning, sensordata och trafikledning och kartlägger grundläggande förutsättningar för att upprätthålla samband. En översiktlig analys pekar på att det kan vara svårt att kontinuerligt fjärrstyra en farkost som utsätts för en kompetent telekrigsinsats långt ute i operationsområdet. Navigationsdata från satelliter är också mycket lätt att störa ut.

Cybersäkerhet analyseras med utgångspunkt från hur sårbarheter uppstår i ett livscykelperspektiv och vilka grundläggande förmågor som kan förväntas från olika typer av motståndare. Exempel på cyberangrepp mot obemannade farkoster analyseras och en grundläggande hotanalys genomförs.

Vi visar hur artificiell intelligens i systemet kan utnyttjas för att bygga robust säkerhet mot cyberangrepp. Speciellt studeras hur en autonom övervakare ombord på farkosten kan upptäcka angrepp på olika systemnivåer och ingripa i nödlägen då operatören inte kan kontrollera situationen.

Nyckelord: RPAS, Robust kommunikation, Cybersäkerhet, Autonomi.

Summary

This report summarizes the results of the first year's work on information security in the project *Unmanned vehicles and cyber threats* within the FoT thematic area *Autonomous vehicles for territorial surveillance*. We focus on remotely operated vehicles for territorial surveillance in a twenty-year perspective.

We analyze robust communication for control and sensor data as well as for flight management and map out basic communication requirements for remote piloting. A cursory analysis suggests that uninterrupted remote control may be difficult to achieve over the entire theater of operations if faced with competent adversarial electronic warfare measures. Navigation relying on data from satellites is also easily disrupted.

The cyber security analysis is grounded in understanding how vulnerabilities arise from a life cycle perspective and what capabilities that can be expected from different types of opponents. Examples of cyber-attacks on unmanned vehicles are analyzed and a fundamental threat analysis is carried out.

We show how autonomous artificial intelligence can be used for building robust multi-layered cyber security. Specifically, we study how an AI supervisor aboard the craft can detect attacks at different system levels and intervene in emergencies when the operator is unable to communicate or otherwise control the situation.

Keywords: RPAS, Robust communication, Cyber security, Autonomy.

Innehållsförteckning

1 Inledning

Denna rapport sammanfattar resultatet under 2014 av arbetet om informationssäkerhet i projektet *Obemannade farkoster och cyberhot* inom FoT temaområde *Autonoma farkoster för territorialövervakning*. Vi fokuserar på frågan hur sårbarheten för antagonistiska attacker i ett cyberhotperspektiv kan värderas och minimeras. Vi betraktar detta problem ur tre perspektiv,

1) Vilka är hoten mot kommunikationsvägarna till farkosten och hur kan kommunikationen göras så robust som möjligt?
2) Vad menas med cyberhot? Vilka är cyberhoten mot obemannade farkoster och hur kan hela systemet göras mer robust mot cyberhot?
3) Hur kan artificiell intelligens användas för att öka säkerheten mot cyberhot?

Vart och ett av dessa perspektiv motsvaras av ett eller flera kapitel i denna rapport.

Enligt anvisningarna för projektet *Autonoma farkoster för territorialövervakning* förutsätter vi att de obemannade farkosterna väsentligen är fjärrstyrda av operatörer, obeväpnade och används för spaning mot främmande missiler, flygplan, helikoptrar och fartyg. Eftersom tidsperspektivet är system som kan vara aktiva år 2030 bortser vi avsiktligt från den i och för sig fullt rimliga möjligheten att det år 2030 finns teknik som kan göra obemannade flygplan väsentligen autonoma. Här studerar vi bara delvis autonoma funktioner som syftar till att öka säkerheten i ett fjärrstyrt system. I enlighet med projektets gemensamma terminologi kallar vi den obemannade farkosten RPA (Remotely Piloted Aircraft). Hela systemet inklusive RPA, operatörer, operatörsstationer, etc. kallas i fortsättningen RPAS (Remotely Piloted Aircraft System).

De tre perspektiven presenteras i separata kapitel men är djupt relaterade. Eftersom RPA förutsätts vara fjärrstyrda och uppgiften är spaning är robust kommunikation en förutsättning för att systemet ska kunna lösa sina uppdrag. En motståndare kan förväntas försöka störa kommunikationskanaler med telekrig och använda kommunikationskanaler för cyberattacker. Fungerande kommunikation är också viktig för att proaktivt och reaktivt hantera cyberhot. För att förstå cyberhotets natur och designa metoder för att förebygga, hantera och kompensera för cyberhot är det viktigt att kartlägga kommunikationskanaler och ha detaljerad insikt i deras egenskaper. Artificiell intelligens ombord på farkosten kan bygga robust säkerhet mot cyberhot i flera lager genom att använda kunskaper om cyberhoten och kommunikationskanalerna till att skapa en lägesbild på olika systemnivåer och självständigt vidta säkerhetsåtgärder i

nödlägen då operatören inte är tillgänglig eller har kapacitet att hantera problemen.

2 Robust kommunikation

Kommunikationssystemet är en kritisk del för en obemannad farkost. Erfarenheter från användande av RPAS i USA visar att ungefär 14 % av alla felhändelser beror på kommunikationssystemet (US Department of Defence, 2005). Därför är det viktigt att kommunikationssystemet är robust. Kommunikationssystemet ska kunna hantera flera olika typer av trafik som går över olika kommunikationslänkar;

- Styrlänk för Command and Control (C2).
- Datalänk för att skicka över data från olika sensorer.
- En eller flera länkar för kommunikation med civil flygledning.

De olika kommunikationslänkarna kommer troligen att använda sig av olika frekvensband och olika radioapparater. En säkerhetsanalys för RPA radiokommunikationssystem finns i (Rudinskas et al., 2009). Olika aspekter av säkerhet behandlas så som tillförlitlighet hos radiokanalen och skydd av data. I artikeln påpekas bland annat att det är viktigt med en robust radiokanal i en RPA-tillämpning och författarna förespråkar att det finns flera radiosystem ombord som använder olika frekvenser.

Piloten som styr en RPA sitter i en markstation vilken kommunicerar med RPA:n. Även kommunikationslänken för sensordata går förmodligen mellan RPA och markstation. För att få flyga i kontrollerat luftrum krävs även kommunikation med civil flygledning. Trafiken från civil flygledning förväntas även inom överskådlig framtid skickas från flygledningen till RPA som sedan vidarebefordrar den till markstationen.

2.1 Styrlänk

En obemannad farkost kan fjärrstyras på olika sätt, antingen via detaljerade styrkommandon eller via genererade banor med brytpunkter. Även om graden av autonomitet hos framtida obemannade farkoster kan förväntas öka kommer styrlänken alltid att behövas. Behovet av att veta farkostens status, t.ex. position, bränslemängd, och kunna ge nya instruktioner, t.ex. nya mål eller sökområden kommer att kvarstå. Kommunikationslänken kan fallera av flera orsaker, exempelvis hårdvarufel, interferenser eller fientlig störning. Frågan är vad som ska hända om markstationen tappar kontakten med en RPA och inte längre kan styra den. I dagens RPA finns speciella procedurer som anropas i ett sådant fall, s.k. LLP (*Lost Link Procedure*). Ett vanligt förfarande är att farkosten flyger till en förutbestämd höjd och försöker återupprätta kommunikationslänken, men om det inte lyckas kan farkosten antingen följa samma bana tillbaka till basen, flyga

direkt tillbaka eller fortsätta med uppdragen (US Department of Defence, 2005). Vid en incident i Afghanistan 2009 förlorades kontakten med en MQ-9 Reaper. Kontrollen kunde inte återupprättas och eftersom MQ-9:an var på väg att lämna Afghanskt luftrum sköts den ner med hjälp av ett bemannat flygplan (Reichhardt, 2009).

2.2 Datalänk

Vid territorialbevakning är det troligt att stora mängder data ska föras över från ett RPAS till marken och att data ska kunna analyseras i realtid. Data kan vara från en mängd olika sensorer till exempel video, radarbilder eller IR. Eftersom mängden data som ska kunna föras över är stor är det lämpligt att komprimera data för att minska mängden som behöver skickas över kommunikationslänken. Nackdelar med komprimering är att det krävs databehandling och att det kan ge upphov till fördröjningar. Dessutom förloras delar av rådata vid användning av vissa komprimeringsmetoder. Ofta märks inte dessa förluster vid måttlig komprimering men kan bli besvärande vid kraftig komprimering. Ett vardagligt exempel är musikfiler komprimerade till mp3-format där effekterna av för kraftig komprimering kan höras. Det är därför viktigt att hitta en balans mellan prestandakrav på kommunikationslänken och krav på komprimering.

2.3 Civil flygledning

Traditionellt har flygledning skett via taltrafik och en del av trafiken förväntas även i framtiden ske via tal med stöttning av datatjänster (ITU, 2009). Taltrafiken sker mellan flygledningen och piloten som sitter i markstationen men skickas via RPA:n eftersom RPA:n, till skillnad från markstationen, befinner sig i närheten av flygledningen, i de flesta av dagens tillämpningar.

En ny tjänst för civil flygledning är på gång att införas, ADS-B (*Automatic dependent surveillance-broadcast*). I Europa kommer det år 2015 krävas att ADS-B transpondrar finns på alla nya flygplan. Säkerheten i ADS-B är mycket omdiskuterad och det finns flera exempel på attacker mot ADS-B som har genomförts i testmiljö (Strohmeier et al. 2013). För ADS-B transpondrar finns två konkurrerande standarder för datalänkenUAT (*Universal Access Transceiver*) och 1090ES (1090 MHz *Extended Squitter*). I (Strohmeier et al. 2013) beskrivs ett antal olika hot mot ADS-B som exempelvis avlyssning och falsksignalering såväl som några möjliga skyddstekniker som autentisering och bandspridning. Slutsatsen var att några tekniker kan införas i nuvarande system för att öka säkerheten, men för en allomfattande säkerhetslösning behövs nya meddelandetyper eller nya protokoll.

2.4 Telekonflikter

Vid integrering av många system på en liten plattform är risken för telekonflikter betydande. Med telekonflikter menas oavsiktliga störningar som stör radiomottagaren via antennen. Störningarna kan komma från andra nyttosändare, t.ex. radio- och TV-utsändningar eller från egna system. Mottagna kommunikationssignaler är ofta svaga relativt signaler från sändande system på plattformen, t.ex. radar. På grund av ofullkomligheter i hårdvaran kan system störa varandra trots separation i frekvens. Störningar kommer inte heller endast från sändande system utan all elektronik, t.ex. datorer, strålar ut elektromagnetisk energi som kan påverka mottagaren. För att minska risken för telekonflikter är det bra att separera antenner, vilket kan vara svårt på en liten plattform med få lämpliga antennplatser. En annan möjlighet är att separera sändande och mottagande system tidsmässigt och även frekvensmässigt. Problem med telekonflikter är relativt vanligt på flygande plattformar eftersom många sändande och mottagande system ska integreras i en liten plattform. Telekonflikter kan få mycket allvarliga konsekvenser och ett exempel på det är den Global Hawk-plattform vars självförstörelsemekanism utlöstes av en telekonflikt under en flygning, varpå plattformen förstördes (Lucchese et al. 2000).

2.5 Hotbild

De största hoten mot kommunikationslänkarna i ett RPAS är troligen signalspaning och störning. En intelligent telekrigsmotståndare strävar efter att genomföra effektiv störning på ett kontrollerat sätt, och bedriver därför signalspaning för att lokalisera sitt offer geografiskt, men även i tid och frekvens. Det vill säga, telekrigsmotståndaren försöker identifiera när och på vilka frekvenser ett RPAS kommunicerar, för att så effektivt som möjligt kunna störa kommunikationen. Det största störhotet är troligen att motståndaren sänder en störsignal som har ett effektövertag över nyttosignalen. Detta kan göra att kommunikationen inte fungerar alls. Det finns olika sätt att skydda sig mot en sådan störning , eller åtminstone minska effekten av den, som diskuteras vidare i kommande avsnitt. Ett kanske allvarligare hot än ren störning är risken för vilseledning av kommunikationssystemen. Ett system utan kryptering eller autentisering är speciellt sårbart mot vilseledning, eftersom en motståndare kan rekonstruera en autentisk signal som innehåller felaktig information. Kryptering kan skydda mot informationsspridning, men är även ett väsentligt skydd mot vissa typer av vilseledning. Kryptering skyddar dock överhuvudtaget inte mot störning. En RPA som befinner sig på hög höjd, och dessutom troligen nära motståndaren, är ett särskilt utsatt offer för signalspaning, störning och vilseledning. Tidigare har kommunikation med RPA:er ofta varit okrypterad

vilket har lett till ett antal incidenter. I Irak 2008 upptäcktes att videoströmmar från Predator-RPA hade kunnat avlyssnas under en längre tid med hjälp av en parabolantenn och ett enkelt datorprogram (Skygrabber) (Gorman et al. 2009). Iran hävdade 2011 att de med hjälp av störning och falsksignalering fått en RQ-170 att landa i Iran efter att den kränkt Iranskt luftrum (Petersen och Faramarzi, 2011). USA hävdar istället att RPA:n fått motorfel i Afghanskt luftrum och sedan störtat i Iran.

2.6 Metoder för förbättrat störskydd

För att bättre skydda sin kommunikation mot fientlig störning kan olika radiokommunikationstekniker användas.

2.6.1 Antenner

Någon typ av riktantenner är troligen nödvändig både för att få upp datatakten på kommunikationslänkarna och på grund av telekrigshotet, både mot kommunikationslänkar och mot satellitnavigeringssystem. Antingen kan en fysisk riktantenn, t.ex. en parabol, eller en elektriskt styrbar antenn användas. Vid användning av riktantenner vid sändning kan energin koncentreras i riktning mot mottagaren genom s.k. *lobformning*, och både öka signalstyrkan hos mottagaren och minska risken för upptäckt av en signalspanare. Vid störning kan störeffekten undertryckas i mottagarantennen om den inte kommer i samma riktning som nyttosignalen. Om en elektriskt styrbar antenn används kan nollställen läggas i riktning mot fientlig störning genom s.k. *nollstyrning* vilket avsevärt kan förbättra störtåligheten för kommunikationssystemet. Fler antennelement ger större möjligheter (fler frihetsgrader) att genomföra lobformning och nollstyrning i olika riktningar.

Att införa avancerade antennlösningar på en flygande farkost innebär dock alltid utmaningar då antennerna riskerar att påverka aerodynamiken hos farkosten samtidigt som de tar plats från annan utrustning. Då RPAn i det aktuella scenariet är relativt stor och främst avsedd för spaning bör dock problemen vara mindre jämfört med hos en stridande plattform där de aerodynamiska egenskaperna troligen har högre prioritet. Antenner kommer troligen inte att kunna monteras i efterhand, utan måste integreras i plattformen från början.

En möjlighet är att samutnyttja samma antenn för radar och kommunikation, en så kallad multifunktionsantenn. Detta kräver dock tidsdelning mellan de olika systemen vilket gör att förmågan hos de enskilda systemen reduceras. Detta måste dock vägas mot vinsten av en avsevärt mycket bättre antenn för kommunikation.

2.6.2 Bandspridning

Bandspridning innebär att ett större frekvensband används än vad som behövs för nyttosignalen och på så sätt kan ett bättre skydd mot fientlig störning erhållas. Bandspridningen kan antingen ske genom frekvenshopp då sändare och mottagare synkront byter frekvens som används på ett till synes slumpmässigt sätt eller via direktsekvensspridning då nyttosignalen sprids med en så kallad spridningskod och upptar en större bandbredd. Båda metoderna ger upphov till en så kallat *processvinst*, vilket är förhållandet mellan bandbredden efter och före bandspridning. Måttet beskriver även den fördel som kommunikationssystemet får gentemot en fientlig störare. Nackdelen med bandspridning är att den tar frekvensutrymme vilket kan vara ett problem eftersom spektrum är begränsat.

2.6.3 Felrättande kodning och omsändningar

Då meddelanden skickas mellan sändare och mottagare uppkommer ofta fel på grund av brus, fädning, interferenser med mera. För att kunna hantera de fel som uppkommer kan man antingen använda sig av felrättande kodning eller omsändningar (ARQ – *automatic repeat request*) eller en kombination, s.k. hybrid ARQ (HARQ). Vid felrättande kodning införs redundans i meddelandet vilket sedan används för att rätta eventuella fel som uppkommit. Ju mer redundans som används desto mer fel kan rättas, men andelen nyttobitar sjunker.

Vid omsändning ber mottagaren att sändaren ska skicka om de paket som det blivit fel i. Om det är många paket som det blir fel i så blir omsändning ineffektivt och omsändningar ger alltid upphov till fördröjningar.

För att kunna sända data mellan en markstation och en RPA behövs troligen inte så mycket felrättningsförmåga i normalfallet eftersom det troligen är fri sikt mellan sändare och mottagare. Behovet ökar då kommunikationssignalen är svag, t.ex. vid långa kommunikationsavstånd, eller om kommunikationen är utsatt för fientlig störning.

2.7 Militära standarder

Det finns idag ett antal standarder för både C2- och ISR-kommunikation, som används runtom i världen. De obemannade farkoster som är operativa i det svenska försvaret idag har analoga kommunikationslänkar som använder de fria s.k. ISM-banden (*industrial, scientific and medical*). Dessa kommunikationslänkar är helt oskyddade, och lätta att både störa och avlyssna. För små och medelstora RPA:er är analog FM den dominerande kommunikationsmetoden för C2 och ISR med en bandbredd runt 25 MHz i L-, C- eller S-band (1-8 GHz). De kortare kommunikationsavstånden medger att

enklare antennsystem kan användas, och den relativt låga frekvensen medger även att viss täckning bortom fri sikt (*line-of-sight*, LOS) är möjlig. Svårigheten är att få tillgång till frekvensspektrum i tillräcklig omfattning. Den amerikanska erfarenheten visar att det är svårt att operera med mer än 3-4 RPA:er i ett område p.g.a. att L-, C- och S-banden är väldigt hårt utnyttjade (Gardner, 2009). För större avstånd används satelliter som relästation, ibland för riktigt stora avstånd flera satelliter. För RPA:er med enkla sensorer kan även lägre frekvenser under 1 GHz utnyttjas. Nackdelen är att tillgänglig bandbredd ofta är starkt begränsad på dessa frekvensband.

För större RPA:er finns idag etablerade standarder och radiosystem som utgör datalänkar för C2 och ISR, t.ex. NATO-standarden STANAG 7085 (Ryan et al., 2002) och den amerikanska militära standarden *Common Data Link* (CDL) (Osterheld, 2007). Dessa länkar är digitala med bättre störskydd och trafikskydd. CDL och STANAG 7085 är så långt vi känner till *state-of-the-art* för C2- och ISR-kommunikation idag. STANAG 7085 är egentligen en implementation av CDL på X-band och Ku-band (NATOs I- och J-band, 8 - 20 GHz). CDL är punkt-till-punkt datalänkar för bemannade och obemannade plattformar med stöd för full duplex (Osterheld, 2007), och kräver *Line-of-Sight* (LOS) mellan alla relästationer eftersom bärfrekvensen ligger på höga frekvenser (8-20 GHz). Stora operationsområden medför att kommunikationsavstånden blir långa och därför är det i allmänhet nödvändigt med ett riktantennsystem som kan följa RPA:ns rörelser. CDL har dock även stöd för *Beyond LOS* (BLOS) kommunikation genom interoperabilitet mellan olika RPAS.

CDL är en asymmetrisk datalänk och erbjuder krypterad och störskyddad kommunikation (Osterheld, 2007). Kontrollänken till den luftburna plattformen, kallad *command link* (CL), har stöd för datatakter på 200~kb/s, 2.0~Mb/s och 10.71~Mb/s. I datalänken från farkosten till markstationen, kallad *return link* (RL), stöds datatakterna 10.71~Mb/s, 137.088~Mb/s och 274.176~Mb/s. Felrättande koder, t.ex. faltningskoder och Reed-Solomon-koder, i kombination med *interleaving* används för felrättning av data. I CDL används även direktsekvens bandspridning (DSSS) med en (*pseudo-random noise*) PRN-sekvens för störskydd. CDL kan konfigureras med olika val av t.ex. datatakt, bandspridning och operativ frekvens. CDL används bl.a. på de amerikanska RPA:erna Northrop Grumman RQ-4 Global Hawk och MQ-1 Predator (GlobalSecurity.org).

2.8 Frekvensspektrum

Internationella teleunionen (ITU) har genomfört en studie med syfte att undersöka behovet av frekvensspektrum för att obemannade farkoster ska kunna operera säkert i gemensamt luftrum med sikte på 2030 (ITU, 2009). För att

RPA:er ska kunna operera över långa avstånd krävs både markbunden och satellitkommunikation. I rapporten från studien analyseras endast kommunikation för att kunna operera en RPA på ett säkert sätt, till det kommer sedan ett behov av spektrum för att t.ex. kunna överföra spaningsdata. I analysen är således styrlänken och trafik till civil flygledning inkluderat.

För en RPA på medelhög eller hög höjd resulterar kraven i datatakter runt 5-7 kbit/s i upplänken och 17-21 kbit/s i nedlänken (ITU, 2009, Tabell 15 och 16), till det kommer 27-270 kbit/s video/väderradar i nedlänken. Kraven på video varierar mycket och de stora skillnaderna i datatakt beror på vilken uppdateringstakt som krävs. För en militär tillämpning med några få farkoster kommer troligen tillgång till spektrum för datalänken vara det stora problemet eftersom det förväntade kravet på den är mycket högre.

Att det finns standarder och radioapparater för kommunikation med en RPA betyder inte automatiskt att det finns färdiga system som går att använda överallt. Idag finns t.ex. inget tilldelat spektrum i Sverige för denna typ av kommunikation. De fria ISM-banden som används för de obemannade farkoster som är operativa i det svenska försvaret idag, kan vara problematiska att använda ur ett militärt perspektiv. Eftersom de är fria att använda för många andra tillämpningar (t.ex. WLAN, Bluetooth, mikrovågsugnar etc.) är det ofta redan en hög interferensnivå, vilket gör att ett systems förmåga att motstå annan störning eller vilseledning kan vara kraftigt degraderad p.g.a. de redan höga störningsnivåerna. Innan upphandling av ett nytt RPAS, och framförallt dess kommunikationslänkar, måste det alltså säkerställas att det finns tillgängligt spektrum som får användas i de regioner där systemet är tänkt att operera.

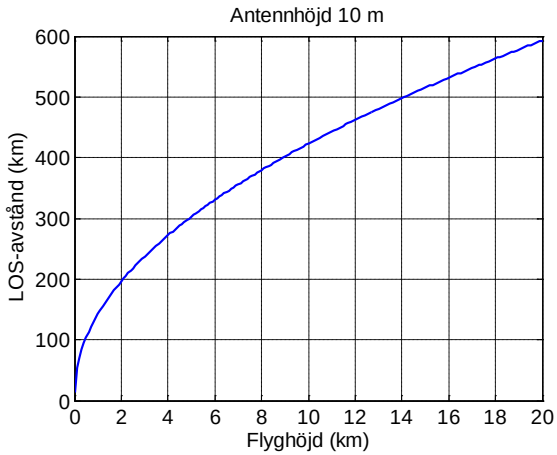
För att få tillgång till större bandbredder, som krävs för att överföra stora mängder sensordata i realtid, kan det vara nödvändigt att använda ganska höga frekvenser. En nackdel med frekvenser över 1 GHz är att de i princip endastmöjliggör kommunikation inom *line-of-sight* (LOS) för den här typen av kommunikationslänk. Räckvidden minskar ju högre frekvenser som utnyttjas och även påverkan från väder t.ex. regn och dimma kan bli ett problem för högre frekvenser.

2.9 Räckvidd för LOS

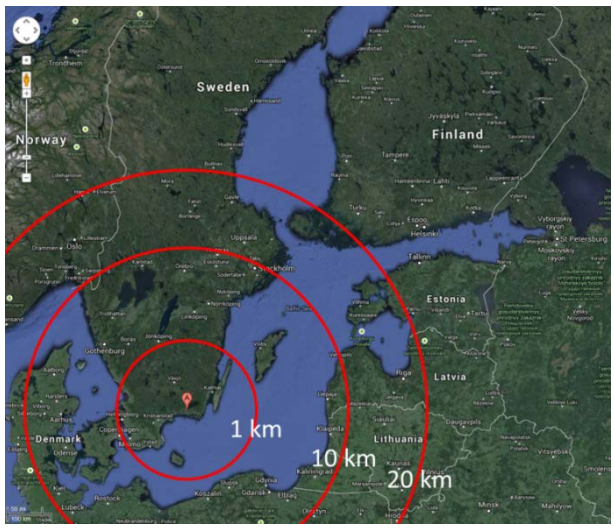
Räckvidden för en kommunikationslänk beror på många faktorer, t.ex. sändareffekt, frekvens och sändar- och mottagarantenner. Även om den mottagna effekten skulle vara tillräcklig på ett givet avstånd med fri sikt, så begränsas räckvidden för LOS av sändar- och mottagarantennernas höjder p.g.a. jordens krökning. En RPA som flyger högre har alltså längre räckvidd.

I figur 1 visas direktsiktsavståndet för olika flyghöjder för en RPA vid kommunikation med en 10 meter hög markantenn (Ahlin och Zander, 2000, ekv. (2.34). Avståndet kan för höga frekvenser ses som maximal räckvidd för ett kommunikationssystem över en jämn yta på jorden.

Enligt samma beräkningar visar figur 2 området där en markstation placerad i Ronneby har fri sikt till en RPA på 1 km, 10 km respektive 20 km flyghöjd, där direktsiktsavståndet är respektive ca 15, 40 och 60 mil.



Figur 1. Direktsiktsavståndet (Line-of-sight, LOS) för olika flyghöjder för en RPA.



Figur 2. LOS-avstånd för en RPA från Ronneby för 1 km, 10 km respektive 20 km flyghöjd.

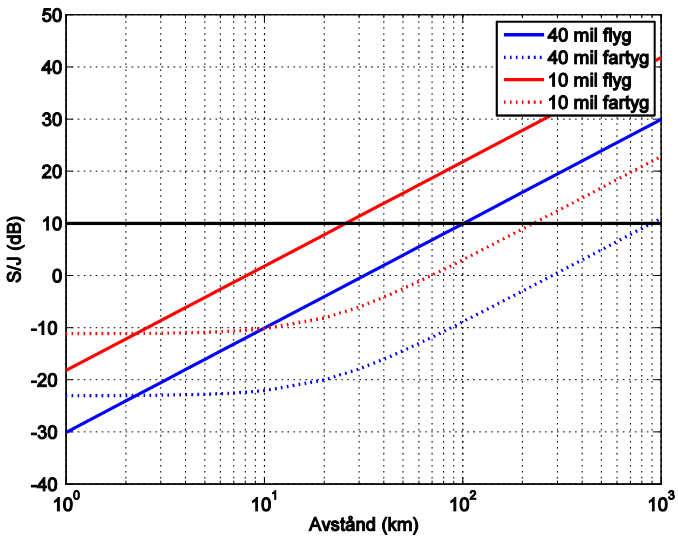
2.10 Störanalys

Ett hot mot RPAS är risken för telekrigsattacker. För att åskådliggöra möjliga risker med fientlig störning av RPAS har några scenarion analyserats. I scenariot har en RPA antagits befinna sig antingen 10 eller 40 mil från markstationen. Vidare antas att RPA:n flyger på 20 km höjd vilket är rimligt för en stor RPA. Markstationen sänder med 50 W uteffekt och har en stor styrbar parabolantenn med en antennvinst på 25 dBi.

Två olika typer av störare analyseras. En störare i ett flygplan som antas flyga på samma höjd som RPA:n med 100 W uteffekt och en rundstrålande antenn. Den andra störaren är på ett fartyg med 1 kW uteffekt och en antennvinst på 9 dBi.

Här antar vi att kommunikationssystemet behöver ett effektövertag på 10 dB för att fungera tillfredsställande.

I figur 3 visas förhållandet mellan nyttosignalens effekt och effekten från en störsändare (S/J) som funktion av avståndet mellan störare och RPA.



Figur 3. Signal-störförhållande som funktion av avståndet mellan störare och RPA, för några olika scenarier.

Kommunikationssystemet har fördel av den stora riktantennen på marken vilket ger en stark nyttosignal i RPA:n. Då RPA:n befinner sig 10 mil från markstationen behöver fartyget vara närmare RPA:n än 20 mil och flygplanet närmare än 3 mil. Då RPA:n befinner sig 40 mil från markstationen behöver störarna istället vara närmare än 90 mil för fartyget och 10 mil för flygplanet.

Vi har antagit att RPA:n har en rundstålande antenn som tar emot lika mycket i alla riktningar. En möjlighet att förbättra för kommunikationssystemet är att använda en riktantenn i RPA:n. Det skulle kunna vara en elektriskt styrbar antennarray som skulle kunna användas för att förstärka nyttosignalen och/eller placera nollställen i riktning mot störaren. En sådan lösning är dock kostsam och utrymmeskrävande och kan möjligtvis vara realiserbar på en stor RPA.

Andra alternativ för att förbättra störskyddet är att använda sig av bandspridning i form av frekvenshopp eller direktsekvensspridning. Vid bandspridning används ett större frekvensband än vad som nyttosignalen kräver för att störaren inte ska kunna koncentrera sin störeffekt just till nyttosignalen. Även felrättande kodning kan användas i viss mån för att sänka kravet på effektförhållandet mellan nytto- och störsignal.

2.11 Sammanfattning

Kommunikationen till en RPAS är viktig för att den ska kunna utföra sin uppgift och flera olika kommunikationslänkar behövs. Styrdata och statusinformation om farkosten ska kunna överföras mellan markstation och RPAS. Sensordata ska kunna skickas till markstationen för analys och även sensorerna kan behöva viss styrning. Ett RPAS behöver även kunna kommunicera med civil trafikledning för att få operera i gemensamt luftrum.

För ett RPAS finns ett telekrigshot med bland annat risk för fientlig störning, avlyssning och vilseledning. Det är därför viktigt att kommunikationslänkarna är robusta och designade utifrån hotbilden.

Frekvensspektrum är en begränsad resurs som används av många olika system och följaktligen kommer tillgången till spektrum att vara en begränsande faktor för mängden sensordata som kan överföras.

3 Satellitnavigering

Den vanligaste formen av navigationshjälpmedel för autonoma farkoster är idag, och troligen även i framtiden, ett tröghetsnavigeringssystem (*Inertial Navigation System*, INS) som stöttas av ett *Global Navigation Satellite System* (GNSS). INS-systemets stora fördel är dess snabba uppdatering. Nackdelen är att INS utan yttre stöttning driver med tiden och tappar i noggrannhet. GNSS-systemet är å andra sidan väldigt stabilt över tiden, men har en ganska långsam uppdateringsfrekvens. Ett oskyddat GNSS är också relativt känsligt för störning och vilseledning vilket INS inte är. INS och GNSS har egenskaper som kompletterar varandra väl och tillsammans ger det ett navigeringssystem som är snabbt, noggrant och stabilt både under långa och korta tidsperioder.

Det enda användbara GNSS har i många år varit GPS med den civila C/A- och den militära (krypterade) P(Y)-signalen. Det finns nu ett antal nya GNSS-konstellationer med nya signaler och tjänster. Dessa nya signaler ger flera möjliga förbättringar för framtida GNSS-mottagares tillgänglighet, noggrannhet och robusthet.

Tillgängligheten kan öka genom att kombinera signaler från flera olika GNSS. På sikt kommer det att finnas 3-4 olika globala GNSS med tillsammans över 100 satelliter i drift. Det planeras en stor mängd nya GNSS-signaler och positionsnoggrannheten kan öka genom att flera av de nya signalerna har större bandbredd och därmed möjlighet till bättre noggrannhet.

För ett RPAS är det viktigt att positioneringssystemet är tillförlitligt och robust. Robusthet kan betraktas ur flera perspektiv, t.ex.

- robusthet mot avskärmning av himlen genom att fler satelliter blir tillgängliga,
- robusthet mot flervägsutbredning,
- robusthet mot störning (avsiktlig eller oavsiktlig),
- robusthet mot vilseledning.

3.1 Hotbild

Precis som för övriga kommunikationssystem på ett RPAS, så är störning troligen det största hotet mot ett satellitnavigeringssystems funktion. Problemet i GNSS är dessutom ofta ännu större än för andra kommunikationssystem, eftersom satellitsignalerna är oerhört svaga, t.o.m. långt svagare än bruset i mottagaren. Därför krävs det relativt liten effekt för att störa ut en GNSS-

mottagare. Det finns idag ett stort utbud av kommersiella GPS-störsändare att köpa för några hundra kronor (se t.ex. Mitch et al., 2012).

Det är även möjligt att köpa ganska avancerade störsändare, med hög uteffekt och riktantenner, på internet. Sådan störsändning är naturligtvis förbjuden i de flesta länder, men det finns flera dokumenterade exempel på att störsändare har använts och påverkat GPS-mottagare under de senaste åren, både medvetet och av misstag:

- Biskopstorp, 18 oktober 2011 (Hallandsposten, 4 jan. 2012): Flera personer rapporterade att GPS-navigatorer och mobiltelefoner inte fungerade i ett område i södra Sverige. Polisen undersökte problemet och fann stöldgods, bl.a. båtmotorer och bildäck, till ett värde av över en miljon kronor. Störsändare hade använts för att hindra att stöldgodset skulle kunna spåras.

- Newark flygplats, New Jersey, 3 augusti 2012 (FCC, 2013): Tekniker upptäckte interferens under testning av ett *ground-based augmentation system* (GBAS). Man upptäckte att en Ford F-150 pickup utsände radiosignaler i det förbjudna frekvensbandet 1559-1610 MHz. Störsignalen från bilen blockerade mottagningen av GPS-signaler i GBAS. Föraren hävdade att han hade installerat och använt störsändaren för att blockera det GPS-baserade spårningssystemet som hans arbetsgivare hade installerat i fordonet.

- Newark flygplats, New Jersey, 2009 (Warburton och Tedeschi, 2011): Ingenjörer upptäckte att GPS-mottagare vid flygplatsen utsattes för dagliga avbrott i mottagningen. Det tog två månader för *Federal Aviation Authority* (FAA) att hitta orsaken till felet: en förare som passerade på en närliggande motorväg varje dag hade en billig GPS-störsändare i bilen för att hindra sin arbetsgivare från att spåra bilen.

- San Diego, 2007 (Hambling, 2011): Två av marinens fartyg genomförde en övning i hamnen i San Diego. För att testa procedurerna när kommunikationen blev utslagen genomförde man störsändning mot radioutrustningen. Oavsiktligt blockerade man även signalerna från GPS-satelliter. En stor del av central San Diego påverkades; systemet för följning av inkommande flygplan på flygplatsen hade funktionsproblem, personsökare för att tillkalla läkare på *Naval Medical Center* slutade att fungera, trafikledningssystemet för att lotsa fartyg i hamnen fallerade, ca 150 basstationer blev utslagna så att mobiltelefoni inte fungerade, uttag från bankomater nekades.

- Nordkorea (GPS World, 8 maj 2012): Störning av GPS har genomförts under militära övningar vid tre tillfällen. Störning av GPS genomfördes

även under perioden 28 april till 13 maj 2012. Ett stort antal flygplan och fartyg påverkades.

- UK, juli 2010: Två personer dömdes till totalt 16 års fängelse för att ha deltagit i stölder av 40 lastbilar med last, till ett värde av sex miljoner GBP. GPS-störsändare hade använts för att skydda stöldgodset från upptäckt (The Economist, 12 mars 2011).
- Tyskland: Lastbilschaufförer har använt störsändare för att undgå landets GPS-baserade vägtullsystem (The Economist, 12 mars 2011).

Förutom alla dessa rapporterade störincidenter, har forskningsförsök genomförts bara under de senaste åren, där man har kunnat visa att vilseledning av GPS-mottagare är möjlig i praktiken (Kerns et al.). Dessa försök har gjorts genom vilseledning av den civila C/A-signalen som sänds helt okrypterad. Eftersom C/A-signalen är väl känd, kan man återskapa och sända ut felaktiga signaler som en GPS-mottagare accepterar istället för de autentiska satellitsignalerna. De militära (P(Y) och M-code) GPS-signalerna är krypterade och därmed svårare att återskapa på samma sätt som de civila signalerna, om man kan anta att kryptoskyddet är fullgott. Därmed kan en militär GPS-mottagare inte vilseledas på ett lika kontrollerat sätt som en civil mottagare, så länge krypteringen i den militära mottagaren används. Hotbilden för störning kvarstår dock även för militära GNSS-mottagare, både från billiga störsändare som man kan köpa på Internet och militär taktisk störning. Dock är de militära GPS-signalerna svårare att störa än de civila, framförallt tack vare att de har en betydligt större bandbredd. En militär telekrigsmotståndare kan ha betydligt kraftigare riktantenner och högre sändareffekt för att störa på långa avstånd. Ett framtida militärt hot är s.k. *emerging threat* (ET) störsändare som kan kombineras med vanliga GNSS-störsändare. På grund av det utbredda användandet av GPS i militära tillämpningar idag så förväntas hotet att öka i framtiden.

3.2 Störskyddsystem

För satellinavigering finns det en uppsjö av kommersiella störskyddsystem (t.ex. GAJT (Novatel), NAVSHIELD (Raytheon), SAS (BAE systems), Top Shield (Thales), DIGAR (Rockwell Collins)), som alla bygger på en gruppantenn och en signalbehandlingsenhet. Några har antennen och signalbehandlingen integrerad i en enhet, medan andra består av en elektronikenhet som kan kopplas till externa antennelement. Dessa störskyddsystem utnyttjar framförallt *nollstyrning*, som har diskuterats tidigare, för att minimera den mottagna effekten från störsändaren. De flesta systemen kan dessutom hantera flera samtidiga störare, och öka motståndskraften mot störning avsevärt.

4 Cybersäkerhet i RPAS

Cyberrymden, cybersäkerhet, cyberförsvar, med mera är begrepp som blir vanligare i media men även inom Försvarsmakten. Ibland har cybersäkerhet jämställts med informationssäkerhet eller informationstekniksäkerhet (IT-säkerhet) medan det vid andra tillfällen gjorts skillnad mellan dessa. Internationellt har begreppet cyber används en längre tid även om definitionerna av begreppen varierat. Detta märks framför allt i bredden av artiklar inom området där så vitt skilda åsikter som risken för ett ”Cyber Pearl Harbor” (Bumiller & Shanker 2012) kan ställas mot ”Cyber War will never happen” (Rid 2011).

I det här kapitlet studeras cybersäkerhet i framtida fjärrstyrda flygande system (eng. Remotely Piloted Aerial System, RPAS). För att kunna beskriva cybersäkerhet inleds kapitlet med att i avsnitt 4.1 identifiera var och hur svagheter i informationstekniksystem (IT-system) uppkommer. Därefter beskrivs traditionell IT-säkerhet i syfte att ligga till grund för en beskrivning och definition av cybersäkerhet. Med cybersäkerhetsbakgrunden avklarad övergår fokus mot att studera hur ett RPAS passar in i en cybermiljö samt vilka hot mot RPAS som finns där. Kapitlet avslutas med en prognos över framtida användning av RPAS inklusive vilka cybermässiga hot en sådan användning medför.

4.1 Svagheter i IT-system

Ett IT-system består av mjukvara och hårdvara men även nätverk, personal, organisation och fysisk miljö (Swedish Standard Institute (SIS) 2011), IT-systemet utgör ofta en komplex miljö av flera system och applikationer vilka tillsammas levererar den funktionalitet som efterfrågas.

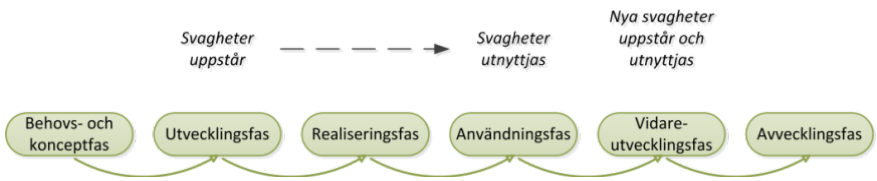
Det är vanligt att tänka på mjukvara när felaktigheter i IT-system påtalas och mjukvarufel utgör en stor del av problemet. IT-system behöver inte vara särskilt stora för att innehålla en stor mängd kod. Det rör sig ofta om miljontals rader kod i system som kan konfigureras och integreras med andra system. Inget IT-system är perfekt. Med hänsyn till den mängd kod och alla möjliga korrekta och inkorrekta sätt som system kan sättas samman är det lätt att inse att alla IT-system innehåller felaktigheter. McDonnell (2004, s.25) menar att det som ett genomsnitt inom IT-branschen uppkommer cirka 1-25 fel per 1000 rader kod. Även om det finns exempel på lägre genomsnitt (till exempel i mjukvaran tillhörande rymdfärjorna) har de mer effektiva metoderna att komma till rätta med felen inte bedömts ekonomiskt försvarbara för IT-industrin i allmänhet. Detta innebär mer eller mindre att alla system innehåller felaktigheter.

Mjukvara är dock inte den enda felkällan i ett IT-system. Fel uppstår även i hårdvara men dessutom även i icke-tekniska delar såsom säkerhetsprocedurer, i design av systemet eller i dess interna kontroller.

Felaktigheter i IT-system vilka exponeras för ett hot benämns enligt SIS (2007) som svagheter. Dessa svagheter kan uppstå på flera ställen från det att ett IT-system kravställs till dess det avvecklas. IT-system testas under utveckling för att tillse att de levererar den funktionalitet som efterfrågas, men endast sällan för att kontrollera att de inte har andra, oönskade, egenskaper. Detta gör att svagheter oftast upptäcks långt senare, i ett redan driftsatt system.

4.1.1 IT-livscykeln

Ett IT-system går igenom flera faser från det att behovet av IT-systemet uppmärksammas till dess att systemet är förbrukat och skall avvecklas. Dessa faser sammantaget kallas för IT-livscykeln och beskrivs av International Organization for Standardization (ISO) i ISO 15288 (SIS 2008), se figur 4.



Figur 4. Utvecklingsfaser för IT-system. (Svenska begrepp enligt Försvarshögskolan 2012).

Den huvudsakliga implementationen av ett IT-system sker i utvecklingsfasen (eng. development stage). Här omvandlas beställarens behov via design till mjukvara. Det är också här som de flesta fel i mjukvaran introduceras (Jones, 1996) vilka kan leda till svagheter. Svagheter skapade inom denna fas benämns mjukvarusvagheter (eng. software flaw vulnerabilities). En annan typ av svaghet inom denna fas är felaktiga antaganden avseende tillitsrelationen mellan olika mjukvarukomponenteter. Detta kallas felanvändning av funktion (eng. software feature misuse vulnerability) och inträffar när en systemdesigner gör antaganden om beroenden men utan att säkerhetsställa skyddet av dessa relationer.

Ett exempel som ges är användning av hyper text markup language (HTML) i en e-postklient. En utveklare som vill möjliggöra att hyperlänkar kan infogas i ett e-postmeddelande och gör antagandet att hyperlänkar inte har några säkerhetsmässiga konsekvenser. En angripare kan dock utnyttja HTML för att dölja verkliga länkar och därmed skicka en användare till en webbsida med skadlig kod istället för den webbsida som hyperlänken säger sig gå till. Svagheter som uppkommer senare, vid integration under realiseringsfasen (eng. production

stage) eller under användningsfasen (eng. utalization stage), beror inte nödvändigtvis på programmeringsfel utan kan vara designfel vilket gör det möjligt att försätta IT-systemet i ett osäkert tillstånd. Konfigurationsfel, det vill säga svagheter som uppkommer av att det är möjligt att med mjukvarans egna kontroller försätta den i ett osäkert läge, benämns konfigurationssvagheter (eng. security configuration issue vulnerability) (Scarfone & Mell 2010).

Vidareutvecklingsfasen (eng. support stage) är egentligen en helt egen livscykel i miniatyr. I fasen ingår att uppdatera programvara då svagheter identifierats men även utveckling av kompletterande funktionalitet. Både uppdateringar och utvecklingen av ny funktionalitet kan föra in nya svagheter i IT-systemet.

Svagheter i IT-system innebär dock inte att ett system kommer att haverera i framtiden. För att en svaghet skall utgöra en sårbarhet (SIS 2007) för ett IT-system måste det finnas en angripare med kompetens och vilja att utnyttja svagheten.

4.1.2 Utnyttjande av svagheter

De system som tillverkas för ledning och informationshantering är i princip uteslutande utvecklade från civila komponenter. Operativsystem och programvara som utvecklats för det civila kontorets verksamhet används som grund för specialiserade militära system med höga krav på sekretess och driftsäkerhet.

Säkerhetsfunktioner i civila system hanteras huvudsakligen genom ständiga reparationer, så kallade patchar, av mjukvaran. Om ett datorsystem byggt på civila standardkomponenter (eng. commercial off the shelf, COTS) inte kan uppdateras regelbundet innebär detta en möjlighet för en angripare att själv analysera patchen och identifiera vilka svagheter den reparerar. Angriparen kan med denna kunskap skapa ett verktyg som utnyttjar denna svaghet. Således finns det ett riskfönster mellan tidpunkten då ett säkerhetshål blir känt och tidpunkten då en patch inte bara har tillverkas och distribueras, utan faktiskt installerats på systemets noder.

På samma sätt är systemskydden mot skadlig kod i hög grad beroende av ständiga uppdateringar av signaturbibliotek. Dagens antivirusprogram fungerar i huvudsak dels genom att jämföra den exekverbara koden med de signaturer av skadlig kod som programmet har i sitt bibliotek, dels genom att försöka avgöra om den exekverbara koden gör något ”avvikande” som kan uppfattas som ett angrepp. Exemplet med ett antivirusprogram visar på likheterna i metoden för en angripare. Ett antivirusprogram är dock inte en del av en ursprunglig systemdesign utan ett tillägg till systemen som görs i efterhand och som oftast är nödvändig.

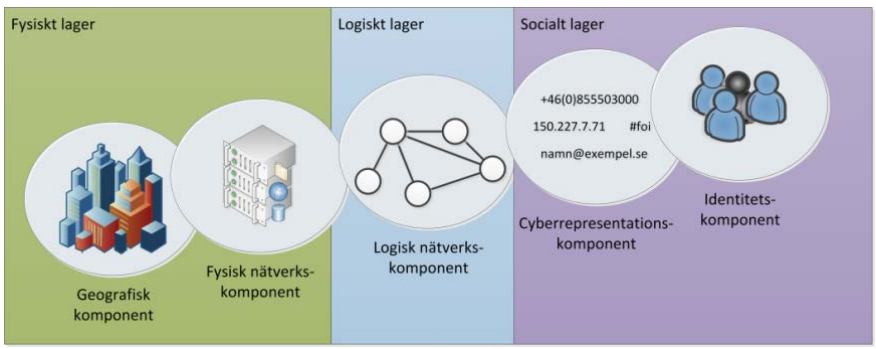
4.2 Cybermiljön

Cyber är ett begrepp som växt sig starkt i media men även i militära kretsar de senaste åren. Det är framför allt sedan 2011 som cyber blivit ett ord på allas läppar i och med att Nato fastställde en cyberstrategi (North Atlantic Treaty Organization (NATO) 2011) och att flera andra länder och organisationer följde efter med nationella motsvarigheter, se till exempel Europeiska Unionen (Europeiska Kommissionen 2013), Storbritannien (Cabinet Office 2011) eller Tyskland (Federal Ministry of the Interior 2011).

Även om cyber ännu inte är ett fastlagt begrepp inom Försvarsmakten så är Försvarsmakten aktiv inom de områden som kan anses omfattas av begreppet cyber. Försvarsmakten har valt att beskriva cyberrymden som en cybermiljö (Försvarsmakten 2012) vilket är det begrepp som kommer att användas i resterade del av det här kapitlet.

Ibland beskrivs cyber som IT eller som internet. En sådan beskrivning tar dock enbart hänsyn till den teknik som möjliggör dagens användning av IT och internet men inte hur den används eller av vem. Till tekniken tillkommer även de arbetsytor eller aktiviteter som skapas med stöd av IT men som inte är designade vid konstruktionen av ett system. Detta mervärde är något som bara finns i IT-systemet och inte i den fysiska världen. För att kunna interagera med IT-system har användare en digital representation, en digital identitet, genom vilken en fysisk person eller ett annat IT-system agerar i IT-systemet. Tillsammans utgör detta en kombination av effekter i den fysiska världen, människor och teknik.

Det finns flera beskrivningar av hur cybermiljön är uppbyggd men ett exempel som tar en bred ansats är amerikanska arméns (Department of the Army (DOA) 2010) uppdelning i en fysisk, logisk och social domän (figur 5).



Figur 5. Cybermiljön enligt (DOA 2010).

Det är teknik som ligger till grund för IT-system. Hårdvara såsom servrar, nätverksenheter, datorer, routrar, med mera är fysiska nätverkskomponenter (eng. physical network components) som utgör IT-system. I och med att dessa komponenter finns i den fysiska världen kan de beskrivas som en geografisk komponent (eng. geographic component) och pekas ut med en adress eller en koordinat. Ändsystem såsom smartphones eller bärbara datorer kan visserligen flyttas omkring men de kan ändå beskrivs med en plats för varje givet ögonblick. Fysiska nätverkskomponenter kopplas samman i ett logiskt system och beskrivs som en logisk nätverkskomponent (eng. logical network component). Det är genom det logiska systemet som användare och tjänster hittar varandra utan att behöver känna till var eller vilken typ av fysisk maskin som finns i andra änden. I slutänden av ett system finns det användare. Det kan vara människor eller andra IT-system, här beskrivna i en identitetskomponent (eng. persona component). Gemensamt för en entitet är att det är någon som på något sätt vill dra nytta av eller påverka ett IT-system. Den fysiska människan eller ett annat IT-system agerar dock inte direkt i aktuellt IT-system utan genom en digital representation. En sådan representation utgörs av en cyberrepresentationskomponent (eng. cyber persona component) vilken exempelvis kan vara en användaridentitet, en mejladress, ett internetprotokollnummer (IP-nummer) eller en hashtagg. Ett alternativt sätt att beskriva komponenterna är att en individ (identitetskomponent i det sociala lagret) agerar i en teknisk miljö (cyberrepresentationskomponent i det sociala lagret, logisk nätverkskomponent i det logiska lagret samt fysiska nätverkskomponenter i det fysiska lagret) vilket påverkar den fysiska världen (Trucotte 2012). Beskrivningen är något begränsad om endast människor tas upp men vidgas individen till att omfatta både människor och system stämmer beskrivningen bättre med en IT- och cybermiljö.
Cybermiljön är den virtuella miljö som skapas mellan fysiska system och fysiska användare och där information skapas, utbyts och lagras. Internet är en del (en komponent) av cybermiljön men där internet fokuserar på teknik genom protokoll och standarder fokuserar cybermiljön på att hantera processer, informationsutbyten, sociala kontexter och policys (McConnell 2011). Affärstransaktioner eller sociala utbyten som tidigare skedde i den fysiska världen men som nu kan ske i den virtuella cybermiljön påverkar hur nutida och framtida affärsverksamheter kommer att genomföras.

4.2.1 Skillnader mellan cybermiljön och den fysiska miljön

Cybermiljön är en miljö helt och hållet skapad av människor. På så sätt skiljer den sig tydligt från de mer konventionella militära miljöerna luft, land och sjö. Ett tydligt exempel på detta är att geografiska avstånd allt som oftast är av underordnad betydelse. En användares agerande får nästan omedelbart

genomslag oavsett var användaren befinner sig geografiskt och var det system som användaren agerar mot befinner sig.

Internet som den huvudsakliga bäraren av kommunikation inom cybermiljön är distribuerat i sin uppbyggnad och de grundläggande funktionerna är robusta. Dock står inte internet under någons specifika kontroll utan mer eller mindre kontrollerade delar ansluter till varandra och bildar nätverk av nätverk. Dessa nätverk har olika ägare, i form av internetleverantörer, företag och länder. För att verka i cybermiljön måste flera nätverk och system användas. Dessa nätverk och system är oftast osynliga för användare då de är stödsystem och inte något som användaren medvetet agerar mot. Den naturliga robusthet och de divergerande ägandeformerna gör att en dominans av cybermiljön på samma sätt som dominans i luftmiljön inte är en rimlig målsättning (DOA 2012).

Den fysiska miljön kan påverka cybermiljön direkt i stor utstreckning men det är väldigt sällan det omvända förhållandet gäller. Ett fysiskt angrepp mot hårdvara såsom servrar och nätverksutrustning men även mot de byggnader och elförsörjning som IT-systemen är beroende av får en direkt effekt på systemens förmåga att utföra sin uppgift. Vid det fysiska angreppet tillförs energi i form av våld vilket skadar IT-systemet utifrån. Ett cyberangrepp kan få samma effekt på IT-systemet (det upphör att fungera) men den direkta effekten utanför IT-systemet är marginell. Cyberangreppet utgörs av instruktioner till det IT-system som angrips. Syftet med instruktionerna är att få IT-systemet att upphöra att fungera, förändra dess innehåll, tillföra felaktigt innehåll eller lyssna av trafiken till och från IT-systemet (Pfleeger & Lawrence Pfleeger 2006). Även om direkta konsevenser är ovanliga är det är dock rimligt att tänka att ett angrepp ifrån cybermiljön kan ge indirekta effekter i den fysiska världen genom att en funktionalitet som IT-systemet levererar slutar att fungera.

4.2.2 Likheter mellan cybermiljön och den fysiska miljön

I och med att cybermiljön även omfattar sådana egenskaper som får effekt i den fysiska världen skiljer sig cybermiljön från ett IT-system genom att den även omfattar den verksamhet som bedrivs med hjälp av IT-systemen. På så sätt är cybermiljön en förlängning av verksamhet som bedrivs i den fysiska miljön. Kritiska resurser såsom produkter, information och system skapas och används i cybermiljön men effekten mäts i den fysiska miljön i form av exempelvis framgång, effektivitet eller vinst. En angripare har som mål att påverka verksamheten till sin egen fördel, vare sig det handlar om att störa, manipulera eller göra vinst. Angreppsformen är ett verktyg för att uppnå ett mål, men det är verksamheten som utgör målet. Det innebär att aktiviteter såsom brottslighet,

underrättelseinhämtning och hacktivism[1] är lika aktuellt för cybermiljön som för verksamheten i den fysiska miljön (Robinson, Gribbon, Horvath & Robertson 2013). Även cyberkrig brukar räknas med i dessa aktiviteter men det är ännu oklart vad begreppet cyberkrig innebär.

4.3 Säkerhet inom IT-verksamhet

De exempel på svagheter i kod som beskrevs i sektion 4.1 kan till viss del beskrivas som kvalitétsproblem. Svagheter som ger oönskade effekter eller skador i den verksamhet som IT-systemet stödjer klassas dock bättre som säkerhetsfrågor. Säkerhetsfrågeställningar avseende IT-system avser antingen frågor rörande skador som system kan åstadkomma på den som brukar IT-systemet (från engelskans safety) alternativt frågor rörande de skador på ett IT-system som en medveten angripare (antagonist) kan åstadkomma (från engelskans security). Till den senare av dessa grupper räknas även brukare av system som oavsiktligt orsakar skada genom ett felaktigt användande. I den här rapporten avses om annat inte anges tolkningen att säkerhetsfrågor rör situationer där det finns en antagonistisk motståndare, det vill säga den engelska tolkningen av security.

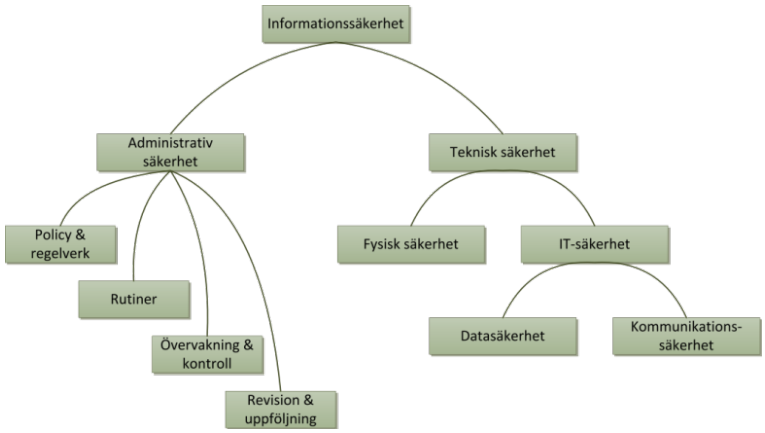
Cybersäkerhet är ännu inte väl definierat och framför allt råder det ingen allmän acceptans för en speciell definition. Av denna anledning beskrivs här först informationssäkerhet och därefter cybersäkerhet.

4.3.1 Informationssäkerhet

Informationssäkerhet kan beskrivas på flera sätt beroende på vad som skall uppnås med beskrivningen. Två vanligt förekommande modeller beskriver informationssäkerhet genom att antingen beskriva var ansvar för säkerhetsfrågor ligger eller genom att beskriva de egenskaper som säkerheten skall upprätthålla.

Att beskriva informationssäkerhet ur ett ansvarsperspektiv underlättas om man vill definiera skyddsåtgärder som behövs och var de skall sättas in (SIS 2007), figur 6. Huvudindelningen av informationssäkerhet utgörs av administrativ säkerhet och teknisk säkerhet.

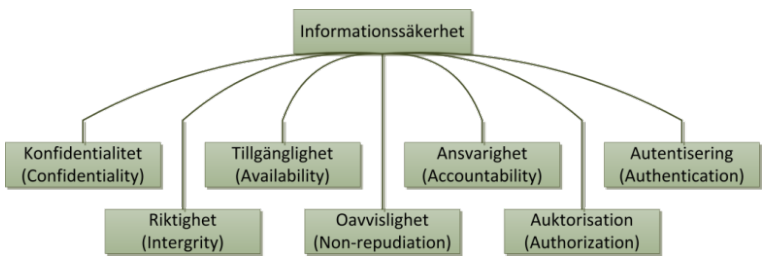
[1] IT-aktivitet som stöder ett politiskt mål, kan vara brottslig, exempelvis datorintrång eller – sabotage, men även propaganda och assistans till politiska aktivister faller in under termen.



Figur 6. Informationssäkerhet baserat på ansvar (SIS 2007).

Inom den administrativa säkerheten beskrivs regler för hur information skall hanteras. Dessa regler är egentligen inte enbart avgränsade för att gälla digitala uppgifter utan bör gälla för all information oavsett vilken typ av media som informationen lagras på. Den tekniska delen hanterar dels den fysiska säkerheten, det vill säga begränsning av fysisk åtkomst till IT-system, dels IT-säkerhet. Här avser IT-säkerhet de tekniska lösningar som krävs för att skydda information i vila och under transport. Modellen är kanske mest inriktad på att statiskt kunna beskriva de system som skall skydda den information de innehåller.

Ett annat vanligt sätt att beskriva informationssäkerhet är genom att ange tre grundläggande skyddsegenskaper som skyddsmekanismer skall uppnå; sekretess (eng. confidentiality), riktighet (eng. integrity) och tillgänglighet (eng. availability). Dessa tre egenskaper, vanligtvis förkortade till CIA efter dess engelska begrepp, kan beskriva information men även de system som skall skydda information. Efterhand har CIA-egenskaperna kompletterats med andra egenskaper allteftersom behov uppstått, se figur 4.



Figur 7. Informationssäkerhet (SIS 2007).

Modellen i figur 7 tar upp egenskaper men till skillnad från figur 6 säger inget om vem eller var ansvar faller för att uppnå eller upprätthålla egenskaperna. Gemensamt för de båda modellerna är systemfokus. Dock tar de inte upp hur systemen skapas eller hur de hanteras i operativ miljö vilket gör dem otillräckliga för att beskriva de behov som finns i en cybermiljö.

4.3.2 Cybersäkerhet

Likväl som att begreppet cybermiljö omfattar mer än bara den teknik som utgör internet och de IT-system som används, bör även begreppet cybersäkerhet spegla denna utökade betydelse. Det som framför allt skiljer cybermiljön från traditionell IT är inkorporeringen av verksamhet vilket ger en något annorlunda problembild.

En verksamhetsorienterad säkerhetsmodell måste kunna hantera problem som uppkommer efterhand. En helt reaktiv modell är dock inte att föredra utan problem måste kunna förekommas. Förberedda processer och rutiner förkortar reaktionstider och gör därmed att en verksamhet kan fortgå eller endast lindrigt hämmas av att den utsätts för påfrestningar i form av ett externt angrepp. Möjligheten att upptäcka och analysera problem allteftersom samt att varna en operatör utgör kritiska förmågor i en cybersäkerhetsmodell. En effektiv implementation av en cybersäkerhetsmodell kräver även en förmåga att dela säkerhetsrelaterade uppgifter med andra IT-system i syfte att kunna minska de risker ett IT-system utsätts för (World Economic Forum 2012).

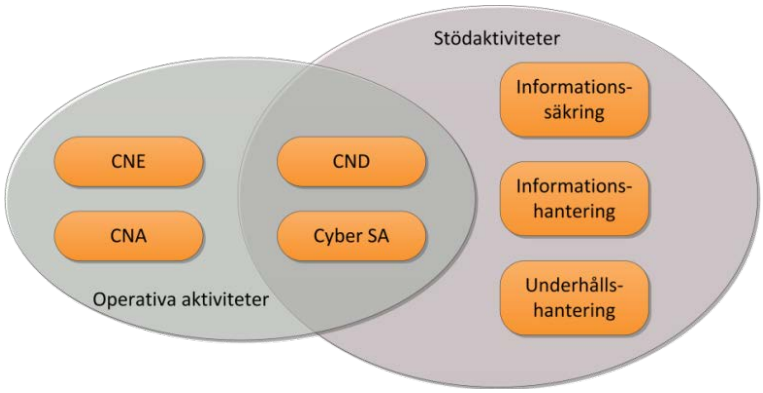
Standarder för hur IT-baserad verksamhet skall hanteras när den utsätts för påfrestningar är än så länge i sin linda. National Institute of Standards and Technology (NIST) (2013) har tagit fram ett preliminärt förslag till ramverk för hur förmåga till cybersäkerhet kan beskrivas (figur 8). Ramverket identifierar fem steg för att beskriva hur cybersäkerhet kan implementeras i en organisation. Inledningsvis i steget Identifiera (eng. identify) görs en inventering av organisationens tillgångar och verksamhetskontext. Det är utifrån detta steg som det är möjligt att fokusera på lösningar, avgränsningar och prioriteringar. Därefter, i steget Värna (eng. protect), tas skyddsmetoder fram vilka ligger i linje med den riskbedömning som gjordes i förra steget. Värna motsvarar den administrativa säkerheten och IT-säkerheten i SIS (2007) beskrivning av informationssäkerhet (figur 4). De två första stegen utgör förberedande funktioner vilka möjliggör ett handlingskraftigt agerande om IT-systemen utsätts för angrepp. I tredje steget, Upptäcka (eng. detect), avser funktioner för att upptäcka händelser i verksamhetssystem som kan utgöra ett hot. Att enbart kunna upptäcka ett hot är inte så meningsfullt om det inte kopplas en reaktion till upptäckten vilket sker i steget Svara (eng. respond). På vilket sätt reaktionen sker beror på typen av verksamhet och de risker verksamhetsföreträdarna är villiga att

ta. En aktiv cybersäkerhet innebär att IT-system kan behöva återtas i drift under pågående angrepp. Vilka dessa system är regleras igenom den prioritering som i säkerhetsanalysen och redovisas i sista steget - Återhämta (eng. recover).

Figur 8. NIST preliminära cybersäkerhetsramverk.

Ramverket bygger på tidigare standarder för informationssäkerhetsledning och koppling av verksamhetsmål till IT-system. Exempel på bakomliggande ramverk är ISO 27001 (SIS 2006) och Control Objectives for Information and Related Technology (CORBIT) (ISACA u.å.). En svaghet i ramverket kan anses vara att det endast tar upp hantering av befintliga system vad avser incidenter men inte underhållsfrågor. Detta har uppmärksammats av preliminärutgåvan och ligger som en förbättringspunkt för kommande versioner.

Ett angrepp inom kontexten cyber är ett logiskt angrepp som har sitt ursprung i cybermiljön, det vill säga den operativa miljön, och som slår mot offrets cybermiljö (Kissel red. 2013). Det innebär att de aktiviteter som genomförs inom ramen för cyberoperationer kan vara offensiva, såsom attacker (eng. computer network attacks, CNA), nätövervakning (eng. computer network exploitation, CNE) samt mer traditionell signalspaning (SIGINT). Även telekrig ingår som en möjlig offensiv aktivitet men det är inte nödvändigtvis ett cyberangrepp. Mer defensiva men ändå aktiva aktiviteter rör sig om försvar (eng. computer network defence, CND) samt övervakning av den egna miljön (eng. cyber situational awareness, Cyber SA). Detta är aktiva handlingar men de förutsätter att en robust IT-miljö har skapats och att tillförlitligheten till IT-miljön och informationshanteringen är adekvat och effektiv. Grunden för ett stabilt IT-system utgör stödfunktioner till cybersäkerhet och är aktiviteter som i huvudsak utförs utanför den operativa kontexten. Här avses aktiviter såsom informationshantering, informationssäkring och underhållshantering (Turcotte 2012, bild 8) (figur 9).



Figur 9. Aktiviteter inom cybermiljön.

Cybersäkerhet är avgränsat till att bevara egenskaperna sekretess, riktighet och tillgänglighet för människor, IT-system och IT-tjänster (NIST 2013) genom skyddsåtgärder mot angrepp från cybermiljön mot den egna verksamheten i en operativ miljö. Till skillnad från exempelvis IT-säkerhet avses inte enbart information eller IT-system utan den verksamhet som bedrivs av den angripna organisationen. IT-systemen som verksamheten bedrivs på är givetvis ett möjligt mål men det är även människorna som agerar genom dessa system, jämför figur 5.

Logiska angrepp, det vill säga angrepp ifrån cybermiljön, omfattar instruktioner som skickas från en angripare till det tänkta målet. Syftet med instruktionerna är att utnyttja en sårbarhet, en felaktighet, i det mottagande systemet för att därefter kunna uppfylla målet med angreppet vare sig det är att ta kontroll över mottagaren eller att kunna lyssna av kommunikationen. En förutsättning för att ett logiskt angrepp skall vara framgångsrikt är att det finns en svaghet att utnyttja och att denna är känd. Instruktioner som skickas på måfå är sällan framgångsrika och målet med sådana angrepp är tveksamt.

De aktiviteter som utförs i den operativa miljön i syfte att skydda en verksamhet finns där för att den ansvarige för verksamheten har förutsatt att det finns svagheter i systemen. Det innebär att de operativa aktiviteterna inte omintetgör sårbarheter men de kan mildra effekten av dem. För att skapa ett system med så lite sårbarheter som möjligt krävs ett stort förarbete och underhållsarbete.

Cybersäkerhet skiljer sig från informationssäkerhet genom att det är andra tillgångar som är hotade eller att tillgången enbart är ett medel för att påverka människor och verksamhet utanför IT-systemet. von Solms och van Niekerk (2013) argumenterar för att tillgångar i en IT-miljö, vare sig det är information eller system, är målet för ett IT-angrepp medan för en cyberattack är tillgångarna

bara medel. Det är människor och deras intressen som är målet med en cyber-attack. Det finns ett värde som skapas med stöd av IT-systemen men som inte utgörs av dem.

4.3.3 Motståndare och förmågor

Det är svårt att på ett meningsfullt sätt identifiera generiska motståndargrupper inom cybermiljön. *Vem* är ibland mindre intressant än syfte och motiv. Till detta kommer förmåga i form av kunskap, träning och resurser. Hoten kan dessutom se olika ut beroende på i vilken fas i ett systems livscykel som hotet realiseras. Metoderna för hur hot realiseras kan vara lika även om syfte, motiv och uppdragsgivare varierar.

Kriminella aktörer, det vill säga aktörer vars främsta syfte är att genom brott tjäna pengar, kan vara väl motiverade och kompetenta. Deras drivkraft gör att de främst väljer mål där vinsten är hög jämfört med insatsen.

Cyberbrottslighet är inte ett primärt militärt intresse även om Försvarsmaktens verksamhet indirekt kan drabbas av konsekvenser av cyberbaserad brottslighet.

Politiskt motiverade grupper, så kallade *hacktivister*, är ofta mycket motiverade till att få fram sitt budskap. Deras generella metoder har dock hittills inte varit på hög teknisk nivå.

Hackerkollektiv är ofta mycket motiverade och högt utbildade. De behöver dock inte vara politiskt motiverade eller uttalat brottsligt motiverade. Deras styrka ligger i deras kunskap och deras kontakter. Sådana grupper kan dock mycket väl jobba på uppdrag av stater, brottsliga eller politiska organisationer.

Statliga aktörer har på senare år etablerat sig tydligt som aktörer i cybermiljön (Marinos 2013). De statliga aktörerna har egna resurser i form av underrättelseorganisationer och militära förband. En stat kan ha flera intressen att agera i cybermiljön. Militärt innebär det att skaffa sig strategiska eller taktiska fördelar över en motståndare, politiskt att skaffa sig kunskap om motståndare men även ekonomiskt för att framhäva den egna marknaden. För att uppnå dessa mål är underrättelsetjänst och sabotage de främsta verktygen. En statlig aktör kan dock jobba med en annan tidshorisont än privata aktörer. Det, tillsammans med ekonomiska resurser, innebär att de också kan agera över ett systems hela livscykel, såväl tekniskt som med andra metoder.

I rapporten Resilient Military Systems and the Advanced Cyber Threat (Defense Science Board (DSB) 2013), delas hotaktörer in i sex klasser baserat på deras förmåga.

1. Angriparen kan använda verktyg och programvara som andra tillverkat.

2. Angriparen har kompetens att tillverka egna verktyg och vapen som angriper kända svagheter.
3. Angriparen kan på egen hand hitta nya okända svagheter genom olika typer av kodanalys och data mining. Angriparen kan tillverka verktyg och vapen skräddarsydda för ett visst mål.
4. Professionella och resursstarka angripare (myndighetspersonal eller kriminella) som arbetar organiserat och i grupp för att tillverka verktyg och utföra angrepp.
5. Nationsstater som skapar förutsättningar för framtida intrång genom att påverka tillverkning och utveckling av produkter.
6. Nationsstater som integrerat cyber- med underrättelse- och militär verksamhet i operationer mot politiska, militära och ekonomiska mål, så kallade fullspektrumoperationer.

Uttrycks indelningen lite förenklat kan man säga att kategori 1 och 2 kan utnyttja befintliga och kända svagheter genom att använda färdiga verktyg. Kategori 3 och 4 har förmåga att upptäcka nya svagheter och utveckla verktyg för att utnyttja dessa sårbarheter. Den högsta grupperingen med kategori 5 och 6 kan på egenhand skapa sårbarheter i system. Ett exempel på en möjlig sådan långsiktig påverkan beskrivs av Newman (2013).
Baserat på DSB:s kategorisering kan man anta att politiskt motiverade grupper, så kallade hacktivister, befinner sig i de lägre grupperingarna. Deras motivation gör att de primärt söker uppmärksamhet för sin agenda och använder därmed cybermiljön som ett verktyg. Den stora majoriteten utgör inget hot mot skyddade system utan angriper webbsidor och liknande. Hackerkollektiv är inte en homogen grupp utan varierar stort i förmåga. De bättre av dem har förmåga att identifiera sårbarheter på egen hand. Sådana grupper har ofta någon form av stöd från en statlig aktör. Det är vanligt att hackerkollektiv består av en mindre kärna av kompetenta angripare understödda av en större grupp medhjälpare med enklare uppgifter. Flertalet statsaktörer har samma kompetens som hackerkollektiv men kan backa upp detta med mer resurser i form av ekonomi och personal. Det blir vanligare med stater som har militära förband helt inriktade på att agera i cybermiljön. Förmågan att kunna skapa sårbarheter i IT-system är dock ännu bara förbehållet ett fåtal nationer enligt rapporten.

4.3.4 Exempel på cyberangrepp

Nedan presenteras tre uppmärksammade angrepp mot RPAS. Beskrivningarna är kortfattade då mängden uppgifter rörande incidenterna är begränsade och bitvis motsägelsefulla men de ger en bild av hur egenskaperna sekretess, riktighet eller tillgänglighet sats ur spel av ett angrepp.

Hezbollah 1996

Hezbollahs generalsekreterare Hassan Nasrallah hävdade i ett pressmeddelande att Hezbollah sedan 1996 kunnat avkoda videosignaler från Israeliska spanings-RPAS:er (Grant 2010). Han hävdade vidare att detta var anledningen till att Hezbollah lyckats med sitt bakhåll i byn Antsaria 1997, där tolv israeliska kommandosoldater dödades.

Exemplet visar på hur RPAS:en inte kunde vidmakthålla sekretess över sin kommunikationskanal.

Irakiska motståndsrörelsen 2008

I december 2008 hittade soldater från USA videomaterial från Predator- RPAS:er på en laptop tillhörande den irakiska motståndsrörelsen (Arthur 2009). Det visade sig vid senare undersökningar att det inte var någon engångshändelse utan att ett datorprogram kallat SkyGrabber hade inhandlats på den öppna marknaden av motståndsrörelsen. Med detta kunde de avlyssna RPAS:ernas sändningar med en vanlig parabolantenn och spela upp sändningarna på en TV.

Exemplet visar på hur RPAS:en inte kunde vidmakthålla sekretess över sin kommunikationskanal.

Irans revolutionsgarde 2011

I december 2011 fick Iran tag på en RPAS av typen RQ-170 tillhörande USA. USA hävdade att den störtat i Iran efter att ha fått motorfel på afghanskt territorium. Iran hävdar att RPAS:en kränkt deras luftrum under ett spionuppdrag och att ett tele/cyberkrigsförband stört RPAS:ens kommunikation och falsksignalerat den för att få den att landa (Jeffe & Erdbrink 2011).

Exemplet visar på hur RPAS:en inte kunde vidmakthålla riktighet i sina kontrollfunktioner.

4.4 Fjärrstyrda flygande system

RPAS blir allt vanligare. De har framför allt haft framgång militärt men civila tillämpningar börjar komma ut på marknaden. Användningen av RPAS i konflikter de senaste tio till femton åren har ökat markant. Bara mellan 2004 och 2008 ökade användningen globalt femfaldigt, från 1000 till 5000 system (Frost & Sullivan 2007, s.5) och idag har ett 40-tal länder tillgång till RPAS (Försvarsmakten 2013, s.37).

Något som är värt att notera när det gäller militära RPAS är att dessa hittills uteslutande används i militärt dominerade luftrum; antingen över luftrum i en krigszon eller över ett avlyst övningsfält. Det innebär att ett fjärrstyrt flygplan (eng. Remotely Piloted Aircraft, RPA) aldrig har behövt ta hänsyn till civil

luftfart eller behövt ett civilt godkännande för att användas. Till detta kommer att i de militärt kontrollerade luftrumen har dessutom ägaren till de använda RPA:erna haft luftherravälde och varit tekniskt överlägsen sin motståndare (Försvarsmakten 2013, s.38-39). Dominansen i luftrummet och den höga utvecklingstakten baserat på det ökade behovet de senaste tio åren har medfört produkter med lägre kvalité jämfört med vad som är normalt för militär utrustning av det här slaget (Kim, Wampler, Goppert & Hwang 2012).

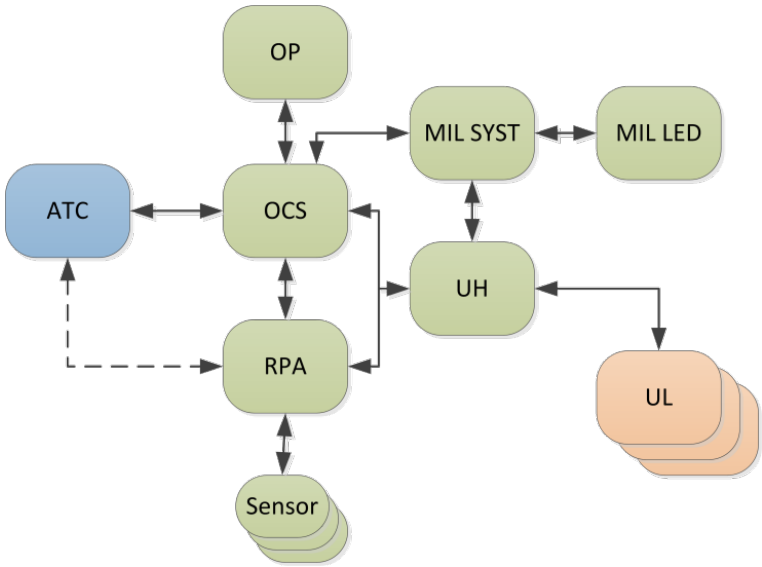
Syftet med det här delkapitlet inte att beskriva hur en RPA är uppbyggd i detalj utan att identifiera de tillgångar och aktörer (SIS 2012) som utgör ett RPAS i syfte att kunna analysera de cyberhot som finns i ett RPAS.

4.4.1 Aktörer

Ett RPAS består inte enbart av en RPA utan av flera delsystem som agerar tillsammas för att uppfylla ett militärt mål. Varje delsystem är en aktör inom RPAS och kan (ibland omväxlande) vara konsument eller producent av tillgångar.

En översiktlig bild av RPAS ger att det finns en RPA, en operatör (OP) som styr RPA:n, samt ett militärt lednings- och kontrollsystem (MLK) respektive ett motsvarande civilt (eng. air traffic control, ATC). Alla dessa aktörer verkar i en miljö (MIL) som påverkar dem. Detta ger dock en lite för enkel bild av RPAS. I avsnitt 4.1.1 beskrevs att svagheter i system uppkommer huvudsakligen i utvecklingsfasen av ett systems livscykel och att svagheten utnyttjas i systemets operativa miljö. Det gör att alla gränsytor där information, mjukvara eller hårdvara ändras eller på annat sätt kommer i kontakt med RPAS måste tydliggöras.

I en något mer detaljerad beskrivning använder operatören en kontrollterminal (eng. operator control station, OCS) för att kontrollera RPA:n. Den civila flygledningen kommunicerar med operatören via OCS men även direkt med RPA:n via automatiserade kontroller som krävs för civilt luftrum. RPA:n samlar in information via de sensorer som den bär med sig. Sensorinformationen förs vidare till andra militära ledningssystem (MIL SYST) via OCS. Information insamlad av en RPA påverkar i slutänden den militära lednigen (MIL LED) som skickat iväg RPA:n på uppdraget.



Figur 10. RPAS utökad systembild.

På den här detaljnivån (figur 10) kommer en ny aktör in som inte var synlig i den första övergripande beskrivningen. Operatören kontrollerar RPA:n under pågående uppdrag men förberedelser för uppdrag sker av servicepersonal. Serviceorganisationen (UH) ansvarar även för underhåll och reparationer av RPA:n men även de andra kontrollsystemen. Serviceorganisationen följer uppsatta regelverk för hur komponenter hanteras och underhållsscheman. Hårdvara och mjukvara levereras dock från lager eller underleverantörer (UL).

4.4.2 Tillgångar

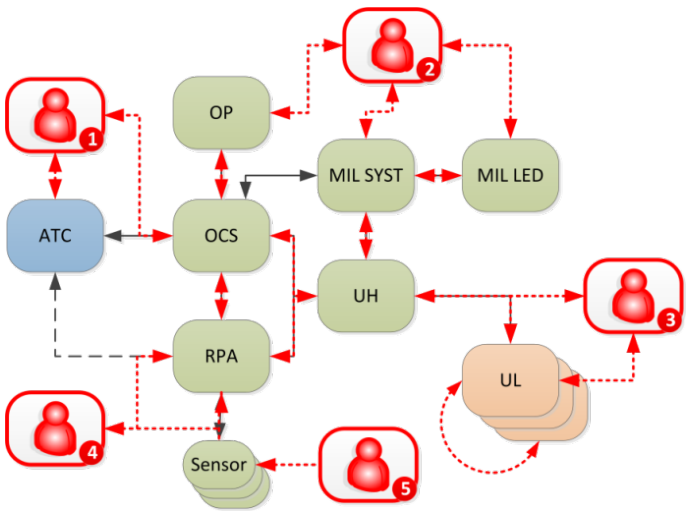
Tillgångar är allt som är värdefullt för en verksamhet. I cybermiljön kan tillgångar vara antingen fysiska eller virtuella. För RPAS är RPA:n och operatören exempel på fysiska tillgångar medan sensordata och navigationsinformation exempel på virtuella tillgångar. Detta gör att tillgångar kan vara väldigt olika artefakter såsom information, mjukvara och hårdvara men även tjänster som förmedlas inom RPAS samt ingående personal.

Det är svårt att i en översiktlig rapport som den här ge en detaljerad bild över tillgångar. Exempel på tillgångar kommer dock att tas upp i nästkommande avsnitt (4.5) i samband med att hotbilden för identifierade aktörer analyseras.

4.5 Hotanalys

Figur 7 i föregående avsnitt identifierade ett antal aktörer vilka ingår i ett RPAS. Dessa aktörer kan vara producenter av information eller tjänster eller konsumenter. Exempelvis producerar RPA:n sensordata till det militära ledningssystemet och samtidigt konsumerar RPA:n styrdata från operatören via kontrollstationen.

Alla gränsytor där ett delsystem kan kommunicera med omvärlden eller där det är möjligt att rent fysiskt komma i kontakt med systemkomponenter är riskytor för angrepp (figur 11). Att det finns en riskyta är dock inte det samma som att en angripare kan genomföra ett framgångsrikt angrepp utan större ansträngning. Det krävs både kunskap och förberedelser för att lyckas med ett angrepp.



Figur 11. Riskytor för RPAS.

Det är svårt att uttrycka några specifika hot mot RPAS med en så generisk systembeskrivning som ges i figur 11. Några tänkbara hot kan dock vara:

- *Angrepp mot militära system*: Angripare 2 har förmåga att påverka operatören och få denne att (sannolikt) omedvetet föra in skadlig kod i kontrollsystemet (OCS), se avsnitt 4.5.1 nedan. Ett alternativ för angripare 1 är att påverka någon i den militära ledningen som har möjlighet att föra in skadlig kod i ledningssystemet (MIL SYST) om inte vägen via underhållssystemet varit framgångsrik.
- *Angrepp via stödfunktioner*: Det finns funktioner i RPAS som systemägaren inte har kontroll över men är beroende av. Exempelvis kan

angripare 1 infiltrera det civila flygledningssystemet (ATC) för att därigenom påverka en RPA. Angripare 3 väljer istället att infiltrera underleverantörer eller underhållsfunktionen (se avsnitt 4.5.2 för ett verkligt exempel) i syfte att föra in egenmanipulerade komponenter i RPA:n.

- *Angrepp mot RPA*: Angripare 4 har kommit över kryptoutrustning som möjliggör direktkontakt med RPA:n. Alternativt har angriparen identifierat en svaghet i RPA:ns interna kommunikation vilket gör att kontrollmeddelanden till styrsystemet kan skickas visa RPA:ns sensorer.
- *Angrepp mot sensorsytemen*: Angripare 5 har inte förmåga att påverka själva RPA:n men har fått reda på ett svaghet i ett av COTS-sensorsystemen. Svagheten gör att angriparen kan dölja sig för sensorn och därmed vilseleda den militära ledningen.

De angrepp som presenterats här är i huvudsak teoretiska. Riskytor är dock en realitet. Nedan visas två exempel på hur riskytor som en användare förbiser kan användas för angrepp.

4.5.1 Angrepp via operatören

En operatör har en dator hemma som hela familjen använder samt ett trådlöst nätverk för mobila enheter. En militär enhet beslutar sig för att genomföra ett riktat angrepp mot operatören med målsättningen att kunna infiltrera RPAS kontrollsystemet. Enheten skapar en uppsättning fiktiva identiteter på den sociala webbtjänsten Facebook och utger sig för att vara barn i samma ålder som operatörens egna barn. De lyckas över en tid på flera månader att bli vänner med operatörens familj och lurar ett av barnen att ladda ner ett spel på familjens dator. Detta spel innehåller ett IT-vapen (ett program med syfte att angripa IT-system) som dolt sprider sig mellan de olika enheterna i familjens hemmanätverk. IT-vapnet lyckas så småningom ta sig över till operatörens smartphone när denne surfar på internet över hemmanätverket. Operatören bär med sig sin smartphone på arbetet för att kunna ring privata samtal men arbetsplatsen saknar trådlöst nätverk då externa anslutningar inte är tillåtna.

En dag upptäcker operatören att han har ont om batteri i sin smartphone och ansluter den till sin OCS via ett USB-uttag för att ladda telefonen. Vapnet propagerar då in i OCS:en.

Bakgrunden till exemplet kommer från (Leyden 2011). 2011 upptäcktes ett virus på vapen- och sensorstationerna till Reaper-RPA:er i USA. Viruset i fråga sprids endast genom spelet Mafiawars som spelas på Facebook. Hur viruset kommit in i stationerna har aldrig förklarats då OCS:erna inte får anslutas till internet.

4.5.2 Angrepp mot kryptering av kommunikation

Ett företag som tillverkar datorchip för vidare försäljning till tillverkare av datorutrustning gör efter påtryckning från en myndighet förändringar i några av de logiska grindar som ett chip består av. En av företagets kunder tillverkar kommunikationsutrustning som används i RPA:er. Vid en uppgradering av RPA:ns kommunikationsutrustningen överförs ett modifierat datorchip med ett kretskort.

Det modifierade chipet påverkar slumptalsgeneratorn för kryptoutrustningen så att endast en 32 bitars variation av slumptalen uppnås istället för det specificerade 256. Resultatet av angreppet är att krypteringen med lätthet kan forceras av angriparna och all kommunikation mellan RPA:n och operatörsstationen kan avlyssnas. Angreppet går sannolikt obemärkt förbi då det inte finns något sätt att detektera sabotaget utan att på egen hand utföra ett forcerat angrepp på den egna kommunikationen.

Bakgrunden till exemplet kommer från en rapport (Becker, Regazzoni, Paar & Burleson, 2013) om hur hårdvarumodifieringar på chip-nivå kan påverka systemsäkerhet.

4.6 Prognoserat nyttjande av RPAS 2030

De prognoser för framtiden som avser RPAS rör främst den funktionalitet som förväntas finnas och hur den skall utnyttjas. Det är sällsynt att frågor rörande cybersäkerhet tas upp specifikt annat än att kommunikationskanaler förväntas vara säkra. Några egenskaper förtjänar dock att lyftas fram ur ett cybersäkerhets-perspektiv. Det bör också påpekas att i detta avsnitt betraktas RPAS som en generisk grupp. I realiteten är det stor skillnad i förmåga på olika typer av RPAS.

Nyttan med RPAS är redan nu tydlig och utvecklingen på både den militära och civila marknaden går fort. Utvecklingen gör att RPAS förväntas vara fullt integrerad med civil flygtrafik (U.S. Army 2010) innan slutet av analysperioden. Sammankopplingen av militära och civila flygsystem är i sig inget nytt då stridsflygplan genom tiderna har fått anpassa sig efter civila regler. RPAS förväntas dock ha en hög grad av autonomitet vilket är något som dagens förarbaserade flygplan inte har. Ett mer eller mindre autonomt flygsystem måste kunna ta emot styrning från civil flygkontroll utan att en operatör skall behöva ingripa. Ur ett cybersäkerhetsperspektiv innebär det att en extern aktör med en annan säkerhetsmålsättning delvis kontrollerar flygsystemet. Ägaren av autonoma flygsystem måste utveckla metoder för att säkerhetsställa att den civila kontrolltrafiken är autentisk och opåverkad av en angripare.

Den förväntade graden av autonomitet varierar, främst beroende på vilken tillämpning av RPAS som avses. Exempelvis anses rutinmässiga uppgifter, såsom spaningsuppdrag, kunna ske autonomt medan mer specialiserade och oförutsägbara uppdrag som evakuering av skadade kräver mänsklig kontroll (U.S. Army 2010). RPAS med en hög grad av autonomitet behöver kunna ta emot militär ledning under pågående uppdrag. Kommunikation av uppgifter och kontroll måste skyddas och bör helst kunna utvärderas. Förmågan att bedöma rimligheten i kontrollmeddelanden ger systemet en robusthet och därmed ett högre skydd mot angrepp över kontrollkanalen.

RPA:s förväntas även kunna kontrolleras som en grupp av en operatör, jämfört med nuläget där en operatör kontrollerar en RPA (Tocher & Wiedemann 2011). En grupp RPA:er utgör en svärm vilket ställer krav på att en RPA kan på egen hand läsa av och förstå sin omgivande miljö. En annan form av autonomitet är en RPA som utgör en lojal rotekamrat (eng. loyal wingman) (U.S. Air Force 2009). Som en lojal rotekamrat kan en RPA utföra spaningsuppdrag åt ett bemannat flygplan eller vara en vapenplattform vilket ger en pilot en högre verkningsgrad. Samspelet mellan flygande system i svärm eller par ger en ny situation där farkoster måste kunna anpassa sig efter varandra. Det är rimligt att anta att en sådan förmåga kräver ett starkt skydd mot telekrigsoperationer. En hög medvetandegrad av det egna systemet innebär ur ett cyberperspektiv att systemet behöver ha hög tilltro till sina sensorer.

Oavsett hur den ökade autonomiteten används förs mer beslutförmåga över till RPAS. En mänsklig operatör förväntas fortfarande finnas kvar i beslutsloopen (Försvarsmakten 2013) men med hög autonomitet blir uppgiften mer att övervaka än att styra.

Det finns ett önskemål om att RPA:er skall kunna kontrolleras genom ett gemensamt gränssnitt. Fördelen med ett gemensamt gränssnitt är förstås att minska behovet av unika plattformar för olika typer av RPAS, men det finns även en tanke om att kunna flytta kontrollen av en RPA mellan olika operatörer (DOD 2007). Ett sådant önskemål ställer stora krav på kommunikations-lösningen, exempelvis vad avser kryptering och hantering av krypteringsnycklar.

Farhågor rörande outsourcad utveckling av cybersystem i allmänhet men även integrationsproblem beroende på komplexa system är något som tas upp (U.S. Navy 2012). Militära system består i stor utsträckning av kommersiella komponenter. Beroende på var dessa komponenter är tillverkade finns det risk för att de kan levereras med inbyggda svagheter vilket gör hela RPAS sårbart.

4.7 Sammanfattning

Ett cyberangrepp är inget angrepp som sker slumpmässigt och utan förberedelser. För att lyckas med ett angrepp måste det finnas en svaghet i ett system och angriparen måste känna till hur svagheten kan utnyttjas. Kvalificerade angripare har förmåga att via underrättelseinhämtning inhämta kunskap om hur system är konstruerade och därefter identifiera svagheter i systemen medan mindre kompetenta angripare får använda de verktyg som finns tillgängliga. Det finns ett fåtal aktörer som dessutom har möjlighet att föra in egna svagheter när komponenter tillverkas. Svagheter kan även uppstå under drift genom att uppdateringar av mjukvara inte kontrolleras ordentligt. Uppdateringar är även ett verktyg för angripare då den kan identifiera vilken svaghet som uppdateringen åtgärdar. Med den kunskapen kan angriparen attackera system som inte har uppdaterats.

Statistik visar att svagheter är vanliga i nästan alla IT-system. Utmaningen för en angripare är att först förstå hur ett målsystem är uppbyggt och därefter identifiera svagheter i detta system. När väl en svaghet identifierats och ett verktyg för att utnyttja svagheten har konstruerats är det avsevärt enklare för en mindre begåvad angripare att använda ett sådant verktyg. Effekten av ett cyberangrepp är svår att bedöma både för angripare och för systemägare. Det beror på vilka skydds-åtgärder som vidtagits i övrigt.

Angriparens förmåga, tillgång till verktyg samt motivation gör risken för cyberangrepp och dess effekt svårbedömd. Gemensamt för förutsättningarna är dock att det krävs förberedelser. Ett cyberangrepp mot ett specialiserat system som RPAS sker inte i stundens ingivelse vilket är möjligt med kinetiska vapen.

En viktig lärdom när det gäller cyberangrepp är att de inte är frontangrepp. Det tar tid från det att en svaghet uppmärksammas till dess den kan utnyttjas och effekt kan uppnås. Den önkade effekten kan dessutom uppnås på flera ställen i ett fjärrmanuvrerat system. Ett angrepp mot operatören eller mot kontrollsystemet kan mycket väl ge den effekt som önskas som om RPA:n angreps direkt. En angripare kommer att utnyttja den vägen som är tillgänglig och enklast för att uppnå angriparens mål. Cyberangrepp är oftast en långsam process med noggranna förberedelser och osäker utgång..

Mängden RPAS kommer inte att minska i framtiden och de kommer inte enbart att finnas i militärt avgränsade luftrum. Framtida RPAS kommer att ha en högre grad av autonom förmåga vilket ställer höga krav på pålitlighet. En tydlig hotanalys av RPAS miljö där alla aktörer ingår och noggranna kontroller av ingående komponenter är en förutsättning för en minskad risk för framgångsrika cyberangrepp.

5 Artificiell intelligens för säkerhet i RPAS

5.1 Mål och begränsningar

Detta kapitel fokuserar på hur autonoma funktioner kan användas för att öka säkerheten i RPAS speciellt med avseende på antagonistiska hot som till exempel cyberattacker. Denna begränsade syn på hur maskinintelligens kan användas i obemannade system är definierad i projektets mål och betyder inte att författaren till detta avsnitt tror att detta är den enda eller den mest betydelsefulla användningen av autonomi i obemannade system på tjugo års sikt.

En bred trend i dagens teknik och samhälle är att maskinintelligens av sociala-, ekonomiska- och säkerhetsskäl tar över fler och fler uppgifter. Sociala skäl för införande av artificiell intelligens handlar ofta om att det anses etiskt oskäligt eller praktiskt omöjligt att använda människor för monotona eller farliga uppgifter. Det finns alla skäl att tro att denna utveckling kommer att fortsätta och accelerera så att framtida obemannade system har ett stort och ökande inslag av artificiell intelligens medan människors uppgifter förflyttas till allt högre kognitiv nivå och alltmer handlar om strategiska avgöranden och framför allt beslut om vad vi i grunden vill och tycker är rätt.

Termen autonomi är omdebatterad och föremål för många tolkningar. I fortsättningen kommer vi att diskutera hur intelligent mjukvara kan hjälpa, komplettera, samarbeta med, leda och ibland helt eller delvis ersätta mänskliga operatörer, analytiker och beslutsfattare. Sådan mjukvara kan ha intelligens på en nivå som spänner över mycket enkel till mycket avancerad. Vi kommer att använda termen artificiell intelligens (AI) för alla sådana intelligenta funktioner oavsett intelligensnivå och oavsett i vilken grad funktionen assisterar, kompletterar, samarbetar med, ersätter eller leder människor.

Huvudinriktningen i forskningen om AI för obemannade farkoster är inriktad på avancerade intelligenta delfunktioner, AI med robust situationsuppfattning och samarbetande autonoma farkoster. På policynivå beskrivs detta perspektiv av USA Department of Defense (2012). Ett representativt arbete i denna forskning är Tian et al. (2012) som beskriver forskningsläge och en högnivåarkitektur. Det finns all anledning att tro att stora framsteg kommer att göras inom allmän autonomi för obemannade farkoster de närmaste tjugo åren men det är inte ämnet för detta kapitel som enligt projektmålen fokuserar på AI för ökad säkerhet i väsentligen fjärrstyrda flygplan - RPAS.

5.2 Litteraturstudier

Det finns inte någon specifik gren av forskningslitteratur som handlar om AI för RPAS-säkerhet. Här beskrivs utvalda resultat från litteraturstudier i några angränsande relevanta områden som är värda att följas av den som intresserar sig för RPAS-säkerhet.

5.2.1 Cyberfysiska system

Cyberfysiska system (cyber-physical systems) är en term som på senare år har börjat användas för att beskriva samverkande system som omfattar både fysiska- och informationselement. Denna breda definition omfattar rymd, flyg, transport, SCADA, medicinska och många andra system inklusive obemannade flygande farkoster. Litteraturen om säkerhet och cybersäkerhet i cyberfysiska system är omfattande (se Das, Kant & Zhang (2012) för en introduktion). Av speciellt intresse för RPAS-säkerhet är forskningen om säker IT-infrastruktur för allt mer autonoma och uppkopplade bilar och lastbilar (se till exempel Nilson & Larson (2009).

Det finns goda möjligeter av att dra nytta av erfarenheterna från andra cyberfysiska system i arbetet med att öka säkerheten för RPAS. Inom telekirurgi utvecklas till exempel Secure ITP som innebär utökad säkerhet i Interoperable Telesurgery Protocol (ITP). Stöd för auktorisering, autentisering och väldefinierade policys och roller implementeras bland annat med tanke på framtida användning av telekirurgi i svåra miljöer som t.ex. på slagfält. Säkerhetskraven för telekirurgi liknar i mycket RPAS-kraven och det förefaller som teknikutvecklingen här har nått längre (se till exempel Lee & Thuraisingham). I sektion 5.6.5 beskriver vi resultat från litteraturen om cyberfysiska system beträffande vi vetoövervakning på realtidsnivå (Mohan et al. (2013). Fördjupade litteraturstudier inom cyberfysiska system har förutsättningar att ge många relevanta insikter.

5.2.2 Intrångsdetektion

AI används för att öka förmågan hos *intrusion detection systems* (IDS) (Scarfone & Mell, 2007) som är system avsedda att upptäcka digitala intrång i informationssystem. AI-tekniker som används är ofta klassificeringsmetoder som artificiella neuronnät eller supportvektormaskiner (Kumar, Kumar & Sachdeva, 2010). Det finns två viktiga klasser av metoder: signaturbaserade och anomalibaserade. De förra bygger på bibliotek av intrångsignaturer och AI som generaliserar från denna kunskapsbas medan den senare bygger på att AI lär sig en normalbild och varnar för anomalier som avviker från normalbilden. Mitchell

& Chen (2013) ger en översikt över intrångsdetektion i cyberfysiska system utan att direkt fokusera by AI-metoder.

Vi har inte hittat någon litteratur som direkt handlar om intrångsdetektionssystem ombord på en RPA. Mitchell & Chen (2013) beskriver ett IDS för att utifrån övervaka en RPA vilket vi återkommer till i sektion 5.6.4. Lauf & Robinson (2010) beskriver kortfattat hur ett intrångsdetektionssystem kan skydda en grupp av obemannade farkoster som bildar ett mobilt ad-hoc-nätverk. Denna typ av intrångsdetektion är dock begränsad till just noder i ett mobilt nätverk och omfattar inte några andra aspekter eller funktioner i RPAS.

5.3 AI för säkerhet

Hur kan man använda AI för att göra system säkrare? AI är automatiserad intelligens så vi kan börja med att fråga oss hur man kan använda intelligens för att göra ett system säkrare för att senare återvända till frågan om hur intelligens kan automatiseras. Intelligens är förmågan att använda kunskap för att uppnå sina mål så analysen av hur intelligens kan användas för att göra system säkrare kan börja med att undersöka vad det finns för källor till kunskap. Kunskap finns ofta antingen som regler eller som erfarenhet. Exempel på regler är fysikens lagar som ingenjörer tillämpar. Exempel på erfarenheter är de samlingar av historiska rättsfall som jurister använder. Ibland kan den som vill göra sitt system säkrare öka kunskapen om regler genom forskning. Ofta går det att öka sin erfarenhet genom experiment och träning.

Om de regler som styr genomförandet av en uppgift är helt kända är det i princip möjligt att bygga en automatiserad intelligent agent som löser uppgiften autonomt, som hjälper en operatör att genomföra uppgiften eller som övervakar andra system eller operatören och ingriper om något går fel. Eftersom människor är mindre pålitliga än maskiner när det gäller att tillämpa exakta algoritmer är i detta fall autonom AI säkrare än operatörer eller operatörer med stöd av AI. Exempel på regelstyrda uppgifter är att planera flygbanor som minimerar bränsleåtgång eller de monteringsuppgifter som utförs av traditionella industrirobotar. I båda fallen är miljön väl väldefinierad och avgränsad och de regler som styr genomförandet av uppgiften är väl förstådda tekniska förhållanden och kända naturlagar.

Industriroboten kan montera i mycket större hastighet och med mycket större säkerhet och precison än vad som är möjligt för människor. Typiskt står dagens robotar i en bur som skyddar människor för att av misstag komma in i robotens arbetsområde. Buren är till för att garantera att miljön är förutsägbar för roboten som inte är konstruerad för att hantera situationer där människor oväntat dyker upp i arbetsområdet. Om något som inte omfattas av de regler som styr roboten

inträffar i robotens arbetsområde är systemet inte längre säkert. En ny generation av industrirobotar som kan jobba nära människor på ett säkert sätt är för övrigt på väg ut på marknaden.

Om det finns dokumenterade erfarenheter av de situationer som systemet ska hantera kan intelligenta agenter, operatörer eller AI, tränas med hjälp av erfarenheterna. Oftast går det att genomföra träningen i en virtuell eller annan ofarlig miljö. Misstag under träning kan styra den fortsatta träningen så att ökad erfarenhet av speciellt svåra eller farliga situationer prioriteras. Människors överlägsenhet när det gäller att lära sig av erfarenheter beror dels på att människor har tränats på liknande situationer under ett långt liv dels på att människor har inbyggda förmågor som tränats av evolutionen. Att en människa snabbt kan lära sig att köra bil beror på att förmågan att förflytta sig till fots redan finns. En maskin måste t.ex. lära sig att känna igen gator, bilar, fotgängare och förstå hur dessa uppträder. Att en människa snabbt kan lära sig att spela handboll beror bland annat på att det finns ett av evolutionen inbyggt program för att fånga saker i luften. Robotar som ska spela bollspel måste programmeras med mjukvara som känner igen bollar, lagar som styr kastbanor och komplexa metoder för att styra robotens servomotorer.

Artificiell intelligens kan överglänsa människor när det som ska tränas in inte stämmer med människans repertoar av erfarenhet och inbyggda förmågor. Fingeravtrycksigenkänning har t.ex. automatiserats med stor framgång. För att hitta ett matchande fingeravtryck i en stor databas jämför AI många små detaljer i fingeravtrycken. Människor ser spontant bara det övergripande mönstret i fingeravtryck och kan bara jämföra de fina detaljerna med koncentrat, mödosamt och långsamt arbete. Artificiell intelligens kommer under de kommande åren att tränas för att hantera fler och fler erfarenhetstyrda mänskliga förmågor. En faktor som dramatiskt skiljer sig mellan mänsklig- och maskinintelligens är att varje människa måste tränas separat medan inträned AI-förmåga kan på ett ögonblick kan kopieras från en maskin till en annan. Maskininlärning fungerar på ett fundamentalt annorlunda sätt än mänsklig utbildning och träning just genom att en gång inträned förmåga blir en allmän tillgång som kan sparas och kopieras obegränsat.

I situationer där vi vill uppnå hög säkerhet ser vi ofta till att en grupp av människor stödjer varandra i att bedöma situationer och ta beslut. Trafikpiloter och kärnkraftsoperatörer arbetar t.ex. inte ensamma. Även en mycket erfaren människa kan missförstå en situation och göra allvarliga felbedömningar. I en grupp kan andra upptäcka och påpeka misstag vilket ökar säkerheten. Forskning visar att säkerheten är lägre i auktoritära och hierarkiska organisationer där underordnade inte vågar ifrågasätta en överordnads bedömning (Fischer & Orasanu, 2000). Auktoritär organisation kan ha andra fördelar i beslutsfattande men säkerheten i besluten är inte optimal.

Om artificiell intelligens ingår i en grupp av intelligenta system som verkar i samma miljö talar vi om ett multiagentsystem. Agenterna kan vara maskiner eller människor. AI-agenter av olika typ eller med olika träning kan bilda en grupp som gemensamt löser en uppgift. Om uppgiften handlar om att klassificera en situation kallas detta för boosting (se Schapire (2002) och Zhou, (2012) för introduktioner; experter bör vara medvetna om tekniska problem med vissa metoder (Long & Servedio (2010). Ett enkelt sätt att använda gruppen är att alla agenterna föreslår tolkningar eller lösningar varefter beslutet fattas genom någon form av viktad omröstning. Majoritetsval är en möjlighet men om det viktiga är att undvika misstag kan även veto-system användas där det räcker att en agent motsätter sig ett beslut. Skyddsombud kan till exempel stoppa arbetet i en fabrik eftersom man här prioriterar säkerhet högre än produktionseffektivitet. Ökad säkerhet uppnås om agenterna kan argumentera för sin ståndpunkt och låta andra agenters argument påverka den egna ståndpunkten. Om andrepiloten upptäcker att förstepiloten har missförstått situationen kan han eller hon förklara varför och därmed hjälpa förstepiloten att verifiera att ett misstag var på väg att begås (Fischer & Orasanu, 2000). Vissa typer av AI-agenter har också förmågan att förklara sina ståndpunkter vilket i framtiden kommer att ha stor betydelse för säkerhet i multiagentsystem där korrekt och gemensam situationsuppfattning är viktig.

Multiagentsystemet måste vara robust mot störd kommunikation och agenter som plötsligt tappar hela eller delar av sin förmåga. Sådana problem kan bero på fysiska skador, telekrigsinsatser, cyberangrepp eller fel i programvara. På samma sätt som andrepiloten kan ta över från en sjuk förstepilot måste AI-agenter ha förmåga att anpassa sig till och kompensera för skador på systemet. Ett sådant system ger robust säkerhet i flera lager där till exempel en lyckad cyberattack tränger igenom ett första lager av krypterad kommunikation och brandväggar men upptäcks via automatisk intrångsdetektion så att agentsystemet kan omorganisera sig till försvar mot intrånget och kompensation för de skador som har uppstått.

Ledning och styrning av RPAS sker nästan alltid i team med roller som pilot, sensoroperatör, bildtolk, underrättelseanalytiker och chef. Hur kan AI öka säkerheten i detta multiagentsystem? Vi ser tre viktiga roller som i det följande definieras och exemplifieras utan avsikt att vara utömmande i exemplen.

A. AI för handling
   a. AI-agenter tar över vissa moment i styrningen eftersom just dessa moment utförs säkrare av maskiner. Till exempel landar vissa RPA idag autonomt eftersom manuell landning innebär högre risk.
   b. När människor inte finns tillgängliga för att utföra en uppgift kan AI ta över och lösa uppgiften – möjligen på ett mindre säkert eller effektivt sätt än människor men ändå bättre än att stå utan styrning. Dagens

RPA kan till exempel övergå till ett säkert autonomt beteende om sambandet till operatören inte fungerar.

B. AI för perception
   a. AI-agenter kan stödja teamet med varningar och förslag. Automatisk objektigenkänning i spaningsbilder kan till exempel redan idag uppmärksamma en bildtolk på ett misstänkt objekt och till exempel föreslå att det är ett fartyg av en viss typ.
   b. AI kan övervaka människor och till exempel varna när operatörens förmåga sviktar. Människors förmåga avtar både när de är för stressade och när de är för uttråkade. Människor karaktäriseras också av mycket begränsad självinsikt i sin egen förmåga. En generell trend är att människor i allt högre utsträckning övervakas av intelligenta maskiner bland annat av säkerhetskäl. Den snabba utvecklingen av psykofysiska sensorer som ögonskanners och hjärnskanners ger stora möjligheter att utveckla sådana system.
   c. AI-agenter kan övervaka varandra. Datorprogram påverkas negativt av till exempel överlastade beräkningsplattformar, chokade kommunikationssystem och cyberangrepp. Felfungerande agenter inser ibland inte sitt tillstånd. Ett system av AI-agenter som övervakar varandras tillstånd är säkrare än system som saknar sådan social kontroll.
C. AI för beslutsfattande
   a. AI-agenter kan fungera som ett skyddsombud som stoppar farliga åtgärder och tvingar in systemet i ett säkrare tillstånd. Både människor och maskiner kan övervakas på detta sätt även om det är känsligt och ibland svårt att få acceptans för att maskiner kan ge veto mot människor. Krockkuddarna i en bil är ett exempel på allmänt accepterat vetosystem där maskinen i extrema situationer tar ifrån föraren kontrollen över fordonet genom en tvingande säkerhetsåtgärd.
   b. Delegering är en viktig form av samarbete. Idag kan operatörer delegera till AI – till exempel att flyga mellan vägpunkter. I framtiden kommer det att bli allt vanligare att AI delegerar till människor vilket idag redan sker i tjänster som till exempel Amazons Mechanical Turk.

RPAS inkluderar farkoster, marksystem och de människor som opererar systemet. Vi är här intresserade av den kognitiva aspekten på systemet det vill säga den del som handlar om kunskap och kunskapshantering. Det kognitiva systemet ses som ett multiagentsystem bestående av både människor och AI-agenter. När vi ovan analyserade AI-funktioner för RPAS-säkerhet fann vi en naturlig uppdelning efter de viktiga kognitiva funktionerna handling, perception och beslutsfattande. I de följande tre sektionerna presenteras exempel på

intelligenta funktioner för var och en av dessa kategorier med fokus på en i sammanhanget viktig form av AI för beslutsfattande - vetoövervakning.

5.4 Autopiloter – AI för handling

Flygning med autopilot inklusive start och landning har varit tekniskt möjligt åtminstone sedan 1947 (Okänd, 1947). Sedan länge har autopiloter automatiskt och med hög precision och säkerhet kunnat kontrollera farkostens styrytor och motorer. Att hålla kurs och höjd, ändra höjd, flygning mellan inplanerade vägpunkter och landning hanteras av de flesta moderna autopiloter på större flygplan (Federal Aviation Administration, 2013). Start under autopilot används sällan men är tekniskt möjligt och stöds av vissa autopiloter. Bemannat flyg startar från hangarfartyg utan pilotens inblandning och autolandning på hangarfartyg testades med F18 i slutet på 90-talet (Mårtensson, Hultgren & Bull, 2013). Autopiloter för RPA har samma förmågor som de för bemannat flyg (se Chao, Cao & Chen, 2010 för en översikt över autopiloter för mindre obemannade flygplan och Micropilot, 2013 för ett exempel). Standardfunktioner i autopiloter för RPA inkluderar dessutom att autonomt återvända till hemmabasen eller till startpunkten. Autopiloter använder tillgängliga navigationshjälpmedel (satelliter, flygledning, tröghetsnavigering) utan att människor behöver agera mellanhand.

När identitet, position och kurs för relevanta mål väl är fastställt och uppdragets mål är formulerade på ett maskinläsbart språk kan AI banplanera lika effektivt eller effektivare än människor. AI överglänser oftast människor om många kvantitativa faktorer ska optimeras samtidigt som till exempel när det är viktigt att flyga bränslesnålt eller då flera farkosters bana ska planeras samtidigt för att lösa ett gemensamt mål. Fokus för den fortsatta utvecklingen av autopiloter är bättre situationsuppfattning baserad på information från farkostens sensorer och underrättelser via extern kommunikation och därmed en utökad förmåga att lösa komplexa uppgifter självständigt. Begränsad förmåga av denna typ finns redan. RPAS Raven kan till exempel autonomt flyga i en bana som där den övervakar ett utpekat mål på marken. Förmågan att med radar eller optiska sensorer upptäcka och undvika kollision med flygande föremål är under utveckling och kommer troligen att bli tekniskt tillgänglig inom de närmaste fem åren. Sådan sense-and-avoid förmåga är kritisk för att obemannade farkoster ska tillåtas i civilt luftrum.

Förmågan att från sensordata och underrättelser skapa en relevant situationsbild – perception – är det som fundamentalt är svårt och kräver fortsatt forskning. Mänsklig perception är oftast bättre och robustare vilket gör att piloter klarar oförutsedda situationer som autopiloten inte kan hantera. AI för perception diskuteras kortfattat i nästa sektion.

Autopiloter kan med känd teknik öka säkerheten i RPAS genom att autonomt styra farkosten i situationer där fjärrstyrning inte är tillgänglig till exempel på grund av brister i radiosamband, cyberangrepp eller operatörens förmåga. Idag kan autopiloter utföra väldefinierade policys som till exempel att återvända till bas, fortsätta planerad bana, planera och följa en bana i syfte att återställa radiosamband eller övervaka ett utpekat mål. I ett tjugoårsperspektiv kommer avancerad perception att integreras med autopiloter vilket kommer att möjliggöra ytterligare säkerhetsfunktioner inklusive autonom sense-and-avoid förmåga.

5.5 AI för perception

Perception är en mycket stor del av forskningen om AI vilket gör att det inte är möjligt att inom ramen för denna rapport ge en översikt. Perceptionsproblemet går under många olika namn och inriktas mot olika tillämpningar i olika grenar av forskningen. Perception handlar om att använda sensorinformation för att förstå vad som händer i omgivningen. Traditionellt brukar det som kallas perceptionsforskning ofta handla om perception i biologiska system eller om artificiella system som är inspirerade av biologisk perception. Generisk forskning om perception i AI kallas ofta för mönsterigenkänning (Pattern Recognition). FOI har nyligen gjort en översikt över metoder för att automatiskt känna igen meningsfulla objekt i bilder (Content-Based Image Retrieval) vilket är ett viktigt delområde av mönsterigenkänning (Ahlberg et al. (2011). När fokus är på att använda information från flera sensorer av samma eller olika typ kallas forskningsområdet ofta fusion, datafusion, sensorfusion eller informationsfusion. När fusion används för att uppnå övergripande förståelse av en situation kallas det ibland Situation Assessment. När taktisk militär tillämpning är det centrala kallas perception ofta automatisk måligenkänning (Automatic Target Recognition).

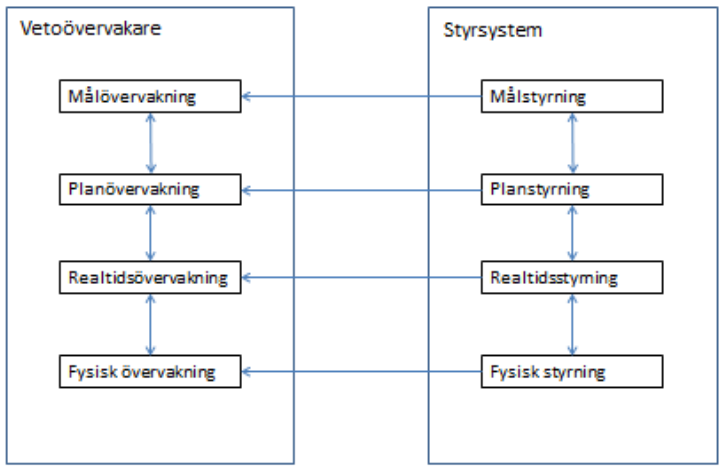
5.6 Vetoövervakning – AI för beslutsfattande

Säkerheten i RPAS kan ökas med en autonom intelligent övervakningsfunktion som i nödlägen kan ta kontroll över farkosten. En sådan funktion kallas en vetoövervakare och måste för att vara effektiv mot cyberangrepp köra på en separat processor och i övrigt vara så isolerad från övriga system som möjligt. Operatörskonsolen skulle kunna ha ett separat övervakningssystem som på samma sätt varnar för cyberattack eller för allvarliga operatörsfel. Även om en vetoövervakare inte utlöser skyddsmekanismer kan övervakningen stödja forensisk analys av incidenter med viktig information. Därför bör vetoövervakarna logga och regelbundet kommunicera loggar till basen.

Notera att vi i denna rapport enlig projektets målsättning fokuserar på AI för säkerhet i RPAS som opererar i fred eller i ett skymningsläge. I strid är det givetvis ofta så att säkerhet inte går att uppnå genom höga trösklar mot misstag utan att förmågan till snabba beslut som ibland innebär högt risktagande är viktig både för förmågan att utföra uppdraget och för systemets överlevnad.

5.6.1 Arkitektur för vetoövervakning

Vetoövervakning innebär att AI övervakar ett RPAS och initierar nödåtgärder vid behov. Övervakningen kan ske på flera olika systemnivåer vilket illustreras i figur 12.



Figur 12. Hierarkiska vetoövervakare och styrsystem

Vi förutsätter att det finns ett styrsystem som inkluderar både operatörer och automatiska funktioner. Funktionerna i detta system kan indelas i,

1) *Fysisk styrning* till exempel av motoreffekt eller av farkostens kontrollytor.
2) *Realtidstyrning* där specialiserade processorer regelbundet övervakar och styr väl avgränsade funktioner. En processor kan till exempel med jämna tidsintervaller läsa av temperaturen i motorutrymmet och aktivera eldsläckare om brand indikeras.
3) *Planstyrning* där systemet följer en given plan som till exempel när autopiloten styr mellan vägpunkter.

4) *Målstyrning* där systemet försöker utföra ett uppdrag som till exempel att spana mot ett utpekat mål.

Vetoövervakaren har samma hierarkiska indelning som styrsystemet där varje funktionell nivå i styrsystemet motsvaras av en funktionell nivå i vetoövervakaren. I de följande sektionerna går vi in på detaljerna i och exemplifierar varje nivå av vetoövervakning. I en avslutande sektion diskuteras hur de olika övervakningsnivåerna kan samverka och integreras.

Vetoövervakaren har en övergripande beslutsfunktion som får information om anomalier som upptäcks på de olika funktionsnivåerna och tar beslut om åtgärder. Vi förutsätter att det finns ett separat underhållssystem som hanterar mindre felfunktioner som t.ex. att koppla bort en felaktig sensor eller starta om en mikroprocessor som har hängt sig (fault detection and diagnosis system). Det förutsätts också att det finns mekanismer som hanterar kortare kommunikationsstörningar där en autopilot håller kurs och flyger mellan inprogrammerade vägpunkter i väntan på att radiokanalen ska öppnas igen. Syftet med vetoövervakaren är att upptäcka och hantera rena nödlägen som när styrkanalen har tagits över av en motståndare eller normala styrsystem är korrumperad av cyberangrepp. Vid sådana nödlägen kan vetoövervakaren vidta åtgärder till exempel enligt följande,

1) Starta om styrsystemet.
2) Öppna en reservkanal till operatören.
3) Stänga av det korrumperade styrsystemet och aktivera ett reservsystem.

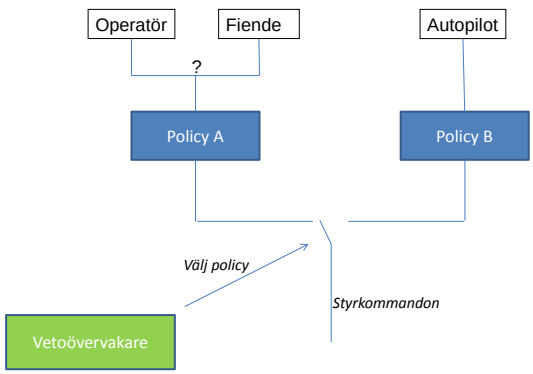
För att vetoövervakaren och andra reservsystem inte ska korrumperas av samma cyberangrepp som har slagit ut huvudsystemet måste dessa säkerhetskritiska delar i möjligaste mån isoleras, köra på separat hårdvara och helst kopplas med separata länkar till sensorer och operatörer. Eftersom autopilotfunktioner behövs även i normal drift kan övervakningssystemet inkludera en extra autopilot som reserv för nödlägen.

5.6.2 Vetoövervakning som icke-stationärt tvåarmadbanditproblem

Figur 12 visar en konceptuell arkitektur där det ombord på farkosten finns en autonom funktion - Vetoövervakaren - som detekterar och hanterar nödlägen som inte operatören har någon möjlighet att upptäcka eller åtgärda. Från AI-litteraturen känner vi problemet som ett icke-stationärt tvåarmadbanditproblem. Fördelen med att på detta sätt identifiera problemtypen är att vi i den fortsatta forskningen kan tappa av den litteratur som finns om problemtypen.

Det mångarmade banditproblemet handlar om att välja vilken av flera möjliga policyer som ska styra. Effekten av att låta en given policy styra är inte möjligt att förutse i detalj men det finns erfarenheter av hur olika policyer har styrt tidigare. Situationen påminner om att i en spelhall välja vilken enarmad bandit man ska spela på. Vissa enarmade banditer kan ha bättre vinstchanser än andra. Genom att pröva olika banditer kan spelaren så småningom bygga erfarenheter som gör att de bästa banditerna kan identifieras. Vinstplanen i varje bandit kan ses som en inbyggd policy. I sin generella form handlar det mångarmade banditproblemet om att balansera risken av att utforska okända policyer mot fördelen av att lära sig mer och därmed bättre kunna bedöma vilken policy som är bäst. I ett icke-stationärt banditproblem kan vissa eller alla av banditernas policyer ändras med tiden vilket innebär att problemlösaren inte ens efter omsorgsfullt utforskande kan slå sig till ro med att använda den historiskt bästa policyn.

Figur 13 visar vetoövervakarens uppgift som ett icke-stationärt tvåarmadbanditproblem. Policy A är att låta kommandon från styrkanalen kontrollera farkosten. Dessa kommandon kan komma från operatören eller från en oönskad källa vilket i bilden förenklas till en fiende. Policy A är därför icke-stationär. Policy B är den inbyggda policyn i farkostens autopilot för nödlägen. Autopilotens policy är inte lika bra som att operatören styr men långt bättre än att fienden styr.



Figur 13. Vetoövervakning som mångarmadbanditproblem.

Vetoövervakarens problem består i att välja mellan policy A och policy B givet att kvalitén i policy A dramatiskt kan ändras vid ett lyckat cyberangrepp. Vetoövervakaren måste alltså försöka känna igen situationer där policy A saboterar uppdraget till exempel genom att störta farkosten eller landa den på fientlig mark. Samtidigt gäller det att inte missförstå vad operatören håller på med och därmed störa uppdraget genom att ingripa i onödan. Vid ett cyberangrepp kan vetoövervakaren ingripa genom att koppla bort fjärrstyrningskanalen och koppla in autopiloten som behåller kontrollen permanent eller lämnar av till operatören först när en återautentiseringsprocess genomförts.

5.6.3 Vetoövervakning i litteraturen

Vi har bara hittat ett arbete som direkt handlar om vetoövervakning för RPAS. Kim et al. (2012) föreslår en övervakningskomponent *Supervisor* som har uppsikt över autopiloten för en RPA. En motsvarande funktion skulle kunna användas även när det inte finns någon autopilot utan allt sker med direkt fjärrstyrning. En förenklad variant av det styrsystem som Kim et al. beskriver innehåller följande komponenter, kompass, GPS, hastighetsmätare, höjdmätare, styrdon för farkostens kontrollytor och motorn samt en kommunikationslänk med operatören. En processor kör program som länkar operatörskommandon till drivrutiner för styrdon och förmedlar data från sensorer till operatören. En cyberattack skulle till exempel kunna korrumpera drivarparametrar så att drivrutiner inte översätter operatörens kommandon till fysiska åtgärder på ett korrekt sätt. En styryta kan t.ex. ge mycket större utslag än avsett och en beordrad fartökning kan leda till minskad motoreffekt istället för ett gaspådrag. Kim et al. beskriver en *Supervisor* som kör en simulering av uppdraget inklusive farkostens interna status och larmar om kontrollytors läge, motoreffekt, hastighet, höjd och position inte motsvarar det som operatören avser.

5.6.4 Vetoövervakning på fysisk nivå

Övervakning på fysisk nivå är det normala i industriella processer, kraftverk och farkoster. Övervakaren kontrollerar att fysiska parametrar hålls inom säkra intervaller. Detta kan gälla varvtalet i en motor, vätskenivå i en behållare eller roderutslag i ett flygplan. Denna typ av övervakningsfunktion är dock sällan konstruerad för att hantera cyberattacker där intrång kan ha skett i mjukvaran som kontrollerar systemet. För att fungera i en miljö med cyberangrepp måste övervakaren köra på en säker plattform och få data över säkra kanaler från intakta sensorer. Idealt ska alltså både övervakningsprocessor, kommunikationsvägar och sensorer vara helt separerade från farkostens övriga system så att inplanterad fientlig mjukvara inte kan påverka någon del av

övervakningssystemet. Detta är dock komplext, dyrt, tar plats och ökar vikten på systemet vilket gör att det sällan implementeras helt och hållet. Bak et al. (2011) beskriver en partiell lösning för *Sandboxing*.

En lösning för att säkra det övervakande systemets integritet är att placera det på en markstation eller ombord på en farkost inklusive andra RPA. Mitchell & Chen (2013a) föreslår ett sådant system där man först analyserar hotmodellen och från denna härleder de beteenderegler som ska övervakas. Ett hot kan till exempel vara att en motståndare tar över farkostens styrsystem i syfte att landa den på egen bas. För varje hot genereras en uppsättning beteenderegler där hotet ovan till exempel genererar beteenderegeln att landningsstället bara får fällas ut nära egen bas. Mitchell & Chen beskriver hur en tillståndsmaskin drivs av externa enheters observationer av farkostens fysiska uppträdande och därmed övervakar beteendereglerna och genererar alarm om dessa bryts.

5.6.5 Vetoövervakning på realtidsnivå

Mohan et al. (2013) beskriver hur ett cyberfysiskt system kan övervakas på realtidsnivå. Det som övervakas är realtidsstyrningen som består av ett antal styrprocesser som exekveras på specialiserade processorer eller PLCer (programmable logic controllers). Varje styrprocess kontrollerar någon fysisk funktion som till exempel en servomotor, en bränslekran eller en styryta. Styrprocesserna exekverar med fasta intervall och har ett mycket förutsägbart uppträdande i realtid. Mohan et al. förutsätter att realtidsövervakaren kör på en separat och mycket säker processor som kan implementeras som en FPGA, ASIC eller som en generell processor där mjukvarans integritet kontrolleras rigoröst. En avancerad realtidsövervakare skulle kunna implementeras på IBM 4758 som är en koprocessor för säkerhetskritiska tillämpningar. Genom säkra icke-störande sidokanaler hämtar realtidsövervakaren data från de processorer som kör realtidstyrningen. Att sidokanalerna är säkra betyder att realtidstyrningens mjukvara inte kan påverka data från sidokanalerna. Att sidokanalerna är icke-störande betyder att kommunikationen där inte påverkar processorns realtidsegenskaper.

Den information som sänds över sidokanalerna kan för varje styrprocess innehålla exekveringstid, antal utförda instruktioner, minnesanvändningsprofil, kommunikationsprofil etc. Lågnivåstyrprocesser är vanligen mycket förutsägbara beträffande dessa egenskaper. Exekveringstiden på de specialiserade processorer som används är till exempel oftast konstant med mycket små variationer. Om en angripare har lyckats ändra eller byta ut koden för en sådan styrprocess är det mycket troligt att någon av de övervakade egenskaperna ändras. Exekveringstiden kan till exempel bli lite längre eftersom angriparens insatta kod exekveras tillsammans med den äkta koden. Det är inte omöjligt för en angripare

att skriva kod som exakt replikerar den äkta kodens realtidsprofiler men övervakning på realtidsnivå gör det i alla händelser mycket svårare att oupptäckt utföra ett angrepp.

En fördel med den metod som lanseras av Mohan et al. är att angrepp kan upptäckas mycket snabbt och ibland till och med innan farkostens fysiska uppträdande har påverkats. I prototypen som beskrivs av Mohan et al. upptäcktes intrång inom sex mikrosekunder baserat på realtidsanomalier på 0,6 mikrosekunder. En annan fördel är att övervakningen inte kräver instrumentering eller andra ändringar av styrprogrammen. Sidokanalerna är implementerade hårdvarunära utan interaktion med styrprogrammen. Om styrprogrammen behöver uppdateras innebär det att realtidsprofilerna måste mätas om och en uppsättning parametrar i övervakningsprogrammet måste uppdateras.

Realtidsövervakaren behöver inte vara komplex och intelligensen i systemet är relativt låg. Mohan et al. implementerar logiken i sin prototyp som en tillståndsmaskin. Intelligensen i övervakaren måste anpassas till komplexiteten i realtidsstyrsystemet men man kan förvänta sig att detta typiskt arbetar enligt ett förutsägbart schema vilket innebär att realtidsövervakaren kan implementeras som ett deterministiskt regelstyrt system.

5.6.6 Vetoövervakning på plannivå: Strömbaserade processer och temporallogik

För att lägga grunden för diskussion om hur AI kan användas för att öka säkerheten i RPAS på plannivå diskuterar vi först en generell arkitektur för informationsbehandling ombord på en RPA. Denna arkitektur har utvecklats av en grupp på Linköpings universitet och beskrivs översiktligt i Heintz, Kvarnström & Doherty (2010a, 2010b). Hela denna sektion bygger på dessa referenser och vi refererar till Heintz, Kvarnström & Doherty med förkortningen HKD.

En viktig skillnad mellan AI ombord på en RPA och traditionell AI är att informationen som ska bearbetas uppdateras kontinuerligt och att tiden är en viktig variabel. Vilka informationsströmmar som är viktiga beror på vilken typ av uppdrag och vilken fas av uppdrag som är aktuell. Det är därför viktigt att kunna koppla ihop och processa informationsströmmar på ett flexibelt sätt. HKD beskriver därför en arkitektur där kunskapsprocesser tar emot strömmar och genererar strömmar som beskrivs av policyer.

En ström är en datastruktur där nya tidstämplade element kontinuerligt genereras över tiden. En sensor som övervakar en bränsletank kan till exempel kontinuerligt leverera en ström av mätvärden och en kamerastyrmodul kan sända en ström av styrkommandon till en servomotor.

En policy beskriver en ströms egenskaper tillräckligt detaljerat för att en mottagare av strömmen med hjälp av policyn kan nyttiggöra informationen i strömmen. Policyn för bränsletanksensorströmmen kan t.ex. ange tekniskt format på mätvärdet, att mätvärdet motsvarar återstående liter bränsle med ett fel på ±0.17 liter och att mätvärdet uppdateras med intervaller på 15 sekunder.

En kunskapsprocess kan ta emot en eller flera strömmar och använder associerade policys för att tolka dessa. Kunskapsprocessen genererar en eller flera strömmar med definierade policys. Bränsletankssensorn är ett exempel på en kunskapsprocess som genererar en ström men inte tar emot någon. Servomotorn är ett exempel på en kunskapsprocess som tar emot en ström men inte genererar någon. Intelligenta delfunktioner som till exempel kamerastyrmodulen implementeras som kunskapsprocesser som tar emot en eller flera strömmar, filtrerar och analyserar samt sänder ut en eller flera strömmar med förädlad information.

Databehandlingen i en intelligent kunskapsprocess kan på hög abstraktionsnivå med fördel beskrivas med någon form av *temporallogik* (Øhrstrøm & Hasle, 1995) Temporallogik är en utvidgning av *predikatlogik* (på engelska kallad *first-order logic*). Med predikatlogik kan man beskriva logiska regler inklusive lagar som gäller för alla medlemmar av en viss klass och dessutom ange att det finns objekt som uppfyller en viss regel utan att specificera vilket objekt som gör det. Med predikatlogik kan man till exempel på ett formellt datorläsbart språk specificera att bränsletank 2 är halvfull (regel om specifika saker); att alla helikoptrar kan hovra (regel om alla objekt av en viss klass); att det finns en ledningsfarkost i en grupp (regel om existens utan att ange individ). Temporallogik innebär att predikatlogik utvidgas med speciella språkelement för att på ett effektiv sätt hantera tidsrelationer.

HKD ger följande exempel på användning av temporallogik för en RPA. Anta att batteriet på en elektrisk RPA har en maximal effekt U_{max} och en normaleffekt U_{norm}. Batteriet tål att maxeffekten används under 20 sekunder förutsatt att effektuttaget därefter ligger på normalnivå i minst fem minuter innan maximal effekt används igen. En banplaneringsmodul bevakar batterieffekten genom att ta emot en ström av mätvärden, kontrollera att regeln om effektuttag respekteras och ta hänsyn till regeln vid planering av hur farkosten manövrerar. Eftersom regeln för effektuttag handlar om tidsrelationer över en lång serie av mätvärden är temporallogik ett bra verktyg för att hantera detta på ett språk som är hanterbart både för människor och maskiner.

HKD och deras forskargrupp vid Linköpings universitet har med hjälp av strömbaserade kunskapsprocesser och temporallogik byggt ett komplett styrsystem för obemannad flygande trafikövervakning. Linköpingsgruppens arbete fokuserar på att så mycket som möjligt automatisera farkosten men deras teknik är också mycket användbar för att implementera en intelligent

vetoövervakare på plannivå för RPAS. En sådan skulle kunna byggas som en grupp av samverkande kunskapsprocesser som tar emot informationsströmmar från farkostens styrsystem, inre sensorer och yttre sensorer och övervakar att det regler som gäller för uppdraget uppfylls och att beslutade planer genomförs.

Villkoren för att vetoövervakaren ska avbryta den normala styrprocessen och genomföra nödåtgärder är till exempel,

1) Farkosten befinner sig bortom en territoriell gräns som anges i reglerna för uppdraget.
2) Farkosten har under två minuter hållit en kurs som för den längre bortom gränslinjen.
3) Minst ett av följande villkor är uppfyllt
    a. Kommunikationen till operatören har varit bruten i fem minuter.
    b. Operatören har fått minst tre varningar om gränsöverskridandet där den senaste varningen sändes för minst fem minuter sedan.

En kunskapsprocess i vetoövervakaren som genomför denna policy tar emot strömmar med navigationsdata både från farkostens normala system och från oberoende positioneringssystem samt strömmar med kommunikationsdata. Regeln som ovan anges i ord implementeras med temporallogik.

En vetoövervakare på plannivå kan upptäcka angrepp på sensorer och informationssystem genom att kontinuerligt följa upp rimligheten i värden av mätserier. Farkostens position kan vara en sådan mätserie. En regel som kan implementeras med temporallogik kan vara att avståndet mellan två tidsstämplade positioner inte kan vara större än vad som medges av farkostens maximala hastighet multiplicerad med tidsskillnaden av tidsstämplarna. En anomali här är ett indicium för en attack mot navigationssensorer eller de program som hanterar navigationsdata.

Det bör noteras att Linköpingsgruppen inte är ensamma om att använda strömbaserade processer och temporallogik. Det finns många system som använder strömmar och flera varianter av temporallogik. Den som vill bygga vetoövervakare med dessa metoder kan dra nytta av relativt mogna tekniker med många alternativa verktyg.

5.6.7 Vetoövervakning på målnivå

Som ett illustrerande exempel på vetoövervakning av uppdragets mål kan vi tänka oss att två RPA samarbetar om att skapa radartäckning för att upptäcka ett angrepp med kryssningsmissiler inom en definierad zon. Mjukvaran för banplanering ombord på farkosterna samarbetar så att de områden som avspanas av respektive farkost överlappar något och alla delar av målområdet skannas av med jämna tidsintervaller. Motståndaren verkställer emellertid ett sofistikerat

cyberangrepp som tar kontroll över delar av mjukvaran i en RPA med syftet att skapa en illusion av att effektiv spaning fortsätter samtidigt som det i realiteten skapas en lucka i täckningen mellan farkosternas spaningsområden. På fysisk och realtidsnivå fungerar allting normalt på den angripna farkosten så vetoövervakarna på dessa nivåer kommer inte att upptäcka några konstigheter. Cyberangreppet gör att banplaneraren lägger en bana som lämnar ett smalt obevakat område i kanten mellan farkosternas ansvarsområden.

Men den planerade banan följs oklanderligt av farkostens styrsystem vilket gör att vetoövervakaren på plannivå inte protesterar. För att avslöja sofistikerade angrepp på denna nivå behövs uppenbarligen en övervakningsfunktion som vet att målet för uppdraget är att helt täcka in en given zon, inser att intakta underliggande system har förmåga att uppnå målet, kontrollerar att målet uppnås och kan ta beslut om nödåtgärder om allvarliga avvikelser tyder på att angrepp har korrumperat systemet.

Notera att en operatör som förutser den specifika risken av ett cyberangrepp mot banplaneringen kan installera ett relevant regelsystem som kan övervakas på plannivå. På denna nivå kan den förutseende operatören lägga in en explicit kontroll av att hela målområdet täcks in. Men det är ofta svårt att förutse alla möjliga problem och programmera motsvarande kontroller på plannivå. Övervakning på målnivå kan därför öka säkerheten och speciellt ge robusthet mot hot som inte kan förutses.

Övervakning på målnivå förutsätter att AI-programmet har en representation av de övergripande målen med uppdraget, tillräckliga bakgrundskunskaper och en god övergripande lägesbild. I denna lägesbild bör även modeller av antagonister inklusive deras förmågor och doktriner ingå. Speciellt behöver systemet konceptuellt förstå cyberattacker och vilka effekter dessa kan ha på systemet. Problemet med att representera och underhålla en övergripande lägesbild är en av de centrala forskningsfrågorna i fusionsforskningen. Hur man uppnår situationsuppfattning på cyberområdet är också ett område där forskningen är på ett tidigt stadium (se Jajodia et al., 2010). Vi har därför inte hittat några detaljerade utkast till vetoövervakare på målnivå men sådana system skulle mycket väl vara kunna finnas i avancerade RPAS på tjugo års sikt.

5.6.8 Integrerad vetoövervakning

Vi har beskrivit vetoövervakning som ett hierarkiskt system i fyra nivåer där varje nivå kan implementeras och agera oberoende. Samverkan mellan nivåerna är dock viktig för många förmågor vilket i figur 12 illustreras av pilar mellan nivåerna.

Goppert et al. (2012) listar i sin analys av cyberattacker på RPAS följande attackmål,

1) Störa uppdraget så att viktiga mål inte uppnås.
2) Ta kontroll över hela eller delar av systemet för att använda detta för egna syften.
3) Förstöra farkosten.

Guppet et al. definierar också kriterier för att en cyberattack har lyckats,

A) Viktiga gränser för hur uppdraget får utföras har brutits till exempel,
    a. Geografiska gränser för någon fas av uppdraget har överskridits.
    b. Regler för flyghöjd har brutits.
    c. Regler för bränsleanvändning och reserver har brutits.
B) Viktiga regler för hur flygningen får utföras har brutits vilket normalt leder till att farkosten förloras.

Olika typer av vetoövervakning är effektiva för olika typer av kriterier. Överskridna geografiska gränser och höjdgränser hanteras bäst av övervakning på mål- och plannivå. Brutna regler för resursanvändning upptäcks lättast med övervakning på plan- och realtidsnivå. Överskridna regler för hur flygning får utföras, som till exempel att planet inte får överstegras, övervakas bäst på realtids- och fysisk nivå. Övervakning på målnivå ger robust säkerhet även mot oförutsedda angrepp och är viktig för att koordinera systemet av övervakare.

Samverkan mellan de olika övervakningsnivåerna är viktig för att realisera hela potentialen i systemet. Antag att vetoövervakaren på plannivå upptäcker att nya vägpunkter som förefaller beordrade av operatören bryter mot övergripande regler för uppdraget som till exempel att inte göra intrång på andra länders luftrum. Det är dock inte självklart att den bästa åtgärden är att lägga ett veto och låta autopiloten flyga tillbaka farkosten till basen. Möjliga orsaker till regelbrottet är att,

1) Operatören har fått nya order och utför dessa på ett korrekt sätt.
2) Operatören gör fel till exempel på grund av trötthet.
3) En fiende har tagit över styrkanalen.
4) Inplanterad fientlig kod skriver över operatörens kommandon.

På plannivå går det inte att avgöra vilken av dessa möjligheter som är realiserad.

Den första möjligheten – nya övergripande order – kan hanteras av att en övervakarens målnivåfunktion informeras om det nya läget eller genom att vetoövervakaren kommunicerar med operatören.

Den andra möjligheten – att operatören gör oavsiktliga fel – kan hanteras genom att vetoövervakaren kommunicerar med operatören som därmed uppmärksammas på felet. Om det finns ett övervakningssystem för operatören skulle vetoövervakaren kunna fråga detta om det finns tecken på att operatören inte klarar sitt jobb. Övervakning av operatörens hjärnvågor skulle till exempel kunna bekräfta att operatören har gått in i väggen mentalt.

Den tredje möjligheten – att en fiende tagit över radiokanalen – skulle kunna avslöjas av övervakning på fysisk nivå. De fysiska egenskaperna hos radiosignalen från en fientlig sändare avviker troligen från motsvarande egenskaper för den egna sändaren. Genom att mäta signalens elektromagnetiska egenskaper som till exempel signalstyrkans riktningsberoende kan det gå att skilja mellan äkta och falsk signal.

Den fjärde möjligheten – att fientlig kod genererar falska meddelanden – skulle kunna avslöjas med realtidsanalys av den kod som ligger mellan radiomottagaren och medelandetolken.

Vetoövervakaren behöver alltså fungera som ett integrerat fusionssystem där anomalier som upptäcks på högre nivåer leder till att lägre nivåer styrs in mot mätningar och observationer som kan bekräfta eller vederlägga olika hypoteser om hur anomalin ska tolkas. Samtidigt får högre nivåer information om anonmalier som upptäcks på lägre nivå och varje nivå integrerar tillgänglig information till en situationsbild som är relevant på den aktuella nivån. En god situationsuppfattning är viktig för att på ett bra sätt kunna bedöma sannolikheter för olika händelser. I ett plötsligt politiskt skymningsläge ökar till exempel sannolikheten för cyberattacker. Övervakare på lägre nivåer behöver måste göra en bedömning av sannolikheten för att observerade anomalier orsakas av ett cyberanfall. Denna bedömning kan bli bättre om övervakaren på målnivå konfigurerar klassificerare på lägre nivåer.

5.7 Forskningsfrågor

I denna sektion listas forskningsfrågor som är av stort intresse men som inte täckts in 2013.

Intelligenta metoder för att styra en grupp av RPAer som samverkar för att lösa en spaningsuppgift till exempel enligt riktlinjer i Lauf & Robinson (2010). Det

finns en stor litteratur om samverkande robotar och multiagentsystem som kan ge vägledning.

Metoder för att verifiera autonoma system. Autonom AI i militära system måste vara mycket pålitlig och detta har på senare år stimulerat till förnyade insatser inom detta forskningsområde. Här ger Fisher, Dennis & Webster (2013) ett introducerande perspektiv som stämmer väl med den agentbaserade synen på AI som presenteras här.

6 Slutsatser

Denna rapport studerar RPA som väsentligen är fjärrstyrda. Resultaten i sektion 2.10 visar att vi i nuvarande kunskapsläge inte kan vara säkra på att det är möjligt att genomföra alla relevanta typer av spaningsuppdrag med fjärrstyrning i en situation där egna RPA utsätts för en beslutsam telekrigsinsats från en tekniskt avancerad motståndare. Eftersom antagandet om fjärrstyrning är en förutsättning för projektet är det viktigt att granska om detta antagande är giltigt under de förutsättningar som systemet förväntas operera under. De preliminära resultaten i sektion 2.10. visar att det behövs detaljerade studier av hur kommunikations-kanaler för styrning fungerar under påverkan av olika former av störning för att avgöra om framtida RPAS kan använda fjärrstyrning under alla uppdragsfaser.

Både fjärrstyrda och autonoma obemannade farkoster behöver tillgång till navigationsdata. Resultaten i kapitel 3 visar att navigationsdata från satelliter kan vara mycket lätt att störa ut. Hur farkosten robust får tillgång till navigationsdata är därför ett viktigt ämne för vidare utredning.

Kapitel 4 beskriver cyberhotets natur och visar speciellt hur viktigt det är att på rätt sätt hantera säkerheten i hela det system som har inverkan på RPAS cybersäkerhet. Cyberattacker utnyttjar ofta långa komplexa och svåröverskådliga kedjor av svagheter i kringliggande system för att ta sig in i de kritiska systemen. Vid konflikter med stater som har cyberkrigförband med förmåga att skapa, upptäcka och utnyttja sådana svagheter blir försvar mot cyberhot en mycket dynamisk och komplex verksamhet som speciellt kräver att cybersäkerhet är en viktig aspekt i alla faser av system- och förmågeutveckling. En viktig slutsats är att det alltid finns svagheter i alla system. Cybersäkerhet är därför inte något man en gång för alla kan konstruera utan bör ses som en kontinuerlig dynamisk verksamhet som spänner över både organisation, människa och teknik.

Eftersom fjärrstyrning inte kan garanteras i alla lägen och det aldrig går att garantera att ett system är immunt mot cyberattacker är det viktigt att bygga robusta system med många lager av säkerhet. De stora effekter som även ganska enkla cyberangrepp kan få beror mycket på att systemen saknar intelligens och är helt försvarslösa så snart ett yttre skal av säkerhetsystem har brutits igenom. I kapitel 5 visas att artificiell intelligens ombord på en RPA skulle kunna övervaka säkerheten på flera olika tekniska nivåer och autonomt hantera nödlägen där kommunikationskanaler eller delar av farkostens mjukvara är korrumperade av cyberangrepp. Eftersom tekniker för artificiell intelligens är under stark utveckling bör det finnas goda möjligheter att på tjugo års sikt införa sådana autonoma övervakningsfunktioner. Det är troligt att alla nationer behöver egen förmåga att underhålla och uppgradera intelligenta säkerhetskritiska system.

7 Referenser

Ahlberg, J.; Johansson, F. Johansson, R.; Jändel, M.; Linderhed, A.; Svenson, P. & Tolt, G. (2011), 'Content-based image retrieval. An introduction to literature and applications.', FOI-R--3395--SE, Technical report, FOI.

Ahlin, L. & Zander, J. (2000), *Principles of Wireless Communications*, Studentlitteratur.

Arthur, C. (2009). SkyGrabber: the $26 software used by insurgents to hack into US drones. *The Guardian*, 17 december. http://www.theguardian.com/technology/2009/dec/17/skygrabber-software-drones-hacked [2013-12-16].

Bak, S.; Manamcheri, K.; Mitra, S. & Caccamo, M. (2011), Sandboxing Controllers for Cyber-Physical Systems, *in* 'International Conference on Cyber-Physical Systems (ICCPS)'.

Becker, G.T., Regazzoni, F., Paar, C. & Burleson, W.P. (2013). Stealthy Dopant-Level Hardware Trojans. I *CHES 2013, Workshop on Cryptographic Hardware and Embedded Systems*. Santa Barbara, USA 20-23 augusti 2013, ss.197-214. DOI: 10.1007/978-3-642-40349-1_12.

Bumiller, E. & Shanker, T. (2012). Panetta Warns of Dire Threat of Cyberattack on U.S.. *The New York Times*, 11 oktober, 2012. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0 [2013-12-08].

Cabinet Office (2011). The UK Cyber Security Strategy - Protecting and promoting the UK in a digital world. London: Cabinet Office.

Chao, H.; Cao, Y. & Chen, Y. (2010), 'Autopilots for Small Unmanned Aerial Vehicles: A Survey', *International Journal of Control, Automation, and Systems* 8, 36-44.

Das, S.; Kant, K. & Zhang, N. (2012), *Securing cyber-physical critical infrastructure*, Elsvier.

Defense Science Board (2013). Resilient Military Systems and the Advanced Cyber Threat. Washington: DOD.

Department of Defense (DOD) (2007). *Unmanned systems roadmap 2007-2032*. https://www.fas.org/irp/program/collect/usroadmap2007.pdf [2013-12-16].

Department of the Army (DOA) (2010). The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028 (TRADOC Pamphlet 525-7-8).

Europeiska kommissionen (2013). Cybersecurity Strategy of the European Union - An Open, Safe and Secure Cyberspace (JOIN(2013)0001). Bryssel: Europeiska Unionen.

Federal Communications Commission (2013), 'NOTICE OF APPARENT LIABILITY FOR FORFEITURE', FCC 13-106.

Federal Ministry of the Interior (2011). *Cyber Security Strategy for Germany*. Berlin: Federal Ministry of the Interior.

Fischer, U. & Orasanu, J. (2000), Error-challenging strategies: their role in preventing and correcting errors, 'Ergonomics for a new millennium', International ergonomics association.

Fisher, M.; Dennis, L. & Webster, M. (2013), 'Verifying autonomous systems', *Communications of the ACM* 56, 84-93.

Frost & Sullivan (2007). *Study analysing the current activities in the field of UAV* (ENTR/2007/065). Bryssel: Europeiska kommissionen.

Försvarshögskolan (2012). *Systemförvaltningsmodell samt instruktioner och styrning för IT verksamhet*. http://www.fhs.se/sv/medarbetarwebben/verksamhetsstyrning/fhs-ledo/styrdokument/hogskoleovergripande-instruktioner/instruktion-for-it-verksamhet-vid-fhs/grundlaggande-principer/ [2013-12-12].

Försvarsmakten (2012). *FM Cyberstrategi*. Stockholm: Försvarsmakten. [Ännu ej fastställd eller publicerad].

Försvarsmakten (2013). Försvarsmaktens redovisning av perspektivstudien 2013, bil. 1 Fördjupningsområden (FM2013-276:1). Stockholm: Försvarsmakten.

Gardner, S.; COMM OPS: Trends in communication systems for ISR.

UAVs. Milsat Magazine, January 2009.

GlobalSecurity.org (2013), 'Common Data Link', http://www.globalsecurity.org/intell/systems/cdl.htm, Tillgänglig 2012-12-13.

Goppert, J.; Liu, W.; Shull, A.; Sciandra, V.; Hwang, I. & Aldridge, H. (2012), Numerical Analysis of Cyberattacks on Unmanned Aerial Systems, *in* 'Proceedings on Infotech@Areospace 2012'.

Gorman, S.; Dreazen, Y. J. & Cole, A. (2009), 'Insurgents Hack U.S. Drones', http://online.wsj.com/article/NA_WSJ_PUB:SB126102247889095011.html.

Grant, G. (2010). Hezbollah Claims it Hacked Israeli Drone Video Feeds (Updated). *Defensetech*, 10 augusti. http://defensetech.org/2010/08/10/hezbollah-claims-it-hacked-israeli-drone-video-feeds/ [2013-12-16].

GPS World (2012), 'Massive GPS Jamming Attack by North Korea'.

Hallandsposten (2012), 'Störningssändare skulle skydda stöldgods'.

Hambling, D. (2011), 'GPS chaos: How a $30 box can jam your life', *New Scientist*.

Heintz, F.; Kvarnström, J. & Doherty, P. (2010), Stream-Based Reasoning Support for Autonomous Systems, *in* 'Proceedings of the 2010 Conference on ECAI 2010: 19th European Conference on Artificial Intelligence', IOS Press, Amsterdam, The Netherlands, The Netherlands, pp. 183--188.

Heintz, F.; Kvarnström, J. & Doherty, P. (2010), Stream-based reasoning in DyKnow, *in* 'Dagstuhl seminar proceedings: Cognitive Robotics'.

http://blogs.airspacemag.com/daily-planet/2009/09/robot-airplane-goes-awol-gets-shot-down/?repeat=w3tc.

IBM 4758 (2013), www.ibm.com/security/cryptocards.

ISACA (u.å.). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. http://www.isaca.org/cobit/pages/default.aspx [2013-12-11].

ITU (2009), 'Characteristics of unmanned aircraft systems and spectrum requirements to support their safe operation in non-segregated airspace'(Report ITU-R M.2171), Technical report, Radiocommunication sector of ITU.

ITU (2009), 'Characteristics of unmanned aircraft systems and spectrum requirements to support their safe operation in non-segregated airspace'(Report ITU-R M.2171), ITU, Technical report, Radiocommunication sector of ITU.

Jaffe, G. & Erdbrink, T. (2011). Iran says it downed U.S. stealth drone; Pentagon acknowledges aircraft downing. *The Washington Post*, 5 december. http://www.washingtonpost.com/world/national-security/iran-says-it-downed-us-stealth-drone-pentagon-acknowledges-aircraft-downing/2011/12/04/gIQAyxa8TO_story.html [2013-12-16].

Jajodia, S.; P. L.; Swarup, V. & Wang, C., ed. (2010), *Cyber Situational Awareness - Issues and Research*, Vol. 46, Springer.

Javaid, A.; Sun, W.; Devabhaktuni, V. & Alam, M. (2012), 'Cyber security threat analysis and modeling of an unmanned aerial vehicle system', IEEE Conference on Technologies for Homeland Security.

Jensen, M.; Rice, M. & Anderson, A.L. (2007), 'Aeronautical telemetry using multiple-antenna transmitters', *Aerospace and Electronic Systems, IEEE Transactions on* 43(1), 262--272.

Jones, C. (1996). Applied Software Measurement: Assuring Productivity and Quality. Mcgraw-Hill.

Kerns, A. J. , Shepard, D. P. & Humphreys, T. E. (2013), 'Unmanned aircraft capture and control via GPS spoofing', *Unpublished*.

Kim, A., Wampler, B., Goppert, J., Hwang, I. & Aldrige, H. (2012). Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles. *Infotech@Aerospace 2012*. Garden Grove, Kalifornien, USA 19-21 juni 2012.

Kissel, R. (red.) (2013). *Glossary of Key Information Security Terms* (NISTIR 7298). Revision 2, National Institute of Standards and Technology. Darby: Diane Publishing.

Kumar, G.; Kumar, K. & Sachdeva (2010), 'The use of intelligence-based techniques for intrusion detection: a review', *Artificial Intelligence Review* 34, 369-387.

Lauf, A.; Robinson, W. H. & Peters, A. (2010), 'A distributed intrusion detection system for resource-constrained devices in ad-hoc networks', *Elsevier Ad-hoc Networks* **8**(3), 253-266.

Lauf, A. & Robinson, W.H. (2010), Fault-tolerant distributed reconnaissance, *in* 'Military communications conference (MILCOM)', pp. 1812-1817.

Lee, G. & Thuraisingham, B. (2012), 'Cyberphysical systems security applied to telesurgical robots', *Computer Standards & Interfaces* 34, 225-229.

Leyden, J. (2011). Drone nerve centre malware was Mafia Wars' infostealer. *The Register*, 14 oktober. http://www.theregister.co.uk/2011/10/14/drone_remote_cockpit_malware/ [2013-12-16].

Long, P. & Servedio, R. (210), 'Random Classification Noise Defeats All Convex Potential Boosters', *Machine Learning* 78, 287-304.

Lucchese, M.; jr, C. L. G. & Joglekar, A. N. (2000), 'Operational Evaluation of Electromagnetic Environmental Effects (E3)', Institute for Defense Analyses, PM.

Marinos, L. (2013). *ENISA Threat Landscape 2013*. Heraklion: European Union Agency for Network and Information Security (ENISA).DOI:10.2788/14231.

Mårtensson, T.; Hultgren, K. & Bull, P. (2013), 'AUVSI, Washington D.C., 12--15 Augusti 2013', FOI Memo 4565.

McConnell, M. (2011). *The Road to Cyberpower – Seizing Opportunity While Managing Risk in the Digital Age*. Booz Allen Hamilton. http://www.boozallen.com/media/file/road-to-cyberpower.pdf [2013-13-10].

McConnell, S. (2004). Code Complete: A Practical Handbook of Software Construction. 2. Uppl., Microsoft Press.

Micropilot (2013), http://www.micropilot.com.

Mitch, R. H.; Dougherty, R. C.; Psiaki, M. L.; Powell, S. P.; O'Hanlon, B. W.; Bhatti, J. A. & Humphreys, T. E. (2012), 'Know your enemy - signal characteristics of civil GPS jammers', *GPS World* 23(1), 64–71.

Mitchell, R. & Chen, I.-R. (2013), 'A survey of intrusion detection techniques for cyber physical systems', *ACM Computing Surveys* In press.

Mitchell, R. & Chen, I.-R. (2013a), 'Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specification', *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 99, 1-12.

Mohan, S.; Bak, S.; Betti, E.; Yun, H.; Sha, L. & Caccamo, M. (2013), S3A: Secure System Simplex Architecture for Enhanced Security and Robustness of Cyber-physical Systems, *in* 'Proceedings of the 2Nd ACM International Conference on High Confidence Networked Systems', ACM, New York, NY, USA, pp. 65--74.

Nahmias, R. (2010), 'Nasrallah describes 1997 ambush', http://www.ynetnews.com/articles/0,7340,L-3932886,00.html.

National Institute of Standards (2013), 'Preliminary Cybersecurity Framework'.

Newman, L.H. (2013). Can You Trust NIST? *IEEE Spectrum*, 9 oktober. http://spectrum.ieee.org/telecom/security/can-you-trust-nist [2013-12-16].

Nilsson, D. & Larson, U. (2009), 'A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure', *Journal of Networks* 4, 552-564.

North Atlantic Treaty Organization (NATO) (2011). *Defending the Networks – The NATO Policy on Cyber Defence*. Bryssel: NATO Graphics & Printing.

National Institute of Standards and Technology (NIST) (2013). *Preliminary Cybersecurity Framework*. http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf [2013-12-11].

Okänd (1947), 'Flight automatic control', http://www.flightglobal.com/pdfarchive/view/1947/1947%20-%201745.html .

Osterheld, C. (2007), 'Common Data Link (CDL) Overview"International Data Links Symposium', www.idlsoc.com/Documents/Symposiums/IDLS2007/IDLS2007_CDL.pdf, Tillgänglig 2012-12-13.

Petersen, S. & Faramarzi, P. (2011), 'Exclusive: Iran hijacked US drone, says Iranian engineer (Video)', http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video.

Peter Øhrstrøm, P. & Hasle, P. (1995), Temporal logic: from ancient ideas to artificial intelligence, Springer.

Pfleeger, C.P. & Lawrence Pfleeger, S. (2006). *Security in Computing*. 4. Uppl., Upper Saddle River: Prentice Hall.

Reichhardt, T. (2009), 'Robot airplane goes AWOL, gets shot down', Blogs at Airspacemag.com.

Rid, T. 2011. Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), ss. 5-32. DOI: 10.1080/01402390.2011.608939.

Robinson, N., Gribbon, L., Horvath, V. & Robertson, K. (2013). *Cyber-security threat characteristation – A rapid comparative analysis*. Cambridge: RAND Corporation.

Rudinskas, D.; Goraj, Z. & StankÅ«nas, J. (2009), 'Security analysis of uav radio communication system', *Aviation* 13(4), 116-121.

Ryan, A.; Zennaro, M.; Howell, A.; Sengupta, R. & Hedrick, J. (2002), 'Interoperable Data links for Imaging Systems', NATO Standardisation Agency, Edition 2.

Scarfone, K. & Mell, P. (2010). The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities (NIST IR 7502). National Institute of Standards and Technology.

Scarfone, K. & Mell, P. (2007), 'Guide to Intrusion Detection and Prevention Systems (IDPS)', Technical report, Computer Security Resource Center (National Institute of Standards and Technology).

Schapire, R. E. (2002), 'The Boosting Approach to Machine Learning: An Overview'.

von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, (38), ss. 97-102.

Strohmeier, M.; Lenders, V. & Martinovic, I. (2013), 'Security of ADS-B: State of the Art and Beyond', *CoRR* abs/1307.3664.

Swedish Standards Institute (SIS) (2006). Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet – Krav (ISO 27001:2006). Stockholm: SIS Förlag AB.

Swedish Standards Institute (SIS) (2007). *Terminologi för informationssäkerhet* (SIS Handbok 550). Utgåva 3, Stockholm: SIS Förlag AB.

Swedish Standards Institute (SIS) (2008). *Systems and software engineering – System life cycle process* (ISO 15288:2008). 2. Uppl., Stockholm: SIS Förlag AB.

Swedish Standards Institute (SIS) (2011). *Information technology — Security techniques — Information security risk management* (ISO 27005:2011). 2. Uppl., Stockholm: SIS Förlag AB.

Swedish Standards Institute (SIS) (2012). *Information technology — Security techniques — Guidelines for cybersecurity* (ISO 27032:2012). Stockholm: SIS Förlag AB.

The Economist (2011), 'GPS jamming: No jam tomorrow'.

Tian, X.; Bar-Shalom, Y.; Chen, G.; Blasch, E. & Pham, K. (2012), 'A unified cooperative control architecture for UAV missions', *Proc. SPIE* 8392, 83920X-83920X-9.

Tocher, M. & Wiedemann, M. (2011). *Technology Trend Survey – Future Emerging Technology Trends*. NATO HQ Supreme Allied Command Transformation.

Turcotte, G. (2012). DRDC Cyber Defence S&T Program – An Overview [Bildspel]. *2013 DHS S&T and DoD ASD (R&E) Cyber Security SBIR Workshop*. Washington, USA 9-11 oktober 2013. http://www.dhs.gov/sites/default/files/publications/csd-day-1-08-part-1-canada-turcotte.pdf [2013-12-11].

US Department of Defense, Defense Science Board (2012), 'The role of autonomy in DoD systems', Technical report.

US Department of Defence (2005), 'Unmanned Aircraft Systems Roadmap 2005 - 2030', Technical report.

U.S. Air Force (2009). *Unmanned Aircraft Systems Flight Plan 2009-2047*. Washington: U.S. Air Force.

U.S. Army (2010). U.S. Army Roadmap for Unmanned Aircraft Systems 2010-2035. Fort Rucker: U.S. Army UAS CoE.

US Federal Aviation Administration (2013), 'Advanced Avionics Handbook'.

U.S. Navy (2012). *Navy cyber power 2020*. http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Cyber_Power_2020.pdf [2013-12-16].

Warburton, J. & Tedeschi, C. (2011), 'GPS Privacy Jammers and RFI at Newark: Navigation Team AJP-652 Results', Federal Aviation Administration.

Whitlock, C. (2012), 'Remote U.S. base at core of secret operations', http://www.washingtonpost.com/world/national-security/remote-us-base-at-core-

of-secret-*operations*/2012/10/25/a26a9392-197a-11e2-bd10-5ff056538b7c_print.html.

World Economic Forum (2012). *Partnering for Cyber Resilience*. Geneva: WEF.

Zhou, Z.-H. (2012), Ensemble Methods: Foundations and Algorithms, Chapman & Hall/CRC.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se