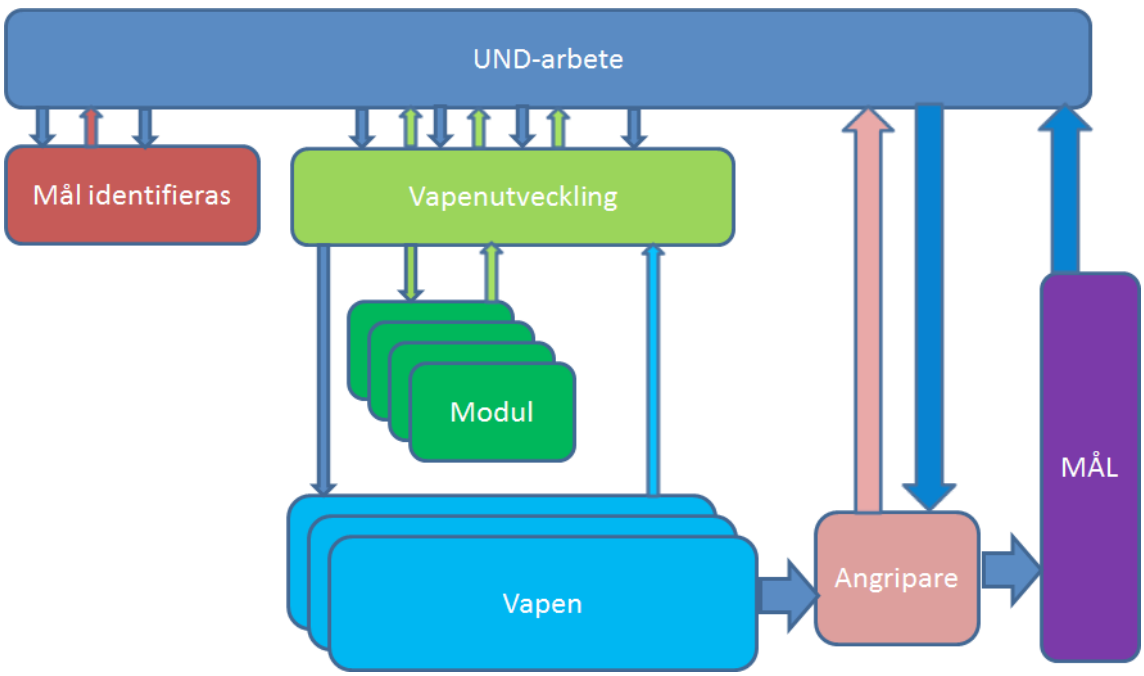
RPAS och cybersäkerhet

DAVID LINDAHL, LARS WESTERDAHL



FOI-R--4046--SE
ISSN 1650-1942 December 2014

David Lindahl, Lars Westerdahl

RPAS och cybersäkerhet

Bild/Cover: (FOI, David Lindahl)

Titel	RPAS och cybersäkerhet
Title	RPAS and cybersecurity
Rapportnr/Report no	FOI-R--4046--SE
Månad/Month	December
Utgivningsår/Year	2014
Antal sidor/Pages	67 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Temaområde
Projektnr/Project no	E34530
Godkänd av/Approved by	Lars Höstbeck
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Användningen av fjärrstyrda flygplan är något som ökat stort under de senaste 10–15 åren. Den militära nyttan har varit stor, främst inom spanings- och underrättelseområdet.

Ett system för att kontrollera fjärrstyrda flygplan (eng. Remotely Piloted Aircraft System, RPAS) består av flera delsystem som måste samverka. Dessa delsystem hanteras huvudsakligen inom Försvarsmakten men civila delsystem och aktörer kommer i framtiden sannolikt även att ingå när RPAS introduceras i kontrollerat luftrum.

Denna rapport undersöker hur cyberangrepp kan påverka fjärrstyrda flygplan och då främst ur ett cyberfysiskt perspektiv, det vill säga där instruktioner från en dator omvandlas till en fysisk påverkan av flygplanet. Även en undersökning av hur fjärrstyrda flygplan kan samverka med varandra och omkringliggande system på sikt har genomförts.

Resultaten av de båda undersökningarna visar på behovet av att se cybersäkerhet för RPAS som en helhet, där alla system som kommer i kontakt med flygplanet eller operatörsplatsen ingår, även icke-militära. I rapporten presenteras även underlag till spelkort för cyberangrepp mot RPAS.

Nyckelord: RPAS, Cybersäkerhet, Samverkande system, Cyberangrepp, Cyberkrig, Scenarion, Spelkort.

Summary

The usage of remotely piloted aircrafts is something that has increased rapidly during the last 10–15 years. The military use of remotely piloted aircrafts has been a success, especially in the intelligence, surveillance and reconnaissance (ISR) area.

A system that controls remotely piloted aircrafts (RPAS) comprises several subsystems which need to work together. Most of these subsystems are under military control, but some will be maintained and operated by civilian authorities, especially when RPAS is introduced into controlled airspace.

This report investigates how cyberattacks affect a remotely piloted aircraft, especially from a cyber-physical perspective. A cyber-physical system is one where instructions from a computer results in a physical change in the aircraft. An investigation of how remotely piloted aircrafts can be used in collaborations in the future is also performed.

The results of the investigations show the need of viewing cybersecurity from a holistic perspective, where every system that comes into contact with the aircraft is included, whether military or non-military. The report also suggests a set of cyberattacks which can be used as an exercise card.

Keywords: RPAS, Cybersecurity, Collaborative systems, Cyberattack, Cyberwar, Scenarios, exercise card.

Innehållsförteckning

1 Inledning

Användningen av obemannade farkoster (eng. Remotely Piloted Aircraft, RPA) har ökat kraftigt under de senaste 10–15 åren. RPA:er har främst använts inom konfliktområden men efterhand som nyttjandet blivit en viktig del av operationerna har idéer om fortsatt användning nationellt framkommit. Det bedöms som rimligt att förhållandet i antal mellan bemannade och RPA:er kommer att var likvärdigt runt 2030 (Lamonte 2009).

Denna rapport sammanfattar arbetet inom cybersäkerhet inom temaområdet *Obemannade farkoster och cyber*. I rapporten beskrivs hur cyberangrepp kan genomföras mot RPA:er och de system (eng. Remotely Piloted Aircraft System, RPAS) som stödjer och stödjs av dessa så som de är uppbyggda idag och antas användas inom en överskådlig framtid. Inom ramen för detta tas ett antal möjliga framtida samarbetsformer upp vilka visar hur RPAS med flera samverkande farkoster kan användas. Dessa tillämpningsfall analyseras därefter ur ett säkerhetperspektiv.

Rapporten presenterar även ett antal uppslag till spelkort. Dessa kan användas som inspel i övningar för att påvisa att ett cyberangrepp sker och vilken effekt angreppet åstadkommer.

1.1 Omfattning

Rapporten fokuserar på att visa RPAS som ett cyberfysiskt system, det vill säga ett system med datorer och information i form av instruktioner som omsätts till fysisk påverkan på en RPA. För att visa hur cyberfysiska system kan angripas används Stuxnet som exempel. De spelkort som skapas avses inte vara en uttömande beskrivning av vad som är möjligt utan utgör exempel på detta.

Den del av rapporten som behandlar system i samverkan utgår ifrån försök som sker idag eller som diskuteras inom forskningsvärlden. För att uppnå samverkan, framför allt så som det diskuteras inom forskningsvärlden, krävs en högre grad av automation än vad som är möjligt eller tillåtet i dagens system. Vid val av möjliga samverkansformer har ingen hänsyn tagits till dagens regelverk.

1.2 Målsättning

I denna rapport analyseras frågan om vilka cyberangrepp som kan riktas mot RPAS samt vilka effekter dessa angrepp kan få. Målsättningen är att skapa ett användbart underlag för att kunna använda cyberangrepp som inspel under övningar.

Målsättningen med att beskriva system i samverkan är att skapa ett diskussionsunderlag för hur framtida RPAS kan nyttjas.

1.3 Läsanvisning

Rapporten har följande struktur.

Kapitel 2 ger en bakgrundsbeskrivning av begreppet cybermiljö och hur RPAS passar in i denna miljö.

Kapitel 3 beskriver vad ett angrepp innebär inom cybermiljön och hur ett angrepp går till. I kapitlet exemplifieras angrepp genom att beskriva hur Stuxnet agerade och tillämpas genom att analysera hur RPAS kan påverkas under de olika angreppsfaserna.

Kapitel 4 ger exempel på möjliga cyberangrepp mot RPAS.

Kapitel 5 presenterar olika samverkansformer för RPAS. De föreslagna samverkansformerna generaliseras till kommunikationsbehov och analyseras genom att studera vilka möjliga risker som RPAS utsätts för inom respektive kommunikationsmönster.

Kapitel 6 sammanfattar resultaten från rapporten samt presenterar slutsatser.

Appendix A ger en kort beskrivning av grundläggande IT-säkerhet.

Appendix B innehåller underlag till de spelkort som presenterades i avsnitt 4.4.

Appendix C ger en beskrivning av ett antal olika kategorier av angripare.

2 Cybermiljön

Det har blivit vanligare att använda ordet cyber när informationsteknik (IT) och verksamhet kopplad till användningen av IT-system diskuteras. Inom ramen för cyberbegreppet ryms dock mer än bara teknik.

I detta kapitel ges en kort introduktion till vad cyberbegreppet kan innebära och hur det används i denna rapport.

2.1 Cybermiljön

Cyber är ett begrepp som växt sig starkt i media men även i militära kretsar de senaste åren. Även om cyber ännu inte är ett fastlagt begrepp inom Försvarsmakten bedriver Försvarsmakten verksamhet och genomför aktiviteter vilka kan sägas härröra till det som oftast kallas för cyber.. Försvarsmakten har valt att beskriva det som på engelska kallas för *cyberspace* som en *cybermiljö* (Försvarsmakten 2012) och det begreppet kommer att användas i denna rapport.

Inom en cybermiljö ryms IT-system och de som använder dessa, men även det verksamhetsvärde som skapas inom och utanför systemen. Ett sätt att se på en cybermiljö är att dela in den i en fysik, logisk och social domän (Department of the Army 2010). I den fysiska domänen finns hårdvara som infrastruktur – det vill säga servrar, nätverkskomponenter och kablar. Dessa har en fysisk plats i världen, en plats som är tämligen statisk. Den logiska domänen utgörs av ändsystem såsom datorer och mobila enheter. De flesta publika nätverk kommunicerar över internetprotokollet (IP). I sådana nätverk utgörs ändsystem av alla enheter som har en IP-adress. Den sociala domänen utgörs av användare och hur de representeras i de tekniska systemen. När en individ (människa eller ett annat system) interagerar med ett system skapas ett värde som kan användas utanför, eller påverka, den tekniska miljön (Trucotte 2012).

2.2 Om RPAS och cyber

En RPA ingår i ett system (RPAS) där människor och tekniska system samverkar. Ofta med syftet att inhämta underrättelser för pågående eller framtida operationer men även andra tillämpningar är tänkbara.

Ett RPAS utgör ett system av system där IT-system samverkar med cyberfysiska system. Som IT-system skiljer sig inte RPAS i stort från andra IT-system. Det är ett militärt system, vilket oftast innebär ett större behov av skydd och det förekommer fysisk separation mellan vissa delar som en del av säkerhetslösningen. Utöver detta är det fortfarande ett system som utbyter uppgifter och skickar instruktioner mellan olika enheter. Att en del av systemet,

själva RPA:n, är flygande och befinner sig på avstånd har ingen påverkan så länge den kan kommunicera med operatören.

Ett cyberfysiskt system är ett system där IT-system kopplas till styrsystem som ger fysisk verkan i den miljö de är placerade. För en RPA kan detta exemplifieras med att en operatör skickar navigationsinstruktioner till RPA:n och styrdatorsystemen ombord omsätter dessa instruktioner till roderrörelser.

Cyberfysiska system skiljer sig ifrån IT-system genom att de oftast används för kontinuerliga processer. Ett IT-system kan oftast hantera rimliga fördröjningar utan att verksamheten de stödjer påverkas negativt. I fallet cyberfysiska system i en RPA kan RPA:n inte sluta flyga bara för att kommunikationen har fördröjts eller tillfälligt avbrutits. Om kommunikationen till RPA:n skulle brytas eller försensas måste RPA:n kunna agera på egen hand, om än på ett förutbestämt sätt.

Ett RPAS utmärker sig också som system genom att det har en relativt lång åtgärdstid om problem uppstår. I händelse av att RPA:n får problem och måste avvika från ett pågående uppdrag tar det lång tid innan RPA:n flugit hem till basen, åtgärdats och flugit tillbaka till uppdragsområdet igen. Givetvis kan en RPA ersättas med en annan men tillgången brukar vara begränsad så det påverkar den övergripande effektiviteten.

3 Cyberangrepp

Ett cyberangrepp är ett angrepp mot IT-system i syfte att påverka den verksamhet som IT-systemen stödjer. I denna rapport begränsas detta begrepp till att vara sådana angrepp vars medel är informationsöverföring och vars mål är att förändra beteendet hos en cybermiljö. Detta innebär att ett angrepp där en människa genom bedrägeri förmås att fysiskt byta ut en modul i flygfarkosten mot en modul som innehåller skadlig kod, faller in under definitionen medan samma angrepp som utförs för att leverera en sprängladdning inte gör det. Denna något snävare definition av begreppet görs för att kunna ha med angrepp som använder sig av social ingenjörskonst för att förmå legitima användare att oavsiktligt försätta systemet i osäkert läge.

Två konsekvenser av intresse följer av ovanstående. För det första är angriparen beroende av förmågan att kommunicera med det IT-system som är målet för attacken. För det andra är angriparen beroende av att IT-systemet som angripits självt utför de aktiviteter som angriparen vill och som leder till ett önskat resultat för attacken. Även på andra sätt skiljer sig cyberangreppen från konventionella angrepp med kinetiska verkansdelar[1].

3.1 Konventionellt militära angrepp jämfört med cyberangrepp

Konventionella militära angrepp i den fysiska världen lyder under fysikens lagar. Det innebär att material påverkas av gravitation, värme, med mera. I en cyber-miljö där IT-system verkar gäller även dessa lagar men för ett cyberangrepp är de inte lika styrande som för ett konventionellt angrepp. Det innebär för- och nackdelar, både för systemägare och för angripare. I detta avsnitt beskrivs ett antal skillnader mellan fysiska angrepp och cyberangrepp.

3.1.1 Geografiskt begränsade

Kinetiska angrepp är begränsade i sin geografiska räckvidd. Konventionella vapen har fix räckvidd och begränsad sensorkapacitet att lokalisera sitt mål.

Cyberangrepp begränsas av möjligheten till kommunikation med målet. Hur långt bort målet finns är inte relevant.

[1] Kinetiska verkansdelar använder sig av rörelseenergi för att skada målet. Hit hör till exempel kulor, splitter och tryckvågor från explosivämnen.

3.1.2 Temporalt begränsade

Konventionella angrepp resulterar normalt i omedelbar verkan. Cyberangrepp består normalt i att förmå målet att köra angreppskod. Denna kan få verkan långt efter tidpunkten för ett angrepp. Det är fullt möjligt att infektera ett målsystem med kod som bara aktiveras under vissa förutsättningar, till exempel när ett visst datum inträffar flera år senare.

3.1.3 Vapnens beteende och funktion är tillförlitliga

De kinetiska vapnens räckvidd, splittermängd och så vidare är i princip fix över tid. Fysikaliska lagar styr verkan och beteende hos vapnen. Exempelvis stoppar en viss bepansring en viss given splitterenergi och en viss motor ger en viss viktgräns för en verkansdel. Kinetiska vapen kan användas mot många olika typer av mål. Om målen har liknande fysikaliska egenskaper får vapnet likartad verkan.

Cyberangrepp riktar sig mot en viss version av en viss programvara. Om ändringar skett, till exempel genom rutinuppdateringar av programvara kan vapnet bli helt verkningslöst eller, dock mer sällan, få förvärrad verkan i målsystemet. En direkt liknelse med den kinetiska situationen skulle vara om en robots verkansdel skulle sluta fungera mot en viss modell av helikopter för att piloten ställt in sätet annorlunda än normalt.

3.1.4 Industriell tillverkning

Konventionella vapen utvecklas och framställs industriellt. Stora investeringar i industri och forskning krävs för att framställa nya versioner av robotar och kanoner. De aktörer som saknar industribas är begränsade till utrustning – ofta av sämre kvalitet och modell – som andra aktörer säljer till dem.

Cyberangrepp sker med konventionell kontorsutrustning som finns öppet tillgänglig på marknaden. Begränsningen för en angripare ligger snarare i underrättelsedata om målsystemet. Specifikt, hur systemet kan nås via kommunikation, och vilka sårbarheter [2] det har. Sårbarheterna ett system har varierar över tid när olika versioner av uppdateringar installeras, inställningar ändras eller olika undersystem kopplas till eller från.

[2] Sårbarhet är en term för en viss egenskap hos ett system som gör att en angripare kan manipulera systemet på något sätt. Till exempel att en dator i systemet accepterar anrop från Internet.

3.1.5 Upprepade angrepp ger förvärrade resultat

För ett kinetiskt vapen gäller normalt att fler alltid är bättre. Om en robot kan ge verkan på målet blir skadan större ju fler robotar som träffar och sannolikheten för nedskjutning ökar ju fler robotar som avfyras mot målet.

Cyberangrepp är en begäran till målsystemet, och får normalt inte bättre verkan av upprepade anfall om angreppen inte sker mot olika punkter i målsystemet. Att angripa via samma intrångsvektor mot samma måldator är alltså oftast meningslöst så vida målet inte är en överbelastningsattack. (Om inte denna ändrats, se tillförlitlighet ovan).

3.1.6 Direkt verkan

Konventionella vapen har en direkt påverkan i de mål eller på den omgivning som befinner sig i dess närhet. Den som avfyrar vapnet förväntar sig att se ett direkt resultat av vapnets verkan och målet förväntas omedelbart bli satt ur stridbart skick.

Ett cybervapen påverkar målet genom att få delsystem i målet att utföra handlingar. Dessa handlingar kan vara att begära att andra delsystem ska utföra handlingar i sin tur. Ett cyberangrepp i en punkt (en viss dator), kan orsaka en kedja av händelser som inte resulterar i skada förrän många led bort.

3.1.7 Oavvislighet

Ett konventionellt angrepp är normalt oavvisligt. En robotträff i ett flygplan lämnar fysiska spår efter sig som gör att det i efterhand kan avgöra att angrepp skett, med vilken typ av vapen och med största sannolikhet i vilket område lavetten varit placerad.

Inget av detta gäller vid cyberangrepp. Det är inte säkert att det i efterhand går att avgöra ens att ett angrepp skett. För att spårbarhet ska finnas måste systemen byggas så att de explicit lagrar data om vad som skett i systemet och vilka åtgärder som vidtagits. Data om vad som skett i ett system sparas i loggar. Dessa måste också bevaras under en längre tid så att de är tillgängliga långt efter angreppet. Slutligen måste kompetens finnas för att gå genom de sparade data som finns och dra korrekta slutsatser.

Men även i de fall där allt ovanstående finns tillgängligt är det inte säkert att det går att säga mer än att en angripare har anslutit till systemet från en viss punkt. Om denna punkt ligger i ett annat land, eller på annat sätt utanför den egna organisationens kontroll är det normalt inte möjligt att uttala sig om vem angriparen är eller var angreppet startade. Därför lämpar sig cyberangrepp väl i så kallade skymningslägen eller för infiltration i fredstid. Dessutom lämpar sig cyberangrepp för en annan typ av politisk påverkan där ett angrepp sker som en

form av osynlig kanonbåtsdiplomati. Angriparen genomför då ett eller flera angrepp i ett land och låter via diplomatiska kanaler förstå att om angreppen fortsätter är beroende på hur landet agerar i någon viss fråga.

3.2 Stuxnet: ett cyberangrepp i detalj

SCADA (Supervisory Control And Data Acquisition) är en term som används för industriella styrsystem. Exempel inkluderar eldistribution, kemisk industri och styrning av kraftverk. Dessa system har ett antal egenskaper som delas med RPAS, exempelvis:

- De styr en fysisk process. Denna är ofta tidskritisk och en försenad eller utebliven styrsignal kan leda till allvarliga olyckor.
- Operatören sitter på avstånd och är beroende av telemetri[3] för att kunna övervaka och styra processen.
- Systemen är hybrider mellan specialiserad utrustning och COTS.[4]

I skrivande stund finns det få exempel på intrång i RPAS i den öppna litteraturen. Men det finns väldokumenterade fall av intrång i SCADA-system. I denna rapport tas ett sådant fall upp för att illustrera hur ett cyberangrepp kan genomföras. I den Iranska staden Natanz finns en gigantisk underjordisk anläggning för upparbetning av uran till halter som lämpar sig för kärnbränsle. USA anser att anläggningen är till för att anrika material för kärnvapen (Albright & Hinderstein 2003).

I juni 2010 upptäckte datorföretaget VirusBlokAda ett nytt exempel på skadlig kod (Keizer 2010). Detta var vapnet som senare skulle bli känt som Stuxnet. Under de följande åren framkom ny information om vapnet och vad det använts till. Av det som framkommit i öppna media verkar följande vara den accepterade tidslinjen: 2005 – fem år innan upptäckt – registrerades fyra adresser på Internet, under namn som smartclick.org och ad-marketing.net, i USA, Kanada, Frankrike och Thailand. Alla fyra hemsidorna var identiska (McDonald, O'Murchu, Doherty & Chien 2013).

Dessa fyra webbplatser var i själva verket konfigurerade för styrning av Stuxnet-infektioner. Vid denna tid infekterades de första styrdatorerna i Natanz av skadlig kod (senare döpt till Stuxnet 0.5) i en första våg.

Upparbetningen av uran sker stegvis genom ett stort antal centrifuger (över 8000 enligt Albright, Stricker & Walrond (2010)). Gasen uranhexafluorid körs genom centrifugerna i syfte att separera de tyngre uranisotoper från lättare.

[3] Automatiserad insamling och sändning av data för att övervaka något på avstånd.
[4] COTS, Commercial Off The Shelf, standardutrustning för många tillämpningar.

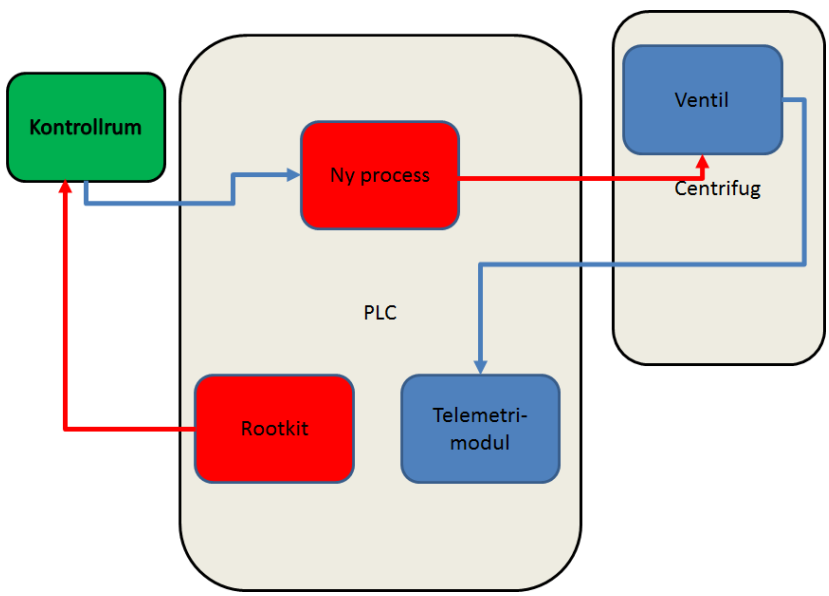
Synkroniseringen av centrifugerna sker genom en industristyrdator (eng. Programmable Logic Controller, PLC) som sitter på varje centrifug. Denna sköter varvtal, temperatur och andra funktioner med hjälp av olika motorer och ventiler som den styr.

Anläggningen kontrollerades ifrån ett kontrollrum där tekniker övervakade tillståndet för alla centrifuger. Därifrån kunde de ändra varvtal, styra om gasflöden och sköta hela anläggningen på distans.

PLC:erna uppdaterades från en central dator. Teknikerna matade in program-ändringar i centraldatorn, och den anropade sedan alla PLC:er som berördes av ändringen och uppdaterade deras interna program automatiskt genom att lägga till nya programmoduler.

På något sätt övertygades eller lurades en insider[5], en tekniker eller konsult, att föra in vapnet i uppdateringsservern och denna uppdaterade PLC:erna precis som vid en normal uppdatering.

Vapnet innehöll två delar. Ett så kallad rootkit som dolde vapnet från operatörerna genom att skicka falska data till kontrollrummet så att allt såg normalt ut, samt en angreppsdel som tog över styrningen av den ventil som matade in gas i centrifugen, se Figur 1. Detta gjorde att gasflödena inte längre fungerade tillförlitligt och anrikad gas kunde blandas ut igen.



Figur 1 Schematisk vy av angrepp från Stuxnet 0.5

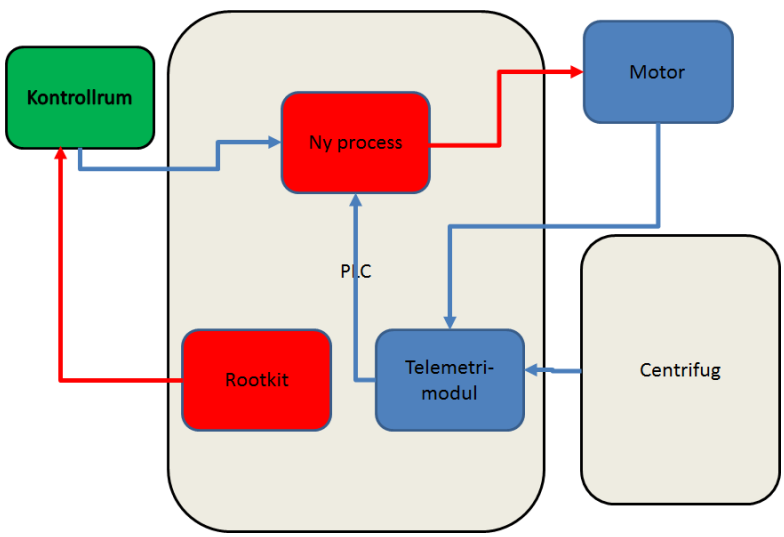
[5] En person som tillhör en organisation men som medvetet eller omedvetet går angriparens ärenden.

Vid ett senare tillfälle uppdaterades vapnet och fick ytterligare funktionalitet. Den nya versionen, kallad version 1.0, behövde inte föras in direkt i uppdateringsservern. I stället spred den sig från USB-enheter om dessa sattes in i windowsdatorer genom att först övertyga operativsystemet att köra den skadliga koden och sedan kopiera sig från dator till dator i nätverket, och därmed infektera alla maskiner den passerade. Om en maskin den nådde hade internetanknytning så ”ringde den hem” till en av två nya kontrollservrar. Den kunde från kontrollservern ladda ner ny kod för att uppdatera sig och även skicka uppdateringarna vidare till andra vapen som fanns i samma nätverk. Inget av detta kunde detekteras från värddatorerna eftersom en rootkit skyddade vapnet från upptäckt.

När vapnet hittade en uppdateringsserver för SCADA-system kontrollerade det att systemet som uppdaterades innehöll en mycket specifik konfiguration av PLC:er och kringutrustningar och endast om denna konfiguration stämde skedde angreppet.

Med två stulna certifikat[6] som hjälp lade vapnet in uppdateringar på servern och såg till att dessa följde med de andra, äkta, uppdateringarna.

Väl på PLC:n fungerade uppdateringarna inte som i den tidigare versionen utan innehöll ett program som manipulerade varvtalet på centrifugmotorn så att centrifugerna hamnade i resonans och kullagren efter en tid gick sönder. Figur 2 visar en schematisk vy över förloppet.



Figur 2 Schematisk vy över angrepp från Stuxnet 1.0

[6] Ett kryptografiskt signerat dokument som garanterade att koden var en äkta uppdatering

Genom detta förfarande kunde driften av anläggningen allvarligt försvåras samtidigt som det verkade som att felet låg i kvalitetskontrollen av kullager och centrifugfästen.

Detta angrepp pågick efter vad som är känt i minst ett år innan orsaken till centrifughaverierna kunde upptäckas. Resultatet av detta angrepp blev att upp till två tredjedelar av centrifugparken inte kunde användas samt att anrikningen blev mycket försenad.

Värt att notera är också att vapnet använde sig av fyra eller fem tidigare oupptäckta säkerhetshål, så kallade zero-day vulnerabilities. Att så många okända säkerhetshål finns i ett och samma vapen är oerhört ovanligt. De flesta intrång sker med redan kända sårbarheter som inte täppts till av offret, eller som öppnas upp av en insider.

Det är fortfarande inte officiellt bekräftat vare sig vem som låg bakom angreppet, eller vem som var det tänkta målet. Stuxnet spred sig inte bara till Natanz, utan till tusentals datorer i många länder, exempelvis Tyskland, Indonesien, Indien och Ryssland. Enligt Washington Post (Nakashima & Warrick 2012) har en högt placerad källa sagt att det var det USA och Israel som gemensamt utförde angreppen. Iran har erkänt att de drabbats, men hävdar att de tidigt upptäckte och neutraliserade problemet.

3.3 Slutsatser av Stuxnetangreppet ur ett RPAS-perspektiv

Operatörens avstånd från processen är en svaghet: om kedjan av sensordata från sensor till operatör blir förvanskad kan operatören bli helt lurad.

De olika styrdatorerna kan angripas och förmås att utföra en angripares order. Varje delsystem är alltså att betrakta som en egen aktör. Farkosten och bas-stationen kan inte antas vara deterministiska, utan är system av system som förändras under drift.

System som är tänkta att vara helt separata från omvärlden är sällan det i verklig-heten. Tekniker och operatörer flyttar lagringsmedia och kopplar tillfälligt upp förbindelser mellan datorer för att hålla systemet i drift.

Det är möjligt att utnyttja en fysisk process för att orsaka fysisk skada på det styrda systemet. En RPAS skulle kunna förmås att flyga in i föremål eller mark. Eller så skulle roder kunna manipuleras för att orsaka ett haveri.

Ett cyberangrepp kan pågå under lång tid och vara oerhört svårt att hitta via normala felsökningsmetoder. En kompetent angripare kan utveckla eller köpa nya vapen som utnyttjar sårbar-heter som inte kan täppas till med normala uppdateringsmetoder. Detta då upp-dateringsmodellen är beroende av att

sårbarheter upptäcks och publiceras en tid innan angrepp, så att motmedel hinner tillverkas.

I fallet med Stuxnet visste angriparna inte bara exakt vilka operativsystem som kördes på kontorsnäten, utan även exakt vilken uppsättning PLC:er och kringutrustning som anläggningen hade (Langner 2013). Angriparen hade troligen använt sig av sin fulla underrättelsekapacitet för att understödja framtagningen av vapnet. I denna underrättelseverksamhet ingår inte bara de normala metoderna som signal-spaning, spionage och utpressning utan också att köpa in eller stjäla system för att kunna leta upp nya sårbarheter och testa vapen under lång tid. Detta för att ha ett vapen färdigt för omedelbar insats om det politiska läget skulle kräva det.

Det är inte känt varför vapnet tilläts sprida sig så mycket när målsökningsfunktionen var så noggrann. En möjlighet är att genom att tillåta urskillningslös infektion skulle Iran inte förvarnas om att de var målet. Men det visar att Sverige inte kan antas vara säkert bara för att inga andra stater provoceras. Om företag och myndigheter i Sverige använder system vars delar utgör mål i andra stater kan även svenska system angripas av misstag eller som en del av en vilseledningsoperation.

3.4 Ett cyberangrepps faser

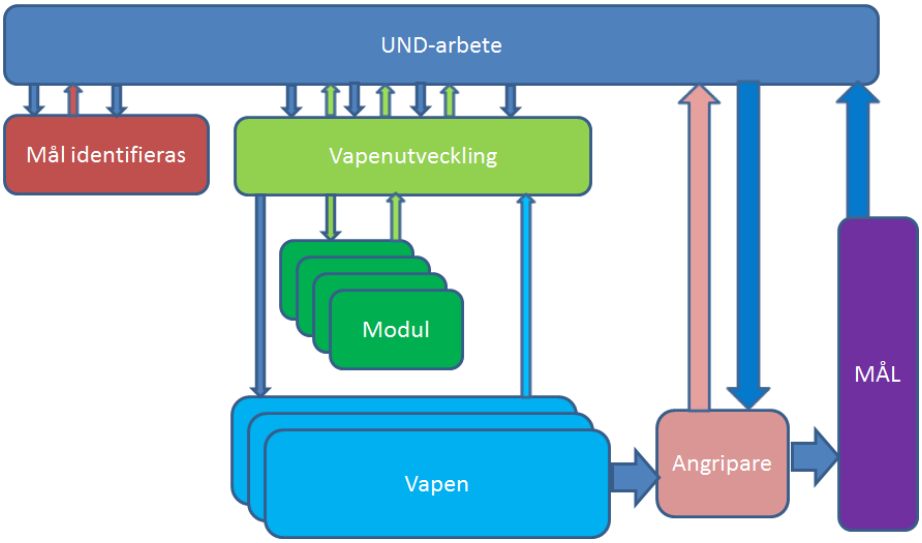
Givet ovanstående exemplifiering kan ett cyberangrepp skissas över tid som en serie överlappande cykler. Figur 3 visar cyberangreppets faser.

3.4.1 Underrättelseinhämtning

Den första cykeln, underrättelseinhämtning, pågår kontinuerligt. Den utförs utifrån de förmågor angriparen har, med resurser som variera från den enskilde som söker information på Internetforum till programmeraren i en statligt finansierad underrättelseverksamhet som arbetar med specialskrivna programbibliotek och spaningsdata inhämtad från en mångmiljardverksamhet.

En angripare måste för det första ta reda på vem som ska angripas. Något som verkar trivialt, men beroende på målsättning kan det vara komplicerat. En hacktivist,[7] till exempel, som vill påverka Sveriges politik i någon fråga, måste komma på vilket mål som skulle få en politiker att fatta önskade beslut. Är det mål som rör politikern personligen, dennes familj, myndighetsservrar, eller ett företag som är viktigt för landets ekonomi?

[7] En hacktivist är en benämning på en angripare som är politiskt motiverad. Hacktivisten bedöms sällan ha hög teknisk kompetens men det finns inget som hindrar hacktivisten från att köpa eller hyra kompetens för att uppnå sina mål.



Figur 3 Faser cybervapenutveckling

I de flesta fall är det angriparens kompetens och resurser styrt målvalet snarare än strategiska och taktiska överväganden. Angreppen mot myndigheters webb-servrar som följde på häktningsordern av Julian Assange är exempel på detta (Olsson 2012). Att slå ut, eller ändra data på, en webbserver är i de flesta fall relativt enkelt, ger ett synbart resultat och gör att budskapet blir uppmärksammat i pressen. Men effekterna på myndigheterna är minimalt. Webbservrarna är normalt inte ens placerade i myndigheternas datornät utan ligger på externa webbhotell. Eventuella angrepp mot myndigheters interna system har än så länge inte uppmärksammats.

Situationen är dock annorlunda för angrepp mot ett RPAS jämfört med att angripa myndigheter och annan civil infrastruktur. En angripare som vill slå mot ett RPAS kan inte välja mellan hundratals dåligt skyddade datorer och göra angrepp mot dem med säkerhetshål som passar angriparens verktygslåda. För att en angripare över huvud taget ska kunna hitta[8] ett RPAS kräver det kunskap om vilka adresser på Internet eller i framtida militära nät som RPAS använder för kommunikation. Dessutom krävs vetskap om hur RPAS ser ut ur logisk synvinkel, det vill säga vilka datorer som kommunicerar med varandra, med vilka protokoll och vilka inställningar de har.

För denna typ av information studeras öppna källor och en angripare med till-räckliga resurser anskaffar en egen uppsättning av systemet för att kunna studera det i detalj. För kommersiella system kan testuppsättningar köpas, medan

[8] Författarna att framtida RPAS inte sitter oskyddade och direkt uppkopplade mot Internet.

militära hemliga system måste återskapas hjälpligt genom hårdvarustölder, spionage och gissningar. Detta är inte något som är nytt för datoreran utan har fungerat på ungefär samma sätt sedan de första maskinkryptona infördes.

Förutom datorers logiska uppbyggnad, exempelvis deras IP-adresser, är det fysiska cybersystemet också intressant. I detta ingår förutom datordelar också de personer som handhar eller interagerar med systemet. Dessa är av intresse både som agenter vilka kan förmås sätta systemet i osäkert läge och som underrättelsekällor.

Ett exempel på ovanstående är de fall i Storbritannien där barn till piloter i Royal Air Force (RAF) befanns ha vänner på Facebook vars adressuppgifter och språk gjorde gällande att de bodde i samma stad som pilotens familj men vars IP-adress visade att de anslöt från Kina.[9]

3.4.2 Vapenutveckling

Vapenutveckling startar när en angripare har fått så mycket underrättelser att målsystemet kan modelleras i rimlig detalj. Angriparen försöker då söka efter kända sårbarheter hos ingående komponenter i systemet, och anpassa dessa efter behov. En resursstark angripare kommer också att inleda ingående analys av mjuk- och hårdvara i systemet för att kunna hitta dittills okända sårbarheter (zero-day vulnerabilities). Några ytterligt få angripare (Defense Science Board (DSB) 2013) kommer att kunna införa sårbarheter i tillverkningen av systemdelar så att framtida reparationer eller nyanskaffning av målsystemen levereras färdiga för intrång.

Vapnet tillverkas troligen i moduler så att delar kan testas oberoende av varandra, och så att så många alternativ som möjligt i fråga om spridning, verkan, kommunikation, och smygegenskaper kan erbjudas i den färdiga produkten.

Om det alls är möjligt kommer angriparen att vilja testa vapnen på kopior av målsystemet. Det föreligger en risk att en angripare kan vilja genomföra inledande tester av ett vapen genom att slå mot orelaterade mål som ligger i stater som inte utgör ett militärt hot och som inte kommer att dela incidentdata med det slutliga målet. När angreppet pågår kommer rättningar och modifieringar att göras inte bara för det aktuella vapnet utan också för att vidareutveckla nya vapen inför framtida operationer. Denna cykel kommer att löpa under vapnets hela livstid, så att nya sårbarheter kan inlemmas och utnyttjas, och förändringar eller uppdateringar av målsystemet kan hanteras.

[9] Uppgiften delgiven till ena författaren under en personlig konversation (2013).

3.4.3 Angrepp

Angreppet inleds med att eventuell kommunikation och kontroll av vapnet etableras. Detta kan ske via så kallade botnät[10] eller genom insiders som i Stuxnetfallet.

Därefter uppstår problemet att hitta en metod att faktiskt få vapnet i angreppsläge – intrångsvektorn. Historiskt sett har social ingenjörskonst visat sig vara mycket vanlig, för att helt eller delvis transportera vapnet till målsystemet. Med detta menas att på något sätt lura en människa att göra något som hon inte inser är en säkerhetsrisk. Exempelvis att lägga USB-minnen utanför en anläggning med förhoppningen att en anställd ska ta med sig det in och ansluta minnet till en dator för att se vad som är på det. Ett annat exempel är eller *watering hole attacks* vilka är angrepp mot externa datorer som tidningars webbplatser där skadlig kod läggs in för att vänta på en intressant dators anrop och till exempel övertyga användaren att ladda ner en uppdatering av sin webbklient. I det som verkar vara en uppdatering finns skadlig kod som för in ett cybervapen i användarens miljö.

Vad som är tydligt är att intrång sällan lyckas i ett enda steg mot en kompetent organisation. Det är till exempel inte troligt att ett RPAS skulle ha några datorer direkt anslutna mot Internet. En angripare skulle alltså först behöva ta sig in i ett system som är anslutet till ett militärt nätverk, och därefter traversera detta förbi intrångsskydd för att nå RPAS. Detta sker inte i ett svep utan kan mer liknas vid en militär kampanj där en angripare försöker ta sig in på många olika sätt på olika ställen, och sedan skaffar ett brohuvud in i en organisation. Därefter följer en sekvens av privilegieeskalering, det vill säga att angriparen skaffar sig ökade rättigheter inne i systemet. Målet är att få en användaridentitet som systemoperatör.[11] Om detta uppnås kan angriparen alltså logga in som om denne vore en legitim anställd systemoperatör och programmera om systemet efter egen vilja. Med ett systemoperatörskonto har angriparen dessutom stora möjligheter att ta sig in igen om ett angrepp upptäcks och systemet stängs ner.

Vid ett intrång är det inte troligt att en angripare kan ansluta hela vägen till målet från Internet, utan vapnet har normalt en förmåga att på egen hand färdas i nätverk och angripa datorer den stöter på. Denna förmåga medger en möjlighet för cybervapen att ta sig in i slutna anläggningar genom att kopiera sig till minnet i en enhet som någon bär med sig, till exempel en USB-sticka eller en mobiltelefon. När denna ansluts inne i anläggningen till exempel för att laddas via USB, kopierar sig vapnet vidare och angriper. Ett troligt exempel på en sådan händelse var Mafiawars-infektionen av RPAS vid Creech Airforce base i USA (Air Force Space Command 2011).

[10] Nätverk av kapade datorer som fjärrstyrs utan ägarnas vetskap
[11] En person som sköter driften av ett system, kallas också systemansvarig eller drifttekniker.

I händelse av att vapnet stöter på en dator av en typ den inte kan angripa, är det vanligt att en signal skickas ut via en redan angripen dators Internet-gränssnitt. Detta meddelande går till en kontrollserver och innehåller information om operativsystem, inställningar och andra data som kan användas för att tillverka en uppdatering av vapnet. När en sådan uppdatering finns tillgänglig skickas den in till vapnet som sedan fortsätter sina angrepp.

Det är alltså inte så att ett IT-vapen gör en och endast en attack, som kinetiska vapenbärare, utan intrånget är en serie av mindre och större angrepp i syfte att söka sig fram genom datornätverken och utföra ett uppdrag. Detta uppdrag kan vara att infektera alla datorer den kan med fjärrstyrningsprogramvara, eller att leta upp en och endast en måldator och leverera verkan där.

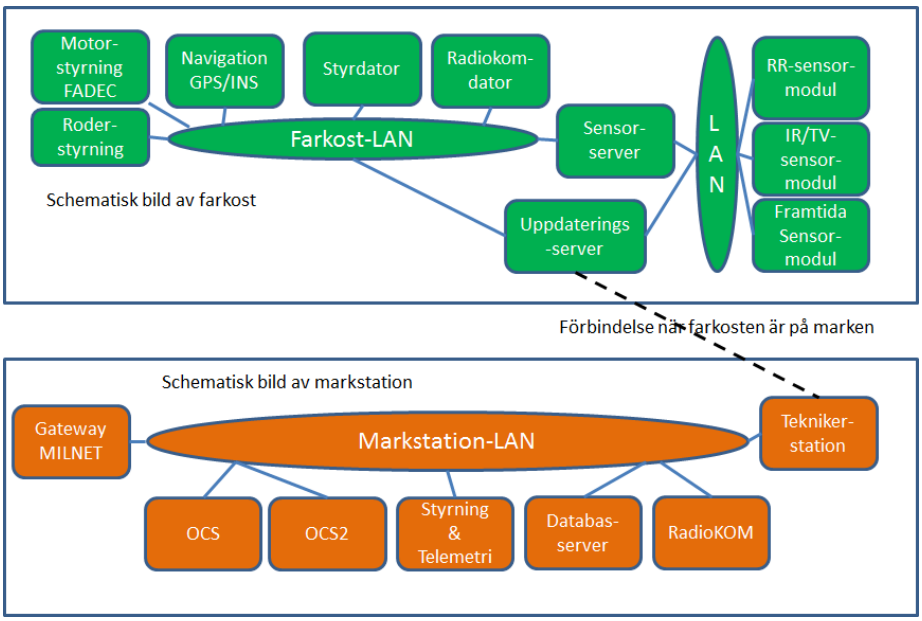
Angreppet kan avslutas på olika sätt – Stuxnet hade en inbyggd mekanism som gjorde att det stängde av alla sina kopior vid ett visst datum (Mills 2010; Gross 2011). I andra fall har vapen lämnats aktiva och utgör då en fara för framtida system som inte har skydd mot vapnet.

4 Cyberangrepp mot RPAS

Eftersom cyberangrepp är så oerhört beroende av detaljer i systemen finns det inget sätt att förutsäga hur ett realistiskt cyberangrepp mot ett framtida RPAS kan ske utan att modellera RPAS i detalj. Det går dock inte i nuläget att precisera hur ett RPAS kommer att se ut om 10–20 år, varvid ansatsen som presenteras i denna rapport fokuserar på den nytta som förväntas av systemet.

För att exemplifiera cyberangrepp tar rapporten sin utgångspunkt ifrån den cyberangreppstaxonomi som är framtagen av Applegate & Stavrou (2013) men taxonomin har modifierats för att passa rapportens syften. Fokus för beskrivningarna ligger på de verksamheter som bedrivs kring ett RPAS och de tjänster RPAS förväntas kunna leverera. I rapporten förs ett resonera kring hur dessa skulle påverkas om motsvarande tjänster i ett av dagens system drabbas av ett av dagens angrepp. Det blir då möjligt att framställa ett fiktivt cyberangrepp för användning som inspel i simuleringar eller övningar genom att välja angreppstyp och systemtjänst samt se vilka konsekvenser detta skulle få.

Figur 4 presenterar en schematisk vy av förmågor hos ett framtida RPAS. Dessa förmågor utvecklas i kommande stycken.



Figur 4 Schematisk vy RPAS.

4.1 Farkostvy

I flygfarkosten finns en uppdragsbeslutande styrdator, vilket utgör ”hjärnan” i farkosten. Den laddas på marken med uppdragsdata och flyger sedan farkosten enligt förbestämd rutt om inte operatören beordrar annat. Det är denna enhet som kommunicerar med Navigation, Motorstyrning, Roderstyrning, Radiokomdatorn och Sensorserver.

Motorstyrning är en dator som sköter alla detaljer kring farkostens motor. Den kallas också FADEC efter engelskans Full Authority Digital Engine Control. Den tar emot order och ser sedan till att varvtal, bränsle och så vidare ger önskat resultat. Navigation är en dator som sköter navigationssystemen med hjälp av satellit-navigering[12] och tröghetsnavigering.[13] Den svarar på anrop från Styrdatorn och talar om var farkosten befinner sig. Roderstyrning är den dator som detaljstyr motorerna för rodren och ser till att farkosten flyger i rätt riktning och vinkel mot marken. Kommunikation med markstation och andra system sköts av en dator som kallas Radiokom. De ingående komponenterna kommuniserar med varandra över ett internt nätverk (eng. Local Area Network, LAN).

Dagens RPA:er är oftast konfigurerade för en typ av sensorsystem. Framtida system kommer sannolikt att ha utbytbara sensorer. Sensorservern för sensorstyrning sitter mellan två lokala nätverk. Ur styrdatorns synvinkel sköter sensorservern alla sensorer samtidigt, men dess egentliga funktion är att ta emot standardkommandon och hålla reda på specifika protokoll och kommunikationsstandarder för de olika sensormoduler som kan tänkas kopplas in. LAN-anslutna sensormoduler är datorer som styr en sensor och dess kringutrustning. Det kan vara en tv-kamera i motoriserad kardanupphängning eller en radarsensor med svängbar antenn. Dessa tar emot order från sensorservern och returnerar sensordata som sensorservern för vidare till styrdatorn.

Uppdateringsservern är en dator som används för att ta emot uppdragsorder och för att lämna ut lagrad sensordata och diagnostik från farkosten. Denna ska endast vara igång på marken och ansluts med en kabel till markstationens nätverk där den kommunicerar med en dator som systemteknikerna sköter.

4.2 Markstationsvy

I markstationen bedöms följande enheter finnas. Operatörsstationer (eng. Operator Control Station, OCS) är användargränssnittet för RPA:n och de platser

[12] Satelitnavigering sker genom Global Positioning System (GPS).

[13] Tröghetsnavigering innebär att farkosten använder sina sensorer för att räkna ut hur den har förflyttat sig ifrån en känd punkt. Den engelska benämningen på detta är Inertial Navigation System (INS).

från vilka en pilot styr farkosten. Stationerna har flyginstrument och ett gränssnitt som låter piloterna se data från farkosten. Eventuellt har stationerna också möjlighet att se radaröverväkningsbilder och data från andra system med vilka RPAS samverkar. Från stationen kan operatören kommunicera med flygledning och högre stab via text och röst.

Styrning och telemetri är den dator som egentligen flyger farkosten. Operatörens order i form av spakrörelser och knapptryckningar översätts till maskinspecifika format som reläas till farkosten via radio. Det är också denna dator som tolkar utdata från farkostens roder- och motordatorer och visar resultatet som indata till operatörsstationerna.

Databaser för loggar och andra data sparar ständigt undan vad som händer för senare användning och analys. Databaserna medger, förutom fullständig återuppspelning av uppdragen så som de upplevs från operatörsstationerna, möjlighet för olika former av dataanalys från högre stab. Efter att farkosten landat och ombordvarande data tankats ur kan även uppdraget återspelas ur farkostens synvinkel.

Markstationen kommunicerar med militära staber och andra enheter via Gateway MILNET, vilken är en gränssnittsdator mellan nätverk.

Kommunikation med farkosten och andra system sköts via en dator som styr en eller flera radio- och radiolänkantenner.

Arbetsplatser för tekniker så att de kan uppdatera och sköta systemet måste finnas – troligen fler än en. Dessa är normala kontorsdatorer, men med högre prestanda. De används för alla uppgifter som rör driften i systemet. Därmed menas även att skicka uppdragsorder till farkosten och att hämta data ur den.

Lokala kommunikationsnät (LAN) antas vara helt utan interna skydd eller spärrar. Säkerhet åstadkoms med brandväggar vid övergångar till andra nät.

4.3 Generiska angrepp

Samtliga ovanstående komponenter kommer att behöva åtminstone följande delsystem:

- Input/Output-modul för in- och utdatatrafik
- Arbetsminne för datalagring
- Processor för beräkningar
- Eventuellt en styrd fysisk process

Det innebär att en angripare kan placera skadlig kod i dessa delsystem och förmå dem att utföra order som är skadliga för systemet. Exakt vilka är inte möjligt att

förutse utan att faktiskt testa de framtida modulerna. Men ett värsta-fall-scenario ger ett antal alternativ.

Gemensamt för alla delmoduler är att det finns risk för att en programvaruuppdatering med skadlig kod drabbar dem. Programmet som enheten kör uppdateras då så att ny funktionalitet införs. När modulen är i drift beter den sig inte normalt. Detta angrepp sker när enheten är på marken och underhåll sker. En sådan uppdatering kan få modulen att utföra följande angrepp mot andra moduler eller enheter:

- Belastningsattack (eng. Denail of Service, DoS). Modulen sänder meddelanden till minst en annan enhet på det lokala nätverket i syfte att förhindra legitima indata till denna. Resultatet varierar beroende på målmodulen. Aktiviteten kan också användas för att sända så mycket att hela det lokala nätverket blir överbelastat och inga komponenter kan ta emot indata. I denna rapport har det antagits att en modul kommer att fortsätta i samma läge tills nya styrdata kommer. En motor håller samma varv, ett roder ligger an i samma vinkel etc.
- Felstyrning. Modulen skickar styrsignaler till den process den kontrollerar för att orsaka händelser skadliga för systemet. De exakta resultaten varierar beroende på vilken process modulen styr.
- Falsksändningsstyrning. Modulen skickar indata till minst en annan modul på det lokala nätverket i syfte att få denna att ge order till den fysiska processen modulen styr så att systemet påverkas på skadligt sätt.
- Falsksändning av data. Modulen skickar felaktiga indata till någon annan modul i syfte att lura denna att systemläget är ett annat än det är. Exempelvis genom att skicka falska mätvärden som indikerar motorfel, eller inget motorfel när det omvända förhållandet råder.

Denna rapport tar ingen hänsyn till hur ovanstående attacker utförs i detalj, utan fokuserar på typer av angrepp snarare än specifika exempel. Anledningen är som ovan nämndes att det utan en faktisk systemdesign inte går att säga vilka angrepp som är rimliga. I rapporten antas alltså ett värsta-fall-scenario där ingen intern säkerhet finns i systemet, utan systemet skyddas genom ett skalskydd av logisk separation genom brandväggar[14] och fysisk separation.

4.4 Spelkort

I appendix B och C av rapporten finns detaljerade listningar av olika angrepp och angripare som kan användas för att framställa spelkort till övningar eller för andra ändamål.

[14] Se Appendix A grundläggande IT-säkerhet

Rapporten tar upp sju olika mål som en angripare kan ha för att utföra cyberangrepp mot RPAS:

- Felnavigering i riktning eller höjd
- Avbrott i spaning
- Röjande signalering från RPAS
- Fysisk förstörelse av RPAS eller annat
- Vilseledning högre stab
- Vilseledning operatör
- Underrättelseinhämtning

För att få fram spelkort eller inspel att använda i simuleringar och övningar, väljs först ett av ovanstående mål som anfallet ska uppnå. Under rubriken för detta val finns en eller flera kombinationer av RPAS-modul och angrepp. Därefter väljs en angripare med lämplig kompetens från angripar-kapitlet

De angripartyper som listas i rapporten är

- Cybersoldaten
- Cyberbrottslingen
- Den omedvetne insidern
- Hämnaren/Den medvetne insidern

Om övningen eller simuleringen inte kräver en politisk eller övrig kontext behöver naturligtvis hela kedjan inte följas till slut.

5 RPAS – system i samverkan

I dagsläget agerar RPAS i huvudsak som isolerade system. En RPA kontrolleras via en kontrollstation (OCS) som i sin tur servas av ett par operatörer och ett bakomliggande arbetslag. Obemannad är ett mycket relativt ord när det gäller obemannade farkoster.

Det finns en tydlig utveckling att vilja få ut mer av RPA:er på olika sätt. Syftet bakom detta varierar men i stort är det en önskan om att få ut mer effekt i ett uppdrag eller av investeringen i systemet.

RPAS har stor bredd vad gäller förmåga och möjliga samverkansområden. De minsta RPAS:en kontrolleras av en enskild soldat och används för att få en lokal överblick över ett insatsområde medan stora och extremt uthålliga system nästan har en statisk karaktär och kontrolleras från en central plats. De system som avses i detta kapitel är av medelstorlek, det vill säga de har i normalfallet en central operatör och en uthållighet motsvarande en vecka.

I detta kapitel beskrivs ett antal samverkansformer mellan människor och RPA:er, bemannade system och RPA:er, RPA till RPA, samt civil samverkan med RPAS. Samverkansexemplen analyseras säkerhetmässigt och säkerhetsmässiga behov diskuteras.

5.1 Samverkansformer

Samverkan mellan system, vare sig de är bemannade eller obemannade, är inte trivialt. Det krävs att systemen är förberedda för informationsutbyte och att de kan förstå varandras information. Interoperabilitet är ett nyckelord men även inom interoperabilitet finns det nyanser då system kan vara interoperabla på flera sätt. I vissa fall är det inte tekniken som är gränssättande. Det kan vara så att ett system kan samverka med andra men att tilltron till dess förmåga inte har kunnat skapas. Då kan en förmåga även behöva mogna i användarnas och beslutfattarnas sinne.

Automation är en viktig egenskap vid samverkan med obemannade system. Utan automation är det fortfarande bara (fjärr-)bemannade system som samarbetar. Tanken med samverkan är att få ut något mer än vad som tidigare var möjligt, utan att tillföra traditionella resurser. Exempel på automation som fungerar väl idag är automatisk start och landning vilket är något som RPA:er gör bättre på egen hand än när de styrs av en operatör. Ett annat exempel som ännu inte är standard men som varit ett viktigt forsknings- och utvecklingsområde är förmågan att upptäcka andra föremål i luften och undvika dessa. Förmågan benämns med dess engelska namn ”sense and avoid”. Tekniker för att realisera förmågan har utvecklats på flera håll och försök har bland annat visat att tekniken och

människan är nästan jämbördig under bra sikt och väderförhållanden men att datorn får avsevärt bättre resultat när förutsättningarna försämras (Batey 2012).

Med automation kan en eller flera RPA:er kontrolleras utan att en operatör aktivt behöver styra dem. Målet med samverkan kan exempelvis vara att utöka sensorförmågan under ett uppdrag genom att en RPA följer en bemannad flygfarkost. I detta fall kontrolleras RPA:n helt eller delvis från den bemannade farkosten. Ett annat exempel kan vara att RPA:er samverkar med varandra i syfte att öka effektiviteten i ett uppdrag men att samtidigt kunna minska mängden operatörer som måste stödja uppdraget.

Nedan följer några exempel på möjliga samverkansmöjligheter mellan RPAS och andra system. En del av dessa är nära att bli operativa i dagsläget medan andra är mer på ett idéstadium.

5.1.1 Rotekamrat

Det koncept som kanske fått mest uppmärksamhet på senare tid är samverkan mellan en bemannad farkost och en RPA. En RPA agerar rotekamrat till den bemannade farkosten, något som har kallats ”loyal wingman” men numera ofta benämns som Man-Unmanned Teaming (MUM-T).

RPA:ns tänkta uppgifter är att stödja piloten i den bemannade farkosten med underrättelser, angrepp mot markmål och närskydd. Den kan också vara en vapenplattform vars syfte är att öka eller bredda eldkraften i roten (United States Air Force (USAF) 2009).

Genom att använda en RPA som sensorplattform uppnår piloten två tydliga fördelar. För det första exponerar sig inte den bemannade farkosten på samma sätt i och med att den kan använda RPA:ns sensorer. En radar utstrålar mer energi än en radio och kan upptäckas lättare än den radiotrafik med sensoruppgifter som skickas mellan RPA:n och piloten. För det andra utökas pilotens omvärdsuppfattning genom att RPA:n kan befinna sig långt framför piloten. Vid försök har videosändningar överförts mellan en RPA och en AH-64E Apache helikopter på mer än 100 kilometers avstånd (Van Riper 2014). Piloten blir då mer medveten om de förutsättningar som gäller på vägen mot, eller i, målet innan den bemannade farkosten behöver komma nära. Lösningen minskar risken för piloten.

5.1.2 Samarbetande RPA:er

Begreppet svärm avser att ett flertal RPA:er uppträder samlat och som en enhet. RPA:erna i svärmen kan vara självständiga och följa ett mål men samtidigt vara medvetna om omgivningen för att inte krocka med andra RPA:er. En operatör styr svärmen som en grupp men de enskilda RPA:erna är självständiga.

Det finns flera tillämpningar av svärmande RPA:er. Genom att en operatör kan styra RPA:erna som en grupp kan mängden operatörer minskas och därmed ge en ökad uthållighet för uppdrag (Drury & Scott 2008). Svärmar kan också användas för att genomföra koordinerade sökningar. I detta fall opererar ett antal RPA:er inom ett fördefinierat område men koordinerar själva sina rörelser inom området (Xiao, Dong, Wu & Duan 2012; Khan, Yanmaz & Rinner 2014) Svärmteknik har främst används för mindre RPA:er men tekniken kan även användas i större system och över större ytor.

Samarbetande RPA:er kan även effektivisera flygrutter. RPA:er som verkar i komplexa dynamiska miljöer med svår terräng och växlande hotbild kan utbyta uppgifter med varandra i syfte att optimera den tänkta flygrutten så att det egentliga målet nås (Zhang, Mao, Liu, Liu & Zheng 2013; Ortiz-Pena, Karwan, Sudit, Hirsch & Nagi 2013). Detta kan ses om en utveckling av MUM-T-konceptet genom att låta en RPA styras av en operatör och en eller flera RPA:er följa denna.

5.1.3 Samverkande sensor- och vapensystem

En RPA har, i alla fall jämfört med ett vanligt flygplan, en lång verkningstid. En Global Hawk har exempelvis en uthållighet på över 34 timmar (USAF 2014). Genom att placera RPA:er utanför normala täckningsområden kan en RPA med radar ge en tidigare förvarning eller komplettera bilden från andra sensorer. Denna kunskap kan användas för att förbereda motåtgärder mer dolt men även utan att exponera de skjutande delarna i förväg.

Idén med samverkan mellan sensor- och vapenplattformar är inte ny (John Hopkins APL Technical Digest 1995). Grundidén kopplar samman satelliter, flyg- och marksystem med fartygsystem i syfte att ge en mer komplett bild av omgivningen och därmed förbättra luftvärnsförmågan (United States Navy 2013). Tankarna har dock utvecklats till att omfatta fler scenarier, exempelvis på land för att förbättra lägesbilden.

5.1.4 Underhåll och logistik

Det görs flera ansträngningar på underhålls- och logistikområdet för RPA:er. Dessa ansträngningar syftar inte enbart till att stödja en RPA i luften utan även på marken. På sina håll har det även utvecklats tillämpningar där RPA:er är en del av underhållstjänsten.

Förmåga till lufttankning är ett viktigt mål för operativ användning av RPA:er. Med lufttankning kan den operativa tiden i luften förlängas och tid behöver inte läggas på att flyga fram och tillbaka till en markbas. På så sätt minskas behovet av antalet RPA:er som totalt är inblandade i en kontinuerlig operation. Framgångsrika försök har genomförts av Defense Advanced Research Projects

Agency (DARPA) och National Aeronautics and Space Administration (NASA) i syfte att påvisa RPA:ers möjligheter till precisionsflygning, vilket är en förutsättning för lufttankning (DARPA 2012).

Även underhållstjänsten på marken påverkas av automation. Hittills har automation syftat till att minska belastningen på operatörerna som flyger RPA:n, men automation kommer även att påverka underhållstjänsten. Markbaserade uppgifter såsom tankning och lastning av eventuell nyttolast (vapen eller sensorer) kan förväntas få en ökad automation (USAF 2009) vilket även innebär att de kan utnyttjas som plattform för angrepp. Sannolikt kommer den mänskliga kontakten med RPA:er att minska i det dagliga arbetet.

5.1.5 Informationsspridning

RPAS har än så länge främst använts för spaning och övervakning. I dagsläget samlas uppgifter in via operatörsstationens sensoroperatör och fördelas därefter vidare för analys, spridning och lagring. Detta resulterar i en fördröjning från det att uppgifter samlas in till dess att de når de enheter som verkar i området som uppgifterna avser. Från befälhavares perspektiv finns det ett ständigt behov av mer detaljerade uppgifter om det insatsområde uppdrag utförs inom.

En målsättning, i alla fall från amerikanskt håll, är att få ut mer nytta av en RPA genom att nyttja uppgifter från dess sensorer även när den flyger till och från sitt primära uppdrag. Inom detta koncept ingår även att ytterligare nyttja andra sensorer som RPA:n bär med sig när den befinner sig i målområdet. Sensordata tappas av direkt och i sådant format att det snabbare kan nå befälhavare men även soldatburna system och därmed ge ökad förståelse för den miljö mottagaren verkar i (Department of Defence (DOD) 2013). Det engelska begreppet för detta är Battlespace Awareness.

Framtida RPA:er bör kunna konfigureras om för olika typer av uppdrag. I dagsläget är en modell av en RPA bunden till de sensorer som ingår i konfigurationen. En mer modulorienterad design ger befälhavaren möjlighet att styra uppdrag efter behov mer än i nuläget. Samtidigt ställer detta krav på RPA-tillverkare att separera farkosten och kommunikationskanalen från sensorspecifika lösningar.

5.1.6 Civil nytta

När RPAS används i fredstid för nationellt bruk skulle sensoruppgifter kunna utnyttjas även för civila behov. På samma sätt som att helikoptrar används idag för att stödja samhället vid exempelvis en skogsbrand, kan RPA:er stödja samhället (Isenor, Allard, Lapinski, Demers & Radulescu 2014). Vid enstaka tillfällen krävs ingen anpassning för en sådan verksamhet, men vid ett mer

regelbundet informationsutbyte krävs att uppgifterna från RPA:n kan göras tillgängliga på ett smidigt sätt.

Ett nationellt utnyttjande innebär även att RPA:n uppträder i kontrollerat luftrum på samma sätt som bemannade flygfarkoster gör. Framtida luftövervakning avser blir mer informationstät i syfte att kunna hantera en förväntad ökning av trafik–volymen. Genom att koppla samman flygplan, kontrolltorn, meteorologitjänster med mera, och låta dessa kommunicera digitalt är målsättningen att flyget skall bli mer effektivt (Luftfartsverket 2014). För RPAS innebär detta att en RPA, och sannolikt även dess kontrollstation, måste kunna kommunicera digitalt med flera olika instanser.

5.2 Kommunikationsbehov

Baserat på de tillämpningar av RPAS nu och i framtiden som presenterades i avsnitt 5.1 har ett antal kommunikationsfall identifierats. De kommunikationsfall som presenteras i detta avsnitt avser någon form av datortrafik. Det innebär att det är inne-hållet i trafiken som är av primärt intresse. Yttre påverkan av kommunikationen, såsom störning av signalen eller avlyssning, ligger utanför cybersäkerhetens ansvar att hantera.

5.2.1 RPA och kontrollstation

Kommunikationen mellan RPA:n och kontrollstationen (eng. Operator Control Station (OCS)) är den mest uppenbara kanalen att skydda. Från OCS:en till RPA:n skickas styrsignaler för att manövrera RPA:n samt styra sensorer. RPA:n skickar lägesuppgifter om sin situation och uppgifter från sensorer.

Denna kommunikation kan delas in i två delar; bärarkommunikation och datakommunikation. Bärarkommunikationen är kanalen som skapas mellan RPA:n och OCS:en. Denna kanal tar egentligen inte någon hänsyn till vilken typ av trafik som transporteras inom kanalen utan kapslar in de data som överförs och behöver bara kunna kommunicera med systemens ytterpunkter. Data-kommunikationen å andra sidan kan ha olika mottagare i form av olika mottagar-system hos OCS:en. Det är inte ovanligt att datatrafiken är oskyddad då bärarkanalen kan förse överföringen med ett trafikskydd. Så har dock inte alltid varit fallet. Det finns exempel där trafiken varit helt oskyddad, exempelvis avslöjandet om att insurgenter i Irak hade kommit över videoflöden från amerikanska Predatorer (Gorman, Dreazen & Cole 2009).

5.2.2 RPAS och andra militära system

Underrättelser och underlag för att skapa ett större medvetande om situationen fångas upp av RPA-sensorer och skickas vidare via OCS och dess analys–

organisation. Det finns även exempel på när videoflöden skickas direkt till mottagare inom spaningsområdet.

För att uppnå en hög grad av informationsspridning direkt från en RPA behöver radiokanalen och dataformaten vara utformade så att flera system kan tolka dessa. Det finns ett behov av att ensa dataformat så att uppgifter ifrån sensorer av samma typ kan jämföras med varandra. Sensorer har allt som oftast tillverkarspecifika dataformat (DOD 2013) vilket gör att liknande sensoruppgifter från olika plattformar blir svårare att analysera effektivt.

Kommunikation från en RPA:s sensorer kan mycket väl spridas från OCS:ens analysenhet eller det informationsdelningssystem som finns etablerat. Ett ökat avstånd från sensor till mottagare ökar dock risken för att uppgifter blir fördröjda eller inte kommer fram alls.

I en framtid med en högre grad av automation kommer RPA:n även att behöva kommunicera med omgivande underhållssystem, exempelvis vid marktankning.

5.2.3 RPA till RPA

Med en högre grad av automation även för RPA:er kan dessa själva lösa problem under pågående uppdrag. Det innebär att de kan behöva vara medvetna om varandra men även kommunicera direkt för att besluta om rutter och optimera sökningar.

Även i luften kommer underhållssystem att vara aktiva, exempelvis genom lufttankning. Detta är en uppgift som inte nödvändigvis behöver automatiseras men sannolikt kan en automatiserad tankningsprocess vara lämplig för obemannade system på samma sätt som att automatisk start och landning är effektivare.

5.2.4 RPAS och civila system

I takt med att RPAS integreras mer i nationellt luftrum kommer mer kommunikation med civila system att krävas. RPA:n måste kunna fånga upp anrop från civil flygledning även om det är operatören som utför de instruktioner som den civila flygledningen ger. Efterhand som moderniseringen av flygledningen inom Europa blir operationell kommer kommunikationsmetoden att förändras. Från att i huvudsak varit talbaserad kommer ett digitalt meddelandesystem att införas (Luftfartsverket 2014).

En utökad kommunikation med civila system kan innebära att RPA:n kommunicerar direkt med det civila systemet, men det kan även ske via kontrollstationen eller de militära ledningssystemen. En utökad digital kommunikationsförmåga i allmänhet och standarder avgör i vilken grad som kommunikation kan ske utan omvägar.

5.3 Säkerhetsanalys

RPAS är ett komplext system med flera mer eller mindre oberoende enheter som samverkar. I en framtida version kan en hög grad av automation förväntas och inom en inte alltför lång framtid även en större civil-militär samverkan, främst vid flygning i kontrollerat luftrum. Det är därför viktigt att studera behov av säkerhet ur ett helhetsperspektiv, det vill säga ett perspektiv där fokus inte enbart ligger på RPA:n, eller ens dess omedelbara närhet.

5.3.1 Traditionella cybersäkerhetsproblem

Traditionell cybersäkerhet innebär förmågan att bevara sekretess, riktighet och tillgänglighet för information och system. RPAS i sig självt är ett system med stor spridning av de ingående delsystemen. Avstånd är dock inte något som påverkar en angripare negativt då de oftast inte behöver fysisk åtkomst till systemen som angrips. Om det finns en möjlighet att kommunicera så har det ingen betydelse hur långt signaler och kommandon behöver färdas.

Fysisk åtkomst till ett system, exempelvis RPA:n eller något stödsystem, är dock en stor fördel. Har dessutom en angripare tillgång till ett system utan tidspress, det vill säga där angriparen ostört kan försöka komma åt innehållet i ett system, är det rimligt att anta att en kompetent angripare förr eller senare kommer att komma åt den information som finns lagrad i det aktuella systemet.

5.3.2 Specifika RPAS-säkerhetproblem

RPAS är till viss del ett vanligt IT-system innehållande programvara, datorer och nätverk men det går också att till viss del även se RPAS som ett cyberfysiskt system. Det går också att se RPAS som ett ledningssystem där effekten är underrättelser från luften.

De samverkansformer som föreslogs i avsnitt 5.1 kan visserligen analyseras ur ett rent tekniskt perspektiv, men då detta är en rapport som avser diskutera RPAS ur ett framtidsperspektiv analyseras RPAS nedan med en helhetssyn.

Kommunikation mellan RPA, kontrollstation och andra militära system.
Kanalen mellan operatören och RPA:n är den mest uppenbara kanalen att skydda men även angripa. Ur ett cyberangreppsperspektiv är det dock inte nödvändigtvis kanalen i sig som är intressant om angriparen utan målet kan istället vara att ta kontroll över operatörsplatsen (OCS) och skicka trafik som en legitim operatör till RPA:n.

I dagsläget är det normala att en operatör styr en RPA. Det är rimligt att anta att framtida RPA:er har en högre grad av autonomitet vilket möjliggör för en operatör att styra flera RPA:er samtidigt. Det finns en risk med att distansera människan från RPA:n, då det kan bli svårare att upptäcka ett avvikande

beteende hos enskilda RPA:er. Säkerhetsfunktioner såsom intrångsdetektering och tröghetsnavigering kan visserligen mottverka effekten av angrepp, men människor är ofta bra på att upptäcka avvikelser.

En RPA kan behöva kommunicera direkt med andra militära system. Den taktiska sidan av detta omfattar att kunna dela kontroll alternativt låta kontrollen av en RPA helt skötas från en bemannad farkost. Ett framtida system med bemannat och obemannat i kombination realiseras troligen med en mer automatiserad rotekamrat. Användningen av RPA:er tillsammans med bemannade farkoster innebär förmodligen att RPA:n utsätts för en högre exponering, exempelvis genom att operera närmre fientliga grupperingar. Ett sådant risktagande är visserligen naturligt för ett obemannat system med det ställer krav på den fysiska säkerheten i RPA:n. Risken för att RPA:n kommer att bli bekämpad, eller på annat sätt tvingas landa, ökar och då måste de system som innehåller och skyddar information ombord klara av att en angripare får fysisk kontroll över systemen.

En annan sida av kommunikation med militära system är kommunikation med underhållssystem. Automatisering omfattar inte enbart RPA:er utan kan även omfatta stödsystem på ett flygfält. System för taxning och tankning har en annan säkerhetsnivå och kan utgöra mål för att störa verksamheten.

Kommunikation från RPA till RPA. RPA:er som kommunicerar med varandra är visserligen en variant av kommunikation mellan militära system men medför att en större datamängd lagras i en RPA. Samverkande RPA:er delar uppgifter och kan även lokalt processa information innan informationen distribueras vidare till en kontrollstation eller något annat system.

Kommunikation med civila system. Civila flygledningssystem har historiskt prioriterat flygsäkerheten när ledningssystem och flygplan skapats. Den primära kommunikationskanalen har varit röst över radio samt signalsystem. Moderniseringen av flygledningssystemen medför att textbaserad datatrafik kommer att sändas direkt till flygplan från flera källor. Genom att införa datatrafik möjliggörs angrepp som tidigare inte varit möjligt. Det gör cybersäkerhet till något som kan påverka flygsäkerheten.

De flygledningssystem som skapas idag hämtar uppgifter från flera system vilket gör att de möjliga angreppsvägarna blir många. Cybersäkerhetsnivån i de omkringliggande systemen har inte nödvändigtvis samma krav på sig som ett system i, eller i direktanslutning till, en RPA.

6 Slutsatser

I detta kapitel presenteras de slutsatser som dragits från tidigare kapitel.

6.1 Cyberangrepp mot RPAS

Ett RPAS är inte en enhet utan ett system av system. I detta system av system ingår farkoster, operatörsstationer, kommunikationslänkar och sensorer. Dessa system ingår i sin tur i ett större system av IT-system som luftförsvarsledning, luftstridsledning, Försvarsmaktens Telesystem och så vidare. Själva farkosten är bara en nod i nätverket.

Ett cyberangrepp i allmänhet sker inte direkt mot det system som är målet. Detta är inte ett medvetet val utan oftast en nödvändighet. En angripare identifierar först en väg in i ett system och därefter en metod att nå aktuellt målsystem. Det gör att vägen från infiltrering i ett system till dess att verkan uppnås kan vara ganska lång. I och med att cyberangrepp är en indirekt metod krävs noggranna förberedelser och en hel del chanstagning.

Cybermiljön är inte enbart teknisk utan innehåller även en social domän med användare. För en angripare innebär detta att även användare utgör mål för informationsinhämtning och, medvetet eller omedvetet, utförande av tjänster.

6.2 System i samverkan

Ett RPAS är ett system som oftast har en större geografisk spridning, exempelvis genom skilda start- och landningsplatser, kontrollplatser och verkansområden. Med undantag av själva RPA:n kan övriga enheter i RPAS skyddas fysiskt av teknik och människor men RPA:n kan vara utsatt i de fall den tvingas landa på fientligt område. Det medför att skyddet av information som finns i RPA:n måste vara starkt och tåla att en angripare med fysisk åtkomst till lagringssystemen kan försöka utvinna information över tiden. Behovet av ett starkare informationsskydd ökar också i takt med att mer information sannolikt lagras lokalt. Om RPA:er börjar samverka och utbyta uppgifter i planeringssyften kommer mängder av sannolikt kritiska data finnas lagrad lokalt.

Civil samverkan är ofrånkomligt om RPA:er skall operera i kontrollerat luftrum. Med kommande luftledningssystem ökar även mängden ingångsvägar till en RPA och RPAS som helhet. Detta gör att det finns ett tydligt behov i kravställnings- och säkerhetsarbetet att tydliggöra vilka system som tillåts kommunicera och vilken typ av information ett system skall tillåta påverka systemet.

6.3 Gemensamma slutsatser

Då RPAS utgörs av flera delsystem är det viktigt att studera helheten när risk- och säkerhetsarbeten genomförs. Alla de gränssnitt där operatörer, informationskällor och servicepersonal interagerar med RPAS eller direkt med RPA:n utgör möjliga angreppsytor för ett angrepp. Det är inte enbart de gränssnitt som är kopplade direkt till RPAS som behöver granskas utan även de som finns tidigare i utvecklings- och underhållssystemen. I och med att ett cyberangrepp oftast sker i flera steg och startar där skyddet är som lägst bör hela kommunikationskedjan analyseras och kontrollfunktioner införas där det är möjligt.

Försvarsmakten som systemägare kan bedriva ett aktivt och preventivt säkerhetsarbete genom bland annat kravställning inför upphandling och utveckling, men även genom noggrant utformade säkerhetsrutiner. Kravställningar kan omfatta vilka system som får kommunicera med varandra men bör även ta upp vilken kommunikation som ett system skall acceptera.

Referenser

Air Force Space Command (2011). *Flying operations of remotely piloted aircraft unaffected by malware*. 12 oktober. http://www.afspc.af.mil/news/story.asp?id=123275647 [2014-12-09]

Albright, D. & Hinderstein, C. (2003). The Iranian Gas Centrifuge Uranium Enrichment Plant at Natanz: Drawing from Commercial Satellite Images. *The Institute for Science and International Security (ISIS)*, 14 mars. http://www.isis-online.org/publications/iran/natanz03_02.html [2014-12-14]

Albright, D., Stricker, A. & Walrond, C. (2010). IAEA Iran Safeguards Report: Shutdown of Enrichment at Natanz Result of Stuxnet Virus?; Downgrade in Role of Fordow Enrichment Site; LEU Production May Have Decreased. *The Institute for Science and International Security (ISIS)*. http://isis-online.org/uploads/isis-reports/documents/IAEA_Iran_Safeguards_Report_ISIS_analysis_23Nov2010.pdf [2014-12-14]

Applegate, S.D. & Stavrou, A. (2013). Towards a Cyber Conflict Taxonomy. I *CyCon 2013, Proceedings of the 5th International Conference on Cyber Conflict*. Tallinn, Estland 4-7 juni 2013, ss. 1-18.

Batey, A. (2012). 2Excel Aviation Gives Drones Virtual Eyes. *Businessweek*, 22 mars. http://www.businessweek.com/articles/2012-03-22/2excel-aviation-gives-drones-virtual-eyes [2014-12-17]

Defense Advanced Research Projects Agency (DARPA) (2012). *Making connections at 45 000 feet: future UAVs may fuel up in flight*. 5 oktober. http://www.darpa.mil/NewsEvents/Releases/2012/10/05.aspx [2014-12-07]

Defense Science Board (DSB) (2013). *Resilient Military Systems and the Advanced Cyber Threat*. Washington: Department of Defence.

Department of Defence (DOD) (2013). *Unmanned Systems Integrated Roadmap: FY2013-2038*.

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

Drury, J.L. & Scott, S.D. (2008). Awareness in Unmanned Aerial Vehicle Operations. *The International C2 Journal*, 2(1), ss.1-28.

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

Försvarsmakten (2013). *Handbok Försvarsmaktens säkerhetstjänst, Informationssäkerhet*. Stockholm: Försvarsmakten.

Gorman, S., Dreazen, Y.J. & Cole, A. (2009). Insurgents Hack U.S. Drones. *The Wall Street Journal*, 17 december. http://www.wsj.com/articles/SB126102247889095011 [2014-12-07]

Gross, M.J. (2011). A Declaration of Cyber-War. *Vanity Fair*, 1 april. http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104 [2014-12-17]

Hand, R., Ton, M. & Keller, E. (2013). Active Security. I *Hotnets-XII, Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks*. College Park (MD), USA 21-22 november 2013. DOI: 10.1145/2535771.2535794

Isenor, A.W., Allard, Y., Lapinski, A-L.S., Demers, H. & Radulescu, D. (2014). Coordinating UAV information for executing national security-oriented collaboration. I *SPIE 9248, Proceedings of Unmanned/Unattended Sensors and Sensor Networks X*, 92480L. Amsterdam, Nederländerna, 22 september 2014. DOI: 10.1117/12.2067066

John Hopkins APL Technical Digest (1995). *The Cooperative Engagement Capability*. 16(4).

Keizer, G. (2010). Is Stuxnet the 'best' malware ever? *Computerworld*, 16 september. http://www.computerworld.com/article/2515757/malware-vulnerabilities/is-stuxnet-the--best--malware-ever-.html [2014-12-11]

Khan, A., Yanmaz, E. & Rinner, B. (2014). Information merging in multi-UAV cooperative search. I *ICRA'14, Proceedings of the IEEE International Conference on Robotics and Automation*. Hong Kong, Kina 31 maj-7 juni 2014, ss. 3122-3129. DOI: 10.1109/ICRA.2014.6907308

Lamonte, J. (2009). The Future of UAVs. Från en presentation under *RUSI Air Power conference "RUSI The Future of UAVs: Concepts and Considerations"*. London, Storbritannien 19-20 oktober 2009. http://www.raf.mod.uk/role/thefutureofuav.cfm [2014-12-11]

Langner, R. (2013). *To Kill a Centrifuge - A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf [2014-12-17]

Luftfartsverket (2014). *SESAR*. http://www.lfv.se/sv/Internationellt/Sesar/ [2014-12-07]

McDonald, G., O'Murchu, L., Doherty, S. & Chien, E. (2013). *Stuxnet 0.5: The Missing Link.* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf [2014-12-14]

Mills, E. (2010). Stuxnet: Fact vs. theory. *CNET*, 5 oktober. http://www.cnet.com/news/stuxnet-fact-vs-theory/ [2014-12-17]

Nakashima, E. & Warrick, J. (2012). Stuxnet was work of U.S. and Israeli experts, officials say. *The Washington Post*, 2 juni. http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html [2014-12-09]

Newman, L.H. (2013). Can You Trust NIST? *IEEE Spectrum*, 9 oktober. http://spectrum.ieee.org/telecom/security/can-you-trust-nist [2014-12-09]

Ortiz-Peña, H.J., Karwan, M., Sudit, M., Hirsch, M. & Nagi, R. (2013). A multi-perspective optimization approach to UAV resource management for littoral surveillance. I *FUSION'13, Proceedings of the 16th International Conference on Information Fusion*. Istanbul, Turkiet 9-12 juli 2013, ss. 492-498.

Olsson, E. (2012). ”Assange-konflikt ökar attacker”. *Svenska Dagbladet*, 1 oktober. http://www.svd.se/nyheter/inrikes/it-polis-assange-konflikten-har-okat-attackerna_7545246.svd [2014-12-14]

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. https://www.dhs.gov/sites/default/files/publications/csd-day-1-08-part-1-canada-turcotte.pdf [2014-12-11]

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

United States Air Force (USAF) (2014). *RQ-4 Global Hawk*. 27 oktober. http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104516/rq-4-global-hawk.aspx [2014-12-17]

United States Navy (2013). *CEC - Cooperative Engagement Capability*. 15 november. http://www.navy.mil/navydata/fact_print.asp?cid=2100&tid=325&ct=2&page=1 [2014-12-07]

Van Riper, S.G. (2014). Apache Manned-Unmanned Teaming Capability. *Army Magazine*, 64(9), 51-52.

Xiao, X., Dong, Z., Wu, J. & Duan, H. (2012). A Cooperative Approach to Multiple UAVs Searching for Moving Targets Based on a Hybrid of Virtual Force and Receding Horizon. I *INDIN'12, Proceedings of the 10th IEEE International Conference on Industrial Informatics*. Peking, Kina 25-27 juli 2012, ss. 1228-1233. DOI: 10.1109/INDIN.2012.6301188

Zhang, B., Mao, Z., Liu, W., Liu, J. & Zheng, Z. (2013). Cooperative and Geometric Learning for path planning of UAVs. I *ICUAS'13, Proceedings of the International Conference on Unmanned Aircraft Systems*. Atlanta (GA), USA 28-31 maj 2013, ss. 69-78. DOI: 10.1109/ICUAS.2013.6564675

Appendix A Grundläggande IT-säkerhet

Enligt Handbok Försvarsmaktens säkerhetstjänst, Informationssäkerhet avses IT-säkerhet vara ” åtgärder som syftar till att uppnå och vidmakthålla den nivå av säkerhet som … verksamhetens behov ställer på ett IT-system”. (Försvarsmakten 2013, s. 235). Detta sker genom att säkerställa tillgänglighet, riktighet, sekretess, autenticitet, oavvislighet och spårning.

Förenklat kan ovanstående beskrivas som att information ska finnas tillgänglig för den som behöver den, när informationen behövs, på ett sådant sätt att användaren kan vara säker på att informationen är korrekt och veta var den kommer ifrån. Dessutom ska en utredare i efterhand kunna avgöra vem som gjort vad, när, och vilken information som varit inblandad.

Detta är inget enkelt problem eftersom målkraven är ömsesidigt uteslutande.

A.1 Total säkerhet finns inte

Om de tre grundkraven sekretess, riktighet och tillgänglighet betraktas, så innebär hög riktighet att det måste finnas spärrar för vem som får införa eller ändra data i systemet. Dessa säkerhetsåtgärder innebär förseningar och försämringar av tillgängligheten.

På samma sätt innebär autentiseringskontroller, alltså att en användares identitet och behörighet kontrolleras innan denne får tillgång till data, att tillgängligheten försämras.

Det är normalt så att alla säkerhetsåtgärder inom IT-området innebär en kompromiss mellan att förbättra en aspekt av säkerheten på bekostnad av en annan. Målet för IT-säkerheten måste alltså vara att den totala effekten av åtgärder leder till en så hög säkerhet som möjligt med hänsyn tagen till verksamhetens krav.

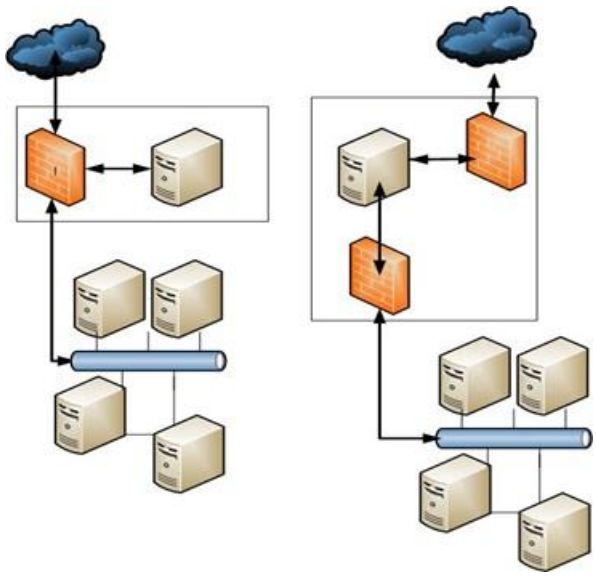
A.2 Exempel på åtgärder

Ämnet IT-säkerhet är så stort att fleråriga utbildningar inte kan täcka alla delar. I denna rapport beskrivs endast de vanligaste åtgärderna som används för att skydda IT-system.

A.2.1 Brandväggar

Termen brandvägg är egentligen felaktig då det inte är en spärr (vägg), utan snarare ett kommunikationsfilter. En brandvägg är en dator som exempelvis kopplas in mellan två datornät. Den kontrollerar all kommunikation mellan dessa

två nät och försöker avgöra vilka data som bör tillåtas passera och vilka som bör stoppas. I teorin är detta enkelt men i praktiken är datorprotokoll och moderna datormiljöer så komplexa att inställningarna av brandväggar blir en av de viktigaste åtgärderna för att balansera säkerhet och fungerande arbetsmiljö.



Figur 5 DMZ – Exempel på uppbyggnad

Ofta placeras brandväggar tillsammans med speciella kommunikationsservrar för till exempel e-post, webbtjänster och liknande i en grupp som kallas DMZ, *De-militarized-zone* (Figur 5). Denna möjliggör en förenkling av säkerhetsarbetet genom att datorer på den säkra sidan får tillstånd att kommunicera med dessa servrar, men inga andra. Dator på det osäkra nätet får kommunicera med DMZ-servrarna men aldrig med datorer på det säkra nätet.

A.2.2 Nätverkssegmentering

Hur datornätverken byggs upp fysiskt och logiskt är en viktig punkt i säkerhets-arbetet. Generellt gäller att datornäten bör byggas så att datorer som av någon anledning är mer skyddsvärda ska sitta på separata nätverk, avskilda med brandväggar från de mindre skyddsvärda. Detta för att förenkla övervakning och möjliggöra så kallad ö-drift: Uppdelningen i mer och mindre skyddsvärda segment (öar) innebär att vid ett misstänkt intrång i eller närvaro av skadlig kod i systemet kan kommunikation mellan essentiell drift och mindre viktiga enheter som kontorsnätverk tillfälligt stänga av all medan rensning pågår.

A.2.3 Autentisering

För att garantera att data överförs endast till behöriga användare används autentiseringsmetoder för att garantera att användare är de som de utger sig för att vara. Ofta används lösenord, en metod som i sig inte är särskilt säker. Det finns många kända angrepp som ger goda resultat och människor är notoriskt dåliga på att välja bra lösenord.

Bättre resultat uppnås när systemet kombinerar något användaren vet – som ett lösenord – med något användaren har – som en nyckel eller ett magnetkort. Att kombinera metoder ger en högre säkerhet än när metoderna används var för sig.

Att mäta något användaren är, till exempel irismönster, fingeravtryck eller annan *biometri* kan användas men bör alltid kombineras med någon av de andra två metoderna. Det bör dock påpekas att biometri har den dubbla nackdelen att mätvärdena normalt inte är hemliga. Fingeravtryck lämnas hela tiden, och irisavläsningar går att göra med vanliga teleobjektiv. Dessutom, skulle systemet bli hackat och en angripare stjäla databasen med mätvärden är det svårare att byta ut kroppsdelar jämfört med ett lösenord eller ett plastkort

A.2.4 Intrångsdetekteringssystem

Nätverksbaserade intrångsdetekteringssystem är funktionalitet som placeras så centralt i nätverken som möjligt. De liknar brandväggar i det att de analyserar datatrafik, men deras enda uppgift är att försöka upptäcka att en angripare använder systemet. De kan fungera så enkelt som att ligga passiva, utan annan funktion än att larma om någon dator försöker kommunicera med dem över huvud taget, så kallade *kanariefåglar* eller *snubbeltrådar.* Andra änden av spektrumet är de intrångsdetekteringssystem (IDS) som analyserar trafikflöden i nätverket över tid och inte bara försöker hitta trafikmönster som liknar kända angrepp utan också lär sig organisationens trafikrytmer och larmar om till exempel en dator som begär åtkomst till data utanför kontorstid när den aldrig brukar göra det.

Just militära organisationer brukar få problem med den senare typen av IDS:er eftersom arbetet under normala förhållanden och vid ett skarpt krisläge skiljer sig så dramatiskt åt. IDS:er bör således ”tränas” på att skilja mellan normal- och ”krigsläge” genom att explicit låta den spela in en serie övningar.

A.2.5 Intrångspreventionssystem

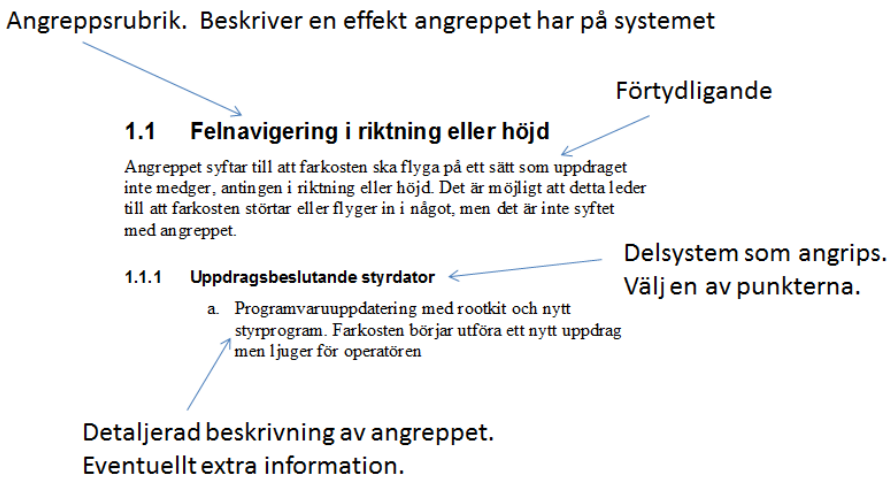
Med en utökning av funktionaliteten hos en IDS, erhålls en Intrångspreventions-system (IPS). Dessa skiljer sig åt i att IPS:en förutom att larma om ett intrång också försöker stoppa det genom att till exempel bryta trafikflöden. Det är av vital vikt att dessa åtgärder anpassas efter organisationens krav eftersom en

felaktigt inställd IPS kan utföra tillgänglighetsangrepp mot den egna organisationen när den försöker stoppa en angripare.

Experiment har gjorts med att låta IPS:er inte bara utföra åtgärder inom det egna nätverket, utan också försöka utföra motangrepp (Hand, Ton & Keller 2013). Denna funktionalitet har både juridiska och politiska problem. De praktiska problemen är också många, till exempel att en angripen dator i en egen organisation kan användas för fjärrstyrda angrepp som leder till motangrepp vilket gör att metoden måste användas med största försiktighet.

Appendix B: Angrepp

Detta appendix listar angreppstyper som kan användas vid konstruera av spelkort, se exempel i Figur 6. Välj en önskad angreppseffekt och välj sedan en av underpunkterna som beskriver angripet delsystem och detaljer av angreppet. Kombinera detta med ett val ur angriparappendix, Appendix C, för fullständiga spelkort.



Figur 6 Struktur för att skapa spelkort.

B.1 Felnavigering i riktning eller höjd

Angreppet syftar till att farkosten ska flyga på ett sätt som uppdraget inte medger, avseende i riktning eller höjd. Det är möjligt att detta leder till att farkosten störtar eller flyger in i något, men det är inte syftet med angreppet.

B.1.1 Uppdragsbeslutande styrdator

- Programvaruuppdatering med rootkit och nytt styrprogram. Farkosten börjar utföra ett nytt uppdrag men ljuger för operatören.
- Falsksändning av intern modul som utger sig för att vara navigationsmodulen. Farkosten försöker återgå till originalkurs men navigerar efter felaktiga koordinater. Farkosten påstår för operatören att den är vid korrekta koordinater.

- Falsksändning från intern modul som låtsas vara kommunikations-modulen med styrorder från markstationen. Farkosten följer de nya orderna och meddelar operatören den nya kursen och verkliga koordinater.
- DoS som hindrar kommunikation med styrdatorn. Angreppet gör att farkostens delar fortsätter att vara aktiva i samma tillstånd som när störningen började. Fortsätter DoS över tid kommer farkosten att störta av bränslebrist eller flyga in i terräng.

B.1.2 Motorstyrning

- Programvaruuppdatering med rootkit och nytt styrprogram. Motor-styrningen börjar utföra nya operationer men ljuger för styrdatorn. Motorn kan stängas av, minska eller öka gaspådrag så att höjd ändras. Farkosten kan störtas om motorn stängs av.
- Falsksändning av styrdata från en intern modul. Samma effekt som ovan, men styrdatorn får utdata som anger motorns verkliga beteende och kan gå in och försöka rätta till problemet. För den mänskliga operatören verkar felet ligga i motorn.
- DoS från en intern komponent gör att motorstyrningen inte kan ta emot instruktioner från styrdatorn. Varv och effekt ligger kvar på samma nivå tills DoS avslutas. Fortsätter DoS över tid kommer farkosten att störta av bränslebrist eller flyga in i terräng.

B.1.3 Navigationsmodul

- Programvaruuppdatering med rootkit och nytt styrprogram gör att modulen lämnar ut felaktiga data till uppdragsmodulen. Farkosten försöker utföra sitt uppdrag men flyger till fel plats och/eller höjd. Den mänskliga operatören kan, om hon har extern information till exempel från radar, se att navigationen inte fungerar. Effekten på farkosten är liknande den som uppstår vid extern falsksändning av GPS-data.
- DoS – modulen får sin indatakanal störd av en annan intern modul och resultatet blir att den inte kan svara på anrop från styrdatorn och lämnar inte ut koordinater. Effekten är densamma som om enheten stängts av. Farkosten försöker meddela operatör om läget men bibehåller riktning och höjd tills extern styrning sker. Läget liknar det som uppstår vid telekrigsstörning mot GPS, men även tröghetsnavigeringen upphör att fungera.

B.1.4 Roderstyrning

- Programvaruuppdatering med rootkit och nytt styrprogram gör att rodren inte ligger an i de vinklar som de ska och farkosten kommer att utföra manövrar som rollar, loopar, stokastiska kursändringar eller dylikt men påstår att allt är normalt. Operatören ser vad som verkligen sker men får ingen feluppgift om varför farkosten beter sig så. Ett alternativ är att farkosten börjar flyga ett nytt uppdrag på död räkning – det vill säga att vid en viss tidpunkt svänger den en viss tid med visst roderutslag och så vidare vilket ger intrycket av att den fjärrstyrs.
- Falsksändning mot roderstyrningen från en intern enhet. En annan modul skickar styrorder till modulen som utför dem i tron att det är styrdatorn som skickar orderna. Effekten är densamma som ovan men styrdatorn kan försöka gå in och styra upp situationen. Felet ger intryck av att ligga i roderstyrmodulen.

B.1.5 Operatörsstationer, OCS för användargränssnitt

- Programvaruuppdatering med rootkit och nytt styrprogram tar emot indata från farkosten och presenterar felaktiga data för operatören för att få denne att skicka ut styrorder baserat på det falska läge som presenteras. Alternativt visar programmet en bild för operatören av att uppdraget framskrider som beräknat men skickar ut falska styrorder till farkosten för att förmå den att ändra höjd eller riktning.
- Falsksändning av data som ser ut att komma från farkosten men som sänds från en enhet på det lokala nätverket. Dessa tas emot och presenteras för operatören som om det vore den verkliga situationen för att få denne att skicka ut styrorder baserat på det falska läge som presenteras.

B.1.6 Styrning och telemetri

- Programvaruuppdatering med rootkit och nytt styrprogram får modulen att sända styrorder till farkosten som får den att utföra manövrar som ändrar dess riktning och höjd samtidigt som modulen sänder data till operatörsstationen som visar att uppdraget fortskrider enligt plan.
- Falsksändning gällande styrning – en enhet på det lokala nätverket sänder falska styrorder som ser ut att komma från operatörsstationen. Dessa sänds vidare till farkosten som försöker utföra dem.
- Falsksändning gällande data – en enhet på det lokala nätverket sänder falska data som verkar komma från farkosten. Beroende på vad som sänds kommer stationen antingen att skicka korrigeringar till farkostens

kurs, höjd och motoreffekt, reläa dem till operatörsstationen och ge operatören en falsk lägesbild, eller båda.

- DoS – en enhet på det lokala nätverket skickar data i stor mängd som hindrar telemetridatorn att ta emot styrorder. Farkosten fortsätter med uppdraget så länge angreppet varar. Ur operatörens synvinkel ser det ut som om farkosten inte kan ta emot sändningar. Angreppet är meningsfullt endast om operatören velat göra avsteg från uppdraget.

B.1.7 Radiokomdator

- Programvaruuppdatering med rootkit och nytt styrprogram gör att datorn ersätter telemetridatorns styrorder med andra för att få farkosten att ändra höjd och riktning på ett felaktigt sätt.
- Falsksändning gällande styrning – en enhet på det lokala nätverket skickar data som verkar komma från operatören i form av styrorder. Farkosten följer de nya orderna och sänder tillbaka korrekt information om ny position och kurs.
- DoS – en enhet på det lokala nätverket skickar data i stor mängd som hindrar telemetridatorn att ta emot styrorder. Farkosten fortsätter enligt planerat uppdrag så länge angreppet varar. Ur operatörens synvinkel ser det ut som om farkosten inte kan ta emot sändningar. Angreppet är meningsfullt endast om operatören velat göra avsteg från uppdraget.

B.2 Spaningsavbrott

Angreppet syftar till att RPAS förmåga till spaning ska minska eller upphöra under hela eller delar av uppdraget. Skador kan uppstå som ett resultat av angreppet men det är inte målet med angreppet.

B.2.1 Uppdragsbeslutande styrdator

- Programvaruuppdatering med rootkit och nytt styrprogram som skickar styrorder till sensormodulen att sensorerna ska stängas av när de borde vara påslagna. Programmet ljuger för operatörerna så att det verkar som att sensormodulen fallerat.
- Falsksändning gällande styrning – en intern modul skickar data som verkar komma från kommunikationsmodulen i form av styrorder. Farkosten följer de nya orderna och sänder tillbaka korrekt information om ny position och kurs.

- Falsksändning gällande data – en intern modul skickar data som verkar vara information från navigationsmodulen. Styrdatorn tror att farkosten är på fel plats och startar aldrig sensorerna. Farkosten kommer att meddela operatören den falska positionen och manövrera för att komma till ”rätt” plats.
- DoS – en intern modul sänder ut data till styrdatorn så att den inte kan ta emot annan trafik. Farkosten fortsätter i samma läge till dess att DoS-angreppet slutar. Farkosten slutar att kommunicera med operatören under angreppet. Om angreppet fortsätter kan flygning in i terräng på grund av bränslestopp ske.

B.2.2 Motorstyrning

- Programvaruuppdatering med en rootkit och nytt styrprogram ändrar motorns effekt, varvtal eller andra egenskaper så att farkostens höjd ökar eller minskar kraftigt. Det är fullt möjligt att motorn går sönder vid längre angrepp. Rootkitet gör att modulen meddelar styrmodulen att allt är normalt.
- Falsksändning styrning – en intern modul skickar order till motorstyrning som verkar komma från styrdatorn. Motorns varv eller effekt varieras kraftigt. Styrmodulen får utdata om motorns verkliga tillstånd, liksom operatören. Farkosten flyger oregelbundet då styrdatorn kämpar med den falsksändande modulen om kontrollen.

B.2.3 Navigationsmodul

- Programvaruuppdatering med rootkit gör att navigationsmodulen skickar falska data till styrdatorn och lurar den att farkosten är på en annan plats än den verkliga. Sensorerna på farkosten aktiveras på fel plats. Om operatören har vetskap om farkostens verkliga läge genom till exempel radar eller flygledningsstöd är hon medveten om problemet. Farkosten beter sig som om den lurats av falsksända GPS-koordinater.
- DoS från en intern modul gör att navigationsdatorn inte får några förfrågningar om positioner och farkosten fortsätter i samma kurs och höjd så länge angreppet pågår. Styrdatorn vet inte när den är på rätt plats och aktiverar inte sensorerna. Om angreppet pågår tillräckligt länge kommer farkosten att få motorstopp av bränslebrist eller flyga in i terräng.

B.2.4 Roderstyrning

- Programvaruuppdatering med rootkit och nytt styrprogram gör att roderstyrningsmodulen vrider rodren så att farkosten utför manövrar den inte borde. Manövrar som är strukturellt farliga kan utföras. Styrmodulen får meddelanden att allt är normalt. Farkosten flyger oregelbundet och når inte platsen från vilken spaningen ska ske. Sensorerna startas aldrig.
- Falsksändning styrning – en intern modul skickar styrorder som verkar komma från styrdatorn. Roderstyrningsmodulen försöker utföra dem och meddelar korrekt läge till styrdatorn. Farkosten flyger oregelbundet under angreppet då styrdatorn och den anfallande modulen båda försöker skicka order till roderstyrmodulen. Manövrar som skulle orsaka strukturell skada kan ej utföras.
- DoS – ett DoS-angrepp från en intern modul gör att roderstyrmodulen inte kan ta emot data från styrdatorn. Farkosten fortsätter med rodren i samma läge, i ungefär samma höjd och riktning, påverkad av vindförhållanden. Operatören är medveten om läget men inte orsaken.

B.2.5 Kommunikationsmodul

- Programvaruuppdatering med rootkit och nytt styrprogram gör att kommunikationsmodulen sänder falska styrorder till styrdatorn för att få den att utföra ett nytt uppdrag. Operatören märker ett beteende som om farkosten lyder en annan fjärrstyrning. Farkosten flyger en annan rutt och försöker utföra de nya styrorderna till dess att angreppet slutar.
- Falsksändning styrning – en intern modul sänder order som om den vore styrdatorn och beordrar kommunikationsmodulen att stänga av radiosändningen av sensordata. Detta upprepas när styrdatorn skickar order att återuppta sändningen. Farkostens sändningar slås av och återupptas i snabb följd med stora dataförluster som följd. Detta fortsätter så länge angreppet pågår.
- DoS – en intern modul sänder data i hög takt och förhindrar kommunikationsmodulen att ta emot data. Inga sensordata sänds vidare till markstationen. Detta fortsätter så länge angreppet pågår.

B.2.6 Sensormodul

- Programvaruuppdatering med rootkit och nytt styrprogram gör att sensormodulen skickar felaktiga styrorder till sin hårdvara, för att till exempel rikta antenner åt fel håll, eller ställa in felaktigt fokus på

kameror. Farkosten verkar ha fått hårdvarufel på sina sensorer och reläar felaktiga data till markstationen.

- Falsksändning styrning – en annan intern sensormodul sänder felaktiga styrorder som verkar komma från gränssnittsdatorn för att få sensormodulen att stänga av sina sensorer eller rikta dem i fel riktning. Gränssnittsdatorn sänder samtidigt order för att få sensormodulen att utföra det verkliga uppdraget. Farkosten sänder data under korta stunder med intermittenta avbrott. Av de data som kommer till markstationen är en del från sensorer som är felriktade.
- DoS – en intern modul sänder data till sensormodulen så att den inte kan ta emot styrorder från Gränssnittsdatorn. Farkosten aktiverar aldrig sina sensorer så länge angreppet pågår.

B.2.7 Sensorserver

- Programvaruuppdatering med rootkit och nytt styrprogram meddelar styrdatorn att sensormodulerna inte kommunicerar. Alternativt skickar Gränssnittsdatorn styrorder till sensormodulerna som gör att antenner och kameror riktas åt fel håll. Farkosten verkar ha fått ett hårdvarufel.

B.2.8 Operatörsstationer, OCS för användargränssnitt

- Programvaruuppdatering med rootkit och nytt styrprogram tar emot indata från farkosten och presenterar felaktiga data för operatören för att få denne att skicka ut styrorder baserat på det falska läge som presenteras. Alternativt visar programmet en bild för operatören av att uppdraget framskrider som beräknat men skickar ut falska styrorder till farkosten för att förmå den att aktivera sensorerna vid fel tillfälle eller inte alls.
- Falsksändning av data från en enhet på det lokala nätverket. Dessa data ser ut att komma från farkosten och tas emot och presenteras för operatören som om det vore den verkliga situationen. Om detta sker utan att samma angrepp riktas mot databasstationen kan operatören och högre stab få helt olika lägesbilder.
- DoS – en enhet på det lokala nätverket skickar trafik till operatörsstationen så att den inte kan ta emot data från telemetristationen.

B.2.9 Styrning och telemetri

- Programvaruuppdatering med rootkit och nytt styrprogram tar emot indata från farkosten och presenterar felaktiga data för operatören för att

få denne att skicka ut styrorder baserat på det falska läge som presenteras. Alternativt visar programmet en bild för operatören av att uppdraget framskrider som beräknat men skickar ut falska styrorder till farkosten för att förmå den att aktivera sensorerna vid fel tillfälle eller inte alls.

- Falsksändning av data från en enhet på det lokala nätverket. Eftersom dessa data ser ut att komma från operatören behandlas och skickas de vidare till farkosten som försöker utföra den falska ordern.
- DoS – en enhet på det lokala nätverket skickar trafik till telemetridatorn så att den inte kan ta emot data från operatörsstationen. Order kan inte ges till farkosten som autonomt fortsätter sitt uppdrag. Angreppet är meningsfullt endast om operatören velat göra avsteg från uppdraget.

B.3 Röjande signalering från RPAS

Angreppet syftar till att få RPAS att röja sig för målet eller ge underrättelsedata om RPAS sensorkapacitet genom att aktivera den utrustning ombord på farkosten som kan ge röjande strålning av något slag.

B.3.1 Uppdragsbeslutande styrdator

- Programvaruuppdatering med rootkit och nytt styrprogram aktiverar sensorer och belysning på farkosten så att dess aktiviteter röjs. Rootkitet gör att farkostens aktiviteter inte meddelas operatören.
- Falsksändning av data från en intern modul verkar vara navigations- eller andra data som leder till att styrdatorn tror sig vara på en plats där spaning ska ske. Därför aktiverar styrdatorn sensorer och andra enheter som röjer farkostens aktiviteter.

B.3.2 Navigationsmodul

- Programvaruuppdatering med rootkit och styrprogram gör att navigationsmodulen sänder koordinater som leder till att styrdatorn aktiverar sensorer och andra enheter som röjer farkostens aktiviteter.

B.3.3 Kommunikationsmodul

- Programvaruuppdatering med rootkit och nytt styrprogram får modulen att skicka styrorder som verkar komma från operatören. Detta leder till att styrdatorn aktiverar sensorer och andra enheter som röjer farkostens aktiviteter.

B.3.4 Sensormodul

- Programvaruuppdatering med rootkit och nytt styrprogram får modulen att aktivera sändande sensorer som till exempel radar.

B.3.5 Sensorserver

- Programvaruuppdatering med rootkit och nytt styrprogram får modulen att beordra sensormoduler för sändande sensorer som radar att aktivera dessa.
- Falsksändning styrning – en intern modul sänder falska styrorder som verkar komma från styrdatorn. Dessa verkar vara order att aktivera sändande sensorer som till exempel radar. Ifall sensorer aktiveras kommer operatören att se detta och kan slå av dem. Angreppet kan då upprepas.

B.3.6 Operatörsstationer, OCS för användargränssnitt

- Programvaruuppdatering med rootkit och nytt styrprogram får stationen att beordra farkosten att aktivera sändande sensorer som till exempel radar.

B.3.7 Styrning och telemetri

- Programvaruuppdatering med rootkit och nytt styrprogram får enheten att beordra farkosten att aktivera sändande sensorer som radar.
- Falsksändning styrning – en enhet på det lokala nätverket sänder falska styrorder som verkar komma från operatören. Dessa verkar vara order att aktivera sändande sensorer på farkosten som till exempel radar.

B.4 Fysisk förstörelse av RPAS eller annat

Angreppet syftar till att RPAS ska flyga in i terräng, byggnad eller annan farkost för att orsaka skada och/eller dödsfall. En minsta-framgång uppnås om farkosten förstörs men på en i övrigt säker plats, till exempel tomt hav. Full framgång vore styrd flygning in i trafikflygplan i luften eller en katastrof av motsvarande storlek.

B.4.1 Uppdragsbeslutande styrdator

- Programvaruuppdatering med rootkit och nytt styrprogram. Farkosten börjar utföra ett nytt uppdrag men ljuger för operatören om vad den gör.

Det nya programmet styr farkosten på ett sätt som får den att störta, eller flyga in i byggnader eller fordon.

- Falsksändning från intern modul som utger sig för att vara navigationsmodulen. Sändningen uppger att farkosten är på väg åt fel håll. Styrdatorn försöker korrigera. Operatören märker vad som händer. Den nya riktningen och höjden för farkosten in i terräng eller byggnader om operatören inte avbryter. Angreppet kan upprepas om operatören släpper kontrollen.
- Falsksändning från intern modul som låtsas vara kommunikationsmodulen. Denna sänder styrorder som ser ut att vara från markstationen. Styrdatorn följer de nya orderna och meddelar operatören den nya kursen och verkliga koordinater. Koordinaterna leder farkosten att flyga in i terräng eller byggnader om operatören inte ingriper.
- DoS som hindrar kommunikation med styrmodulen. Intern DoS gör att farkostens delar fortsätter att vara aktiva i samma tillstånd som när störningen började. Fortsätter DoS över tid kommer farkosten att störta av bränslebrist eller flyga in i terräng eller byggnader.

B.4.2 Motorstyrning

- Programvaruuppdatering med rootkit och nytt styrprogram. Motorstyrningen börjar utföra nya operationer men ljuger för styrdatorn. Motorn stängs av, eller gaspådrag minskas så att höjd ändras. Farkosten flyger in i terräng.
- Falsksändning av styrdata från en intern modul. Samma effekt som ovan, men styrdatorn får utdata som anger motorns verkliga beteende och kan gå in och försöka rätta till problemet. För den mänskliga operatören verkar felet ligga i motorn.

B.4.3 Navigationsmodul

- Programvaruuppdatering med rootkit och nytt styrprogram gör att modulen lämnar ut felaktiga data till uppdragsmodulen. Farkosten försöker utföra sitt uppdrag men flyger till fel plats och eller höjd. Den mänskliga operatören kan, om hon har extern information till exempel från radar, se farkostens verkliga läge. Om operatören inte ingriper kommer farkosten att flyga in i terräng eller byggnad. Effekten på farkosten är liknande den som uppstår vid extern falsksändning av till exempel GPS.

B.4.4 Roderstyrning

- Programvaruuppdatering med rootkit och nytt styrprogram gör att rodren inte ligger an i de vinklar som de ska och farkosten börjar flyga ett nytt uppdrag på död räkning – det vill säga att vid en viss tidpunkt svänger den en viss tid med visst roderutslag och så vidare vilket ger intrycket av att den fjärrstyrs. Farkosten flyger in i terräng eller bebyggda områden. Precision vid död räkning medger inte träff mot enskilda byggnader men en större tätort kan träffas.
- Falsksändning mot roderstyrningen från en intern enhet. En annan modul skickar styrorder till modulen som utför dem i tron att det är styrdatorn som skickar orderna. Effekten är densamma som ovan men styrdatorn kan försöka gå in och styra upp situationen. Felet ger intryck av att ligga i roderstyrmodulen. Farkosten flyger in i terräng eller bebyggda områden. Precision vid död räkning medger inte träff mot enskilda byggnader men en större tätort kan träffas.

B.4.5 Kommunikationsmodul

- Programvaruuppdatering med en rootkit och nytt styrprogram gör att modulen falsksänder mot styrdatorn, motorstyrning eller roderstyrning för att åstadkomma flygning in i terräng eller byggnad. Precision vid död räkning medger inte träff mot enskilda byggnader men en större tätort kan träffas.

B.4.6 Operatörsstationer, OCS för användargränssnitt

- Programvaruuppdatering med rootkit och nytt styrprogram tar emot indata från farkosten och presenterar felaktiga data för operatören för att få denne att skicka ut styrorder baserat på det falska läge som presenteras. Alternativt visar programmet en bild för operatören av att uppdraget framskrider som beräknat men skickar ut falska styrorder till farkosten för att förmå den att ändra höjd eller riktning. De nya orderna styr farkosten in i byggnader, terräng eller andra farkoster.
- Falsksändning av data, från en enhet på det lokala nätverket men som ser ut att komma från farkosten, tas emot och presenteras för operatören som om det vore den verkliga situationen. Om operatören korrigerar efter det felaktiga läget, till exempel vad som verkar vara en stigande farkost, kommer farkosten att flyga in i terräng.

B.4.7 Styrning och telemetri

- Programvaruuppdatering med rootkit och nytt styrprogram får modulen att sända styrorder till farkosten som får den att utföra manövrar som ändrar dess riktning och höjd samtidigt som modulen sänder data till operatörsstationen som visar att uppdraget fortskrider enligt plan. Det nya uppdraget leder farkosten in i terräng, byggnader eller andra farkoster.
- Falsksändning styrning – en enhet på det lokala nätverket sänder falska styrorder som ser ut att komma från operatörsstationen. Dessa sänds vidare till farkosten som försöker utföra dem. De nya orderna leder farkosten in i byggnader eller terräng.
- Falsksändning data – en enhet på det lokala nätverket sänder falska data som verkar komma från farkosten. Beroende på vad som sänds kommer stationen antingen att skicka korrigeringar till farkostens kurs, höjd och motoreffekt, reläa dem till operatörsstationen och ge operatören en falsk lägesbild, eller både och. Korringeringar av till exempel vad som verkar vara en stigande farkost kommer att leda farkosten in i terräng.

B.4.8 Radiokomdator

- Programvaruuppdatering med rootkit och nytt styrprogram gör att datorn ersätter telemetridatorns styrorder med andra för att få farkosten att ändra höjd och riktning på ett felaktigt sätt. Dessa för farkosten in i terräng eller byggnader.
- Falsksändning styrning – en enhet på det lokala nätverket skickar data som verkar komma från operatören i form av styrorder. Radiokomdatorn sänder dessa. Farkosten följer de nya orderna och sänder tillbaka korrekt information om ny position och kurs. Orderna för farkosten in i terräng eller byggnader.

B.5 Vilseledning högre stab eller operatör

Vilseledning högre stab eller operatör är egentligen två angrepp. Målet är att uppnå vilseledning. Mot högre stab angrips databaserna så att felaktiga data ska sändas ut via MilNet. För att lura den lokala operatören måste trovärdiga data presenteras inte bara under angreppet, utan övergången till angrepp och från angrepp måste vara sådan att operatören inte märker skillnaden mellan förfalskat läge och verkligt läge. Det torde vara betydligt svårare än att lura högre stab.

B.5.1 Uppdragsbeslutande styrdator

- Programvaruuppdatering med rootkit som skickar falska data tillbaka till markstationen. Dessa kan vara falska sensordata som indikerar till exempel närvaro eller frånvaro av farkoster, eller falska navigationsdata som får operatören att tro att inkommande sensordata kommer från en annan plats än de gör.

B.5.2 Kommunikationsmodul

- Programvaruuppdatering med rootkit som skickar falska data tillbaka till markstationen. Dessa kan vara falska sensordata som indikerar närvaro eller frånvaro av farkoster, eller falska navigationsdata som får operatören att tro att inkommande sensordata kommer från en annan plats än de gör.
- Falsksändning data, en intern modul skickar falska sensordata som reläas till markstationen.

B.5.3 Sensormodul

- Programvaruuppdatering med rootkit och nytt styrprogram som får sensormodulen att skicka falska data till sensorgränssnittsdatorn. Dessa data tas emot som korrekta och reläas till operatören.

B.5.4 Sensorserver

- Programvaruuppdatering med rootkit och nytt styrprogram som får modulen att ersätta korrekta data från sensorerna med falska och skicka dessa till styrdatorn. Dessa data tas emot som korrekta och reläas till operatören.

B.5.5 Operatörsstationer, OCS för användargränssnitt

- Programvaruuppdatering med rootkit som visar falska data för operatören. Dessa kan vara falska sensordata som indikerar till exempel närvaro eller frånvaro av farkoster, eller falska navigationsdata som får operatören att tro att inkommande sensordata kommer från en annan plats än de gör.
- Falsksändning data, en enhet på det lokala nätverket skickar falska sensordata till operatörsstationen. Dessa kan vara falska sensordata som indikerar närvaro eller frånvaro av farkoster, eller falska navigationsdata

som får operatören att tro att inkommande sensordata kommer från en annan plats än de gör.

B.5.6 Styrning och telemetri

- Programvaruuppdatering med rootkit som ersätter data med falska som skickas till operatörsstationen. Dessa kan vara falska sensordata som indikerar närvaro eller frånvaro av farkoster, eller falska navigationsdata som får operatören att tro att inkommande sensordata kommer från en annan plats än de gör.
- Falsksändning data – en enhet på det lokala nätverket skickar falska sensordata till Telemetristationen. Dessa kan vara falska sensordata som indikerar närvaro eller frånvaro av farkoster, eller falska navigationsdata som får det att verka som om farkosten är på en annan plats än den är.

B.5.7 Databaser för loggar och andra data

- Programvaruuppdatering med rootkit och ett program som ändrar data i databaserna innan de skickas vidare till högre stab. Detta påverkar inte operatörens lägesbild. Högre stabs lägesbild visar till exempel närvaro eller frånvaro av olika aktiviteter som inte stämmer med verkligheten.
- Falsksändning data – en lokal dator skickar databasuppdateringar med falska data för att ändra databaserna innan de skickas till högre stab. Detta påverkar inte operatörens lägesbild. Högre stabs lägesbild visar till exempel närvaro eller frånvaro av olika aktiviteter som inte stämmer med verkligheten.

B.6 Underrättelseinhämtning

Angreppet syftar till att få ut underrättelsedata från systemet till angriparens dator. Idealt ska detta ske utan störning av RPAS så att upprepning kan ske av angreppet.

B.6.1 Operatörsstationer, OCS för användargränssnitt

- Programvaruuppdatering med rootkit och ett program som lagrar uppdragsdata lokalt på hårddisken för senare hämtning av en insider.
- Programvaruuppdatering med rootkit och ett program som sänder data via MilNet till en dator som kontrolleras av angriparen.

B.6.2 Styrning och telemetri

- Programvaruuppdatering med rootkit och ett program som lagrar uppdragsdata lokalt på hårddisken för senare hämtning av en insider.
- Programvaruuppdatering med rootkit och ett program som sänder data via MilNet till en dator som kontrolleras av angriparen.

B.6.3 Databaser för loggar och andra data

- Programvaruuppdatering med rootkit och ett program som lagrar uppdragsdata lokalt på hårddisken för senare hämtning av en insider.
- Programvaruuppdatering med rootkit och ett program som sänder data via MilNet till en dator som kontrolleras av angriparen.

B.6.4 Teknikerstationer

- Programvaruuppdatering med rootkit och ett program som lagrar uppdragsdata hämtade från farkosten lokalt på hårddisken för senare hämtning av en insider.
- Programvaruuppdatering med rootkit och ett program som sänder uppdragsdata hämtade från farkosten via MilNet till en dator som kontrolleras av angriparen.

Appendix C Angripare

Detta kapitel listar olika typer av angripare som kan tänkas hota ett RPAS. De kopplas ihop med ett angrepp ur angreppskapitlet för att tillverka ett fullständigt spelkort. Det viktigaste att komma ihåg är att välja en angripare som kan åstadkomma det angrepp som valts. Angriparnas kompetens beskrivs dels i generella termer, dels som en hotklass enligt nedan.

C.1 Angriparen förmågor

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

1. Angripare som kan använda verktyg och programvara som andra tillverkat.
2. Angripare som har kompetens att tillverka egna verktyg och vapen som angriper kända svagheter.
3. Angripare som på egen hand kan 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.

Lite förenklat kan det sägas 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).

C.2 Cybersoldaten

Denne är en professionell anställd i ett cyberkrigsförband eller statlig underrättelsetjänst. Har följande egenskaper:

- Professionell
- Arbetar långsiktigt, i team med andra.

- Mycket stora resurser. Cybersoldaten ligger åtminstone på nivå fyra, och några länders representanter ligger på fem och sex.
- Kan förväntas ha tillgång till zero-day exploits i sina vapen. Detta innebär att normala antivirusprogram inte detekterar dem.
- Har understöd av underrättelseorganisationer.
- Har en politisk agenda. Långsiktiga strategiska överväganden styr agerande. Exempel inkluderar men är inte begränsade till
    - Politiska påtryckningar mot ett lands regering eller mot andra politiska aktörer.
    - Försämra karriärmöjligheter för individer så att andra mer vänligt inställda kan klättra i rang i stället.
    - Testa vapen och öva metodik för framtida angrepp mot andra aktörer.
    - Etablera bakdörrar in i system för att ha snabb tillgång till dessa i framtiden.
    - Hämta underrättelsedata ur systemen för långsiktig användning.
- Kan åstadkomma:
    - Programvaruuppdateringar med dolda cybervapen som kommer från leverantör.
    - Programvaruuppdateringar med dolda cybervapen som kommer på konsults laptop eller lagringsmedia.
    - Programvaruuppdateringar med dolda cybervapen som kommer via en anställds telefon, laptop eller annan lagringsmedia som den anställde använt på sitt hemnätverk.
    - Programvaruuppdateringar med dolda cybervapen som kommer med en mask som letat sig in från MilNet till RPAS-nätet.
    - Hot eller mutor mot anställd som får denne att medvetet föra in uppdateringar med dolda cybervapen.
    - Ovanstående cybervapen kan antas vara specialskrivna för RPAS och kunna utföra alla angreppen i angreppskapitlet.

C.3 Cyberbrottslingen

Denne är en yrkeskriminell som agerar för vinning större delen av tiden men som kan motiveras av patriotism eller ideologi delar av tiden. Exempel inkluderar organisationer som Russian Business Network (RBN). Har följande egenskaper:

- Semiprofessionell, har vana av långsiktigt arbete i team med andra och vana att dölja sina spår från polisorganisationer.
- Arbetar långsiktigt i vinstintresse men korsiktigt utifrån ideologi.
- Medelgoda resurser. Kan förväntas ha tillgång till botnät och enstaka zero-day exploits. Skickliga på social engineering, men dåliga eller mycket dåliga gällande lokalkännedom och underrättelseinhämtning. Angrepp begränsas av vad som kan göra snarare än vad angriparen vill göra. 1–4 på hotskalan.
- Har som mål att åstadkomma tillfällig uppmärksamhet för att stödja ett politiskt mål. Eventuellt kompletterande mål är att införskaffa underrättelsedata eller åtkomstmöjligheter för att skänka till cybersoldater. Exempel på mål:
    - Stänga ner kommunikationsvägar.
    - Utföra intrång och ta ut bevis på det för att sprida till media som propaganda.
    - Försöka föra in förstörande kod. Det vill säga vapen som orsakar kortsiktiga raderingar och tvingar organisationen till att installera om systemen.
- Kan åstadkomma:
    - Programvaruuppdateringar med dolda cybervapen som kommer via en anställds telefon, laptop eller annan lagringsmedia som den anställde använt på sitt hemnätverk. Dessa vapen är begränsade till spionprogram som infiltrerar COTS-maskiner och kommunicerar underrättelsedata via lagringsmedia buren av en anställd, eller via internettrafik om maskinen har en sådan anslutning.

C.4 Den omedvetne insidern

En person på något sätt kopplad till RPAS i vid mening. Hon kan vara anställd eller en familjemedlem. Hon blir med någon form av social ingenjörskonst lurad att ladda ner skadlig kod till ett system som tillhör RPAS eller som hon bär med sig in till RPAS. Har följande egenskaper:

- Oprofessionell i sitt säkerhetsagerande. Kan vara oerhört kompetent inom IT-hantering men samtidigt slarvig när det kommer till säkerhet.
- Agerar omedvetet. Omständigheterna kring angreppet styrs av slumpen.

- Kan i vissa fall medvetet sätta säkerhetsmekanismer ur spel eller skapa anslutningar mellan system som inte borde ha kontakt med varandra. Hotnivå 1–2.
- Kan i vissa fall försöka sopa igen spår efter sig för att dölja sitt agerande när angreppet upptäcks.
- Har som mål att använda systemen på ett sätt som underlättar det egna arbetet.
- Kan tänkas åstadkomma:
    - Leverans av skadlig kod och cybervapen som andra tillverkat och som är riktad mot RPAS.
    - Leverans av skadlig kod riktad mot generella system som ställer till skada för RPAS men inte är del av en riktad attack.
    - Avstängning av säkerhetsmekanismer eller sammankoppling av nät som tillåter andra att leverera vapen. Till exempel anslutning av en trådlös åtkomstpunkt i ett skyddat nät för att kunna ladda ner uppdateringar från Internet.

C.5 Hämnaren – den medvetne insidern

Denna kategori tillhör tillsammans med cybersoldaten de farligaste angriparna. Hämnaren är en insider som av någon anledning vill skada sin egen organisation. Anledningen kan vara hämnd för någon upplevd kränkning, monetär eller ideologisk övertygelse eller liknande. Har följande egenskaper:

- Professionalismen hos hämnare ligger över hela spektrumet från amatör till tränad infiltratör. Gemensamt är att hon genom att ha tillgång till systemet och lokaler har en stor fördel.
- Agerar medvetet. Hon försöker systematiskt att maximera skadorna av angreppet genom att utnyttja sitt kunnande, och tillfälligheter. Hotnivå 1–4 beroende på individ.
- Försöker aktivt sätta säkerhetsmekanismer ur spel eller sammankoppla system som inte borde ha med varandra att göra.
- Försöker efter kompetens sopa igen spåren efter sig.
- Kan tänkas åstadkomma:
    - Tillverkning av egna vapen efter kompetens, eller leverans av vapen som andra tillhandahållit.

- Röjande av information runt systemet och kring de anställda för utomstående och därmed underlätta social ingenjörskonst och andra angrepp.
- Avstängning av säkerhetsmekanismer eller sammankoppling av nät som tillåter andra att leverera vapen. Till exempel anslutning av en trådlös åtkomstpunkt i ett skyddat nät för att kunna ladda ner vapen från Internet eller att bära med sig lagringsmedia in på skyddat område och koppla in det i RPAS.

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