Bedömning av sannolikhet och konsekvens för informationssäkerhetsrisker

En studie av vikt

JONAS HALLBERG, JOHAN BENGTSSON, HENRIK KARLZÉN

Bedömning av sannolikhet och konsekvens för hot mot Försvarsmaktens planerade IT-system görs i dagsläget på varierande sätt. Samtliga varianter av bedömningsmetoden har dock gemensamt att absoluta sannolikhets- och konsekvensvärden anges individuellt för varje identifierat hot. Årets studier inom FoT-projektet Bedömning och analys av IT-system (BAIT) har fokuserat på alternativa sätt att genomföra bedömning av sannolikhet och konsekvens för hot mot Försvarsmaktens planerade IT-system. Den första studien utgjordes av en behovsanalys relaterat till bedömningen av sannolikhet och konsekvens för hot. Den andra studien resulterade i ett förslag på bedömningsmetod som utgår från parvisa jämförelser av hot för att bedöma sannolikhet och konsekvens.

Behovsanalysen resulterade i att en uppsättning med 8 övergripande och 12 underliggande behov identifierades. Bland annat identifierades behov av att kunna jämföra sannolikheter och konsekvenser för olika hot samt att ha spårbarhet i de bedömningar som görs.

Den jämförelsebaserade bedömningsmetoden som föreslås utgår från Analytical Hierarchy Process (AHP) och baseras på teorier kring att det är lättare att göra relativa bedömningar än absoluta. En jämförelse av två hot görs genom att både sannolikheten för och konsekvensen av det ena hotet jämfört med det andra bedöms relativt. Innan den föreslagna metoden kan användas behöver dock ett antal parametrar fastställas för att avgöra hur metodens steg mer specifikt ska genomföras. Exempelvis måste det avgöras vilken skala som ska användas när hoten jämförs.

Ett experiment genomfördes för att utvärdera den föreslagna metoden jämfört med den nuvarande bedömningsmetoden inom Försvarsmakten. I experimentet användes den föreslagna metoden med standardiserade parametrar. Experimentet visade dock på att den föreslagna metoden inte hade någon fördel jämfört med Försvarsmaktens nuvarande metod.

Behovsanalysen, den föreslagna metoden och resultaten från experimentet visar att det finns såväl behov av som möjligheter till att utveckla de metoder som används vid bedömning av sannolikheter och konsekvenser inom Försvarsmakten. En ny metod baserad på jämförelser av hot behöver dock ha mer anpassade parametrar än vad som användes i det genomförda experimentet. Det finns utrymme för vidare experiment för att avgöra hur en jämförelsebaserad metod ska utformas.

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

FOI-R--4152--SE
ISSN 1650-1942 December 2015

Jonas Hallberg, Johan Bengtsson, Henrik Karlzén

Bedömning av sannolikhet och konsekvens för informationssäkerhetsrisker

En studie av vikt

Bild/Cover: Johan Bengtsson

Titel	Bedömning av sannolikhet och konsekvens för informationssäkerhetsrisker – En studie av vikt
Title	Assessment of likelihood and consequence for information security risks – A weighted study
Rapportnr/Report no	FOI-R--4152--SE
Månad/Month	December
Utgivningsår/Year	2015
Antal sidor/Pages	43
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E36078
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk. All form av kopiering, översättning eller bearbetning utan medgivande är förbjuden

This work is protected under the Act on Copyright in Literary and Artistic Works (SFS 1960:729). Any form of reproduction, translation or modification without permission is prohibited.

Sammanfattning

Bedömning av sannolikhet och konsekvens för hot mot Försvarsmaktens planerade IT-system görs i dagsläget på varierande sätt. Samtliga varianter av bedömningsmetoden har dock gemensamt att absoluta sannolikhets- och konsekvensvärden anges individuellt för varje identifierat hot. Årets studier inom FoT-projektet Bedömning och analys av IT-system (BAIT) har fokuserat på alternativa sätt att genomföra bedömning av sannolikhet och konsekvens för hot mot Försvarsmaktens planerade IT-system. Den första studien utgjordes av en behovsanalys relaterat till bedömningen av sannolikhet och konsekvens för hot. Den andra studien resulterade i ett förslag på bedömningsmetod som utgår från parvisa jämförelser av hot för att bedöma sannolikhet och konsekvens.

Behovsanalysen resulterade i att en uppsättning med 8 övergripande och 12 underliggande behov identifierades. Bland annat identifierades behov av att kunna jämföra sannolikheter och konsekvenser för olika hot samt att ha spårbarhet i de bedömningar som görs.

Den jämförelsebaserade bedömningsmetoden som föreslås utgår från Analytical Hierarchy Process (AHP) och baseras på teorier kring att det är lättare att göra relativa bedömningar än absoluta. En jämförelse av två hot görs genom att både sannolikheten för och konsekvensen av det ena hotet jämfört med det andra bedöms relativt. Innan den föreslagna metoden kan användas behöver dock ett antal parametrar fastställas för att avgöra hur metodens steg mer specifikt ska genomföras. Exempelvis måste det avgöras vilken skala som ska användas när hoten jämförs.

Ett experiment genomfördes för att utvärdera den föreslagna metoden jämfört med den nuvarande bedömningsmetoden inom Försvarsmakten. I experimentet användes den föreslagna metoden med standardiserade parametrar. Experimentet visade dock på att den föreslagna metoden inte hade någon fördel jämfört med Försvarsmaktens nuvarande metod.

Behovsanalysen, den föreslagna metoden och resultaten från experimentet visar att det finns såväl behov av som möjligheter till att utveckla de metoder som används vid bedömning av sannolikheter och konsekvenser inom Försvarsmakten. En ny metod baserad på jämförelser av hot behöver dock ha mer anpassade parametrar än vad som användes i det genomförda experimentet. Det finns utrymme för vidare experiment för att avgöra hur en jämförelsebaserad metod ska utformas.

Nyckelord: sannolikhet, konsekvens, risk, informationssäkerhet, AHP

Summary

The likelihood and consequence of threats against the IT systems planned for the Swedish Armed Forces has to be assessed early in the life-cycle of these systems. Currently, several different method are used for this purpose. The different approaches have a common characteristic that absolute values for the likelihood and consequence are to be provided for each threat.

This report describes two studies focused on finding an alternative method for assessing likelihood and consequence. The first study included a needs assessment performed to identify needs related to the assessment of likelihood and consequence of threats against planned IT systems. The second study resulted in a method based on the comparisons of threats rather than the assignment of absolute likelihood and consequence values.

An experiment was performed in order to evaluate the proposed method. The evaluation was performed as a comparison with a method based on assigning absolute likelihood and consequence values. In the experiment a basic version of the proposed method was used and the results show no advantages of this configuration of the proposed method as compared to the currently used method.

The needs analysis, the proposed method, and the results of the experiment show that there are needs as well as opportunities to improve the methods for assessment of likelihood and consequence. Consequently, the proposed method should be further developed in order to be able to out-perform the method currently used and further experiments on various aspects of comparison-based methods are needed.

Keywords: likelihood, consequence, risk, information security, AHP

Innehåll

1 Inledning

Det kan upplevas som svårt och krävande att bedöma sannolikhet och konsekvens för hot mot IT-system. En svårighet ligger i att det sällan finns kvantitativa data som grund för bedömningarna. Detta medför att bedömningarna blir kvalitativa och därmed kan påverkas av många faktorer som inte utgör saklig grund. Exempel på sådana faktorer är medierapportering och personliga erfarenheter av informationssäkerhetsincidenter. Fenz m.fl. (2014) pekar ut just prediktionen av riskerna som en utmaning vid hantering av informationssäkerhetsrisker.

I de säkerhetsanalyser som genomförs för Försvarsmaktens IT-system används olika metoder för att bedöma sannolikheter och konsekvenser. Samtliga metoder har dock det gemensamt att absoluta sannolikhets- och konsekvensvärden anges för varje identifierat hot, även om använda skalor kan variera. Syftet med att ange dessa värden är dock gemensamt; de ska ligga till grund för det riskvärde (ofta på en femgradig skala) som utgör en grund för riskprioritering och riskhanteringsbeslut. Det är bra att basera riskvärden på bedömningar av sannolikhet och konsekvens då det inte är givet att direkta bedömningar av riskvärden skulle få med båda dessa parametrar. En studie som genomfördes av Sommestad m.fl. (2015) visar att direkta bedömningar av risk hamnar närmre den associerade konsekvensen än produkten av sannolikhet och konsekvens.

I denna rapport återges de resultat som uppnåtts i de studier som under 2015 har genomförts i FoT-projektet *Bedömning och analys av IT-system (BAIT)*. Syftet med årets studier är att hitta en metod som både upplevs som enklare och ger bättre resultat för bedömning av sannolikhet och konsekvens än de metoder som idag används för Försvarsmaktens IT-system. Det finns två aspekter av resultaten från riskbedömningar som är väsentliga, riskers absoluta och relativa värden. För att bedöma om risker kan accepteras är riskers absoluta värden väsentliga. För att prioritera risker är det deras relativa värden som är väsentliga. Baserat på att det kan vara enklare att jämföra den relativa skillnaden mellan sannolikheter för olika hot respektive mellan konsekvenser av olika oönskade händelser snarare än att sätta absoluta värden på dem direkt (Thurstone, 1927; Yokoyama, 1921), kan det vara fördelaktigt med en metod baserad på parvisa jämförelser av hot.

En metod baserad på parvisa jämförelser av hot för bedömning av sannolikheter och konsekvenser har tagits fram som ett steg mot att uppnå syftet. När denna föreslagna metod ska användas behöver ett antal parametrar fastställas för att avgöra hur metodens steg mer specifikt ska genomföras. Exempelvis måste det avgöras vilken skala som ska användas vid jämförelse av två hot. Anledningen till att inte alla parametrar är fastställda i den föreslagna metoden är dels att det behövs mer empiriskt underlag gällande vilka möjliga lösningar som fungerar bäst, dels att vilken lösning som är mest ändamålsenlig kan vara beroende av

aktuell kontext. En behovsanalys avseende stöd vid bedömning av sannolikheter och konsekvenser genomfördes som en grund för framtagandet av metoden.

Genom ett experiment jämförs en konkretisering av den föreslagna metoden med en metod som utgår ifrån att absoluta sannolikhets- och konsekvensvärden anges direkt för vart och ett av hoten. En direkt angivelse av absoluta sannolikhets- och konsekvensvärden är gemensamt för de metoder som används vid säkerhetsanalyser för Försvarsmaktens IT-system. Denna metod kallas i denna rapport för *nuvarande metod*. Eftersom det vid analys av experimentet inte finns något rätt resultat att utgå ifrån testas hypoteser avseende kognitiv belastning för försökspersonerna och samstämmighet avseende resultaten. Experimentet visar att den konkretisering av den föreslagna metoden som användes i experimentet inte har någon fördel jämfört med nuvarande metod, där absoluta sannolikhets- och konsekvensvärde anges direkt för vart och ett av hoten.

Den föreslagna metoden har också implementerats i demonstratorn Sublime. Detta ger möjligheten att via parvisa jämförelser av hot erhålla förslag på vilka sannolikhets- och konsekvensvärden de identifierade hoten bör erhålla. Sublime har vid experimentet använts för att omvandla de parvisa jämförelser som gjorts av hot till relativa vikter för de olika hoten.

Behovsanalysen, den föreslagna metoden och resultaten från experimentet visar att det finns såväl behov av som möjligheter till att utveckla de metoder som används vid bedömning av sannolikheter och konsekvenser inom Försvarsmakten. En ny metod baserad på jämförelser av hot behöver dock sannolikt vara mer avancerad än den variant som användes i det genomförda experimentet. Det finns utrymme för vidare experiment för att avgöra hur en jämförelsebaserad metod ska utformas. Sublime kan användas som stödverktyg vid genomförandet av sådana experiment.

Återstoden av denna rapport disponeras enligt följande. I Kapitel 2 ges definitioner av centrala begrepp samt beskrivs den genomförda behovsanalysen och den föreslagna metoden. I Kapitel 3 presenteras Sublime och det tillägg som gör det möjligt att använda parvisa jämförelser för att erhålla sannolikhets- och konsekvensvärden. I Kapitel 4 beskrivs upplägg, resultat och analys av det genomförda experimentet. I Kapitel 5 diskuteras slutligen erhållna resultat och framtida arbete.

2 Bedömning av sannolikhet och konsekvens

I detta kapitel beskrivs bakgrund till och därefter en metod för att bedöma sannolikheter och konsekvenser associerade med hot. Först diskuteras definitioner av centrala begrepp. Därefter beskrivs tillvägagångssätt och resultat av den genomförda behovsanalysen. Slutligen beskrivs vilka steg som ska ingå i en metod för att bedöma sannolikheter och konsekvenser genom parvisa jämförelser samt hur dessa steg kan realiseras.

2.1 Definitioner

Användningen av begreppen *hot*, *risk*, *sannolikhet* och *konsekvens*, vilka är centrala i denna rapport, varierar något i såväl litteraturen som tal. Tabell 1 nedan innehåller definitioner av begreppen hot och risk som återfinns i begreppslistor i Försvarsmaktens handböcker H Säk Infosäk (Försvarsmakten, 2013c) och H SÄK Grunder (Försvarsmakten, 2013b), KSF v3.1 (Försvarsmakten, 2014a) och standarden SIS HB 550 (SIS, 2007). Tabell 2 innehåller definitioner av sannolikhet och konsekvens från samma dokument.

Hot definieras samstämmigt i de olika dokumenten utgående från den formulering som återfinns i SIS HB 550, dvs. ett hot är en *möjlig, oönskad händelse med negativa konsekvenser för verksamheten*. Det är också med den betydelsen som begreppet hot används i denna rapport.

Risk används i tal ofta även med betydelser motsvarande konsekvens eller sannolikhet, vilket också påtalas i SIS HB 550. Användningen av begreppet risk med dessa betydelser smyger sig också in i skriftspråket, vilket kan orsaka begreppsförvirring. Även om risk definieras något olika i dokumenten har det i samtliga fall innebörden av en kombination av sannolikhet och konsekvens. H Säk Infosäk och H SÄK Grunder är samstämmiga. I KSF v3.1 och SIS HB 550 har begreppet konsekvens ersatts med begreppen *men* (skada) respektive *uppkommande skadekostnad*, där uppkommande skadekostnad definieras med hjälp av konsekvens. I denna rapport används begreppet risk med betydelsen att en risk är en kombination av sannolikhet och konsekvens kopplat till ett hot.

Sannolikhet definieras endast i H SÄK Grunder, och då med en cirkelreferens. I denna rapport används begreppet sannolikhet med en övergripande betydelse som inkluderar såväl kvalitativa som kvantitativa beskrivningar. Denna användning av begreppet överensstämmer med det engelska begreppet *likelihood* och dess definition enligt ISO Guide 73:2009 (ISO International Organization for Standardization, 2009), *chance of something happening*, med en kommentar om att *likelihood* kan beskrivas i generella termer eller matematiskt.

Konsekvens definieras liksom hot samstämmigt utgående från den formulering som återfinns i SIS HB 550, dvs. en konsekvens är ett *resultat av en händelse med negativ inverkan*. Det är också med den betydelsen som begreppet konsekvens används i denna rapport.

Tabell 1: Definitioner av begreppen hot och risk.

Dokument	Hot	Risk
H Säk Infosäk	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten (SIS HB 550 Utgåva 3). Indelas i aktörsdrivet respektive icke aktörsdrivet hot (H SÄK Grunder).	Risker uttrycks ofta i termer av en kombination av en händelses konsekvenser (inklusive ändrade omständigheter) och därtill relaterad sannolikhet för förekomst (ISO/IEC Guide 73:2009). I en säkerhetsanalys innebär risk en systematisk sammanvägning av förväntad sannolikhet för och konsekvens av att en oönskad händelse inträffar till följd av ett visst hot, kopplat till en definierad verksamhet, en specifik skyddsvärd tillgång och en specifik konsekvensskala. En bedömd risk uttrycks i en av fem risknivåer.
H SÄK Grunder 2013	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten (SIS HB 550 Utgåva 3). Indelas i aktörsdrivet respektive icke aktörsdrivet hot (H SÄK Grunder 2013).	Risker uttrycks ofta i termer av en kombination av en händelses konsekvenser (inklusive ändrade omständigheter) och därtill relaterad sannolikhet för förekomst (ISO Guide 73:2009). I en säkerhetsanalys innebär risk en systematisk sammanvägning av förväntad sannolikhet för och konsekvens av att en oönskad händelse inträffar till följd av ett visst hot, kopplat till en definierad verksamhet, en specifik skyddsvärd tillgång och en specifik konsekvensskala. En bedömd risk uttrycks i en av fem risknivåer.
KSF v3.1	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten. Hoten avser såväl aktörsdrivna som icke aktörsdrivna.	Ett hot som har bedömts avseende sannolikheten för att det inträffar samt vilket men (skada) hotet förorsakar under förutsättning att det har inträffat.
SIS HB 550, Utgåva 3	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten	Kombination av sannolikhet för att ett givet hot realiseras och därmed uppkommande skadekostnad

Tabell 2: Definitioner av begreppen sannolikhet och konsekvens.

Dokument	Sannolikhet	Konsekvens
H Säk Infosäk	-	Resultat av en händelse med negativ inverkan (SIS HB 550 Utgåva 3). I en säkerhetsanalys behandlas främst utfallet av oönskade händelser, dvs. händelser med en eller flera konsekvenser som är negativa för verksamheten. Konsekvensen skall i en säkerhetsanalys ses som en bedömning av värdet eller kostnaden av den skada som uppstår i en skyddsvärd tillgång om en oönskad händelse inträffar till följd av ett visst hot.
H SÄK Grunder 2013	Sannolikheten för att en händelse inträffar. (ISO/IEC Guide 73:2002)	Resultat av en händelse med negativ inverkan (SIS HB 550 Utgåva 3). I en säkerhetsanalys behandlas främst utfallet av oönskade händelser, dvs. händelser med en eller flera konsekvenser som är negativa för verksamheten. Konsekvensen skall i en säkerhetsanalys ses som en bedömning av värdet eller kostnaden av den skada som uppstår i en skyddsvärd tillgång om en oönskad händelse inträffar till följd av ett visst hot.
KSF v3.1	-	Resultat av händelse med negativ inverkan.
SIS HB 550, Utgåva 3	-	Resultat av en händelse med negativ inverkan. Skadekostnad: Sammanlagt värde av ett angrepps konsekvenser.

2.2 Behovsanalys

Det har skett förändringar avseende hur säkerhetsanalyser för planerade IT-system inom Försvarsmakten ska genomföras. En förändring är att det som tidigare benämndes hot-, risk- och sårbarhetsanalyser nu benämns säkerhetsanalys för att följa användningen av begreppet inom andra områden. Denna förändringar följer med att H Säk Infosäk (Försvarsmakten, 2013c) har ersatt H SÄK IT (Försvarsmakten, 2006) och pekar på H SÄK Grunders

(Försvarsmakten, 2013b) beskrivning av metod för säkerhetsanalys. Vidare har KSF 3.1 (Försvarsmakten, 2014b) ersatt KSF 2 (Försvarsmakten, 2004b). Även den övergripande processen för hantering av IT-system ska förändras.

Försvarsmakten hade som målsättning att den 31 december 2014 ändra hanteringen för godkännande av IT-system inom Försvarsmakten (Försvarsmakten, 2013a). DIT 04 (Försvarsmakten, 2004a) skulle upphävas och den nya IT-processen (Försvarsmakten, 2013d) skulle börja gälla fullt ut. De nya IT-system som därefter togs fram inom Försvarsmakten skulle hanteras i enlighet med den nya processen. Samtidigt skulle även metoden för säkerhetsanalys enligt H Säk Grunder börja användas vid analys av planerade IT-system. Något beslut om att upphäva DIT 04 har dock ännu inte tagits, vilket innebär att IT-processen inte nödvändigtvis används fullt ut ännu.

För att skapa en bild av hur den nya arbetsprocessen tillsammans med den nya analysmetoden påverkar Försvarsmaktens arbete med att auktorisera och ackreditera IT-system, genomfördes inom ramen för projektet en intervjuserie med personal inom Försvarsmakten. Fokus för intervjuserien var primärt metodiken som används vid bedömning av sannolikhet och konsekvens för de hot som identifieras mot planerade IT-system. Målsättningen var att identifiera vilka behov som finns inom Försvarsmakten avseende dessa bedömningar. Under intervjuseriens gång framkom det att den nya arbetsprocessen och framförallt den nya analysmetoden inte hade slagit igenom. Då tillvägagångssättet att bedöma just sannolikhet och konsekvens för identifierade hot är likartat mellan de olika metoderna så bedömdes förändringsarbetet avseende metoder och processer inom Försvarsmakten inte ha någon större påverkan på denna behovsanalys.

För att få en så rättvisande bild som möjligt av det nya arbetssättet bedömdes det vara av vikt att intervjua både personer som har rollen som utförare av analyserna och personer som är mottagare av analysresultaten. Utförarna bedömdes kunna ge en god inblick i hur arbetet går till när de olika bedömningarna görs, medan mottagarna kunde ge en inblick i hur de olika analysresultaten nyttjas. På så sätt är det möjligt identifiera vad som krävs av en metod för att den ska vara till stöd för utförarna samtidigt som den ger ett analysresultat som är till nytta för mottagarna.

Det kan tyckas onödigt att genomföra en behovsanalys kring denna typ av metodstöd eftersom många ju redan anser sig veta vad som är problematiskt eller svårt med dagens arbetssätt. Bilden av var problemen ligger är ganska likartad, men det som ofta skiljer sig åt är vilka förändringar som anses behöva genomföras för att komma till rätta med problemen. Att genomföra en behovsanalys med personal på olika positioner i organisationen kan ge en bättre sammantagen bild av alternativa lösningar på ett och samma problem. Därmed kan de behov som motsvarar denna sammanlagda bild identifieras.

Syftet med de studier som beskrivs i denna rapport är att hitta en metod som både upplevs som enklare och ger bättre resultat för bedömning av sannolikhet och konsekvens än nuvarande metod. Därmed är det viktigt att även kunna stämma av huruvida den föreslagna metoden har de egenskaper och ger de resultat som Försvarsmakten förväntar sig att en säkerhetsmålsättning ska innehålla. Utöver att en metod upplevs som enkel att använda och ger rimliga resultat är det även av stor vikt att den ger stöd i att besvara de frågor och ger det resultat som krävs för att en granskare ska kunna avgöra huruvida det planerade IT-systemet eller den tänkta verksamheten kan genomföras med ett rimligt risktagande. Denna behovsanalys är alltså ett nödvändigt underlag för att visa på om alternativa metodstöd ger bättre eller sämre stöd än det metodstöd som används i dagsläget.

2.2.1 Tillvägagångssätt

Arbetet med att identifiera behov kopplade till bedömning av sannolikhet och konsekvens för identifierade hot genomfördes utifrån följande sju steg.

1. Förfrågningar skickas ut till ett antal anställda inom Försvarsmakten där de ombeds medverka i en intervju alternativt föreslå personer som är lämpliga att intervjua.
2. Intervjuer bokas in med de personer som lämnat positivt besked.
3. Intervjuerna genomförs och dokumenteras.
4. Anteckningar från varje intervju sammanställs till löpande text.
5. Den intervjuade ges möjlighet att ändra och kommentera den löpande texten innan den fastställs.
6. Utsagor relaterade till bedömning av sannolikhet och konsekvens identifieras i de löpande texterna från intervjuerna.
7. Behov relaterade till bedömning av sannolikhet och konsekvens identifieras utifrån utsagorna.

2.2.2 Resultat

Studien omfattade fem intervjutillfällen där totalt sju personer från Försvarsmakten deltog. Tre av intervjutillfällena inbegrep personer som representerade utförarperspektivet medan de resterande två intervjutillfällena utfördes med personer som representerade mottagarperspektivet. Intervjuerna genomfördes på en relativt fri form som mer liknade en diskussion än en intervju. För att leda diskussionen i rätt riktning, och förhoppningsvis få svar på de frågor vi hade, användes en intervjuguide med förberedda frågor som kunde ställas vid behov.

Något som framkom ganska snabbt under intervjuerna var att den nya analysmetoden (säkerhetsanalys enligt H Säk Grunder) och den nya IT-processen inte användes i förväntad utsträckning. Den nya IT-processen skiljer sig ganska mycket från det tidigare arbetssättet, vilket har lett till att det inte är helt på plats ännu hur de olika rollerna ska bemannas.

En skillnad i H SÄK Grunder jämfört med många andra metodbeskrivningar är att sannolikhet och konsekvens för ett hot inte bedöms under samma steg i metoden. Även om de riskanalysmetoder som används mestadels skiljer sig åt genom att de olika momenten sker i olika ordning så kan bytet av metod ta tid att arbeta in. Att den nya IT-processen ännu inte är på plats kan även påverka motivationen att börja använda den nya analysmetoden. Säkerhetsmålsättningar tas idag fram på i stort sett samma sätt som under de senaste året, oberoende av om utföraren är Försvarsmaktsanställd eller extern konsult.

Vid genomgång av anteckningarna från de fem intervjuerna identifierades 30 utsagor som relaterade till bedömningen av sannolikhet och konsekvens för hot mot planerade IT-system. Dessa utsagor utgjorde underlaget för att identifiera behov som relaterar till just bedömningen av sannolikhet och konsekvens. Utvinningen av behov gjordes med stöd av så kallade *Voice of the Customer Tables* (VCTs) (N. Hallberg, Pilemalm, & Timpka, 2012; Mazur, 1992) som är ett stöd för att identifiera det bakomliggande behovet eller behoven till en utsaga. Totalt identifierades 58 behov från utsagorna. Då behoven identifierades utifrån utsagor från olika intervjuer fanns en del behov med flertalet gånger samtidigt som vissa behov delvis överlappade med andra behov. Därmed var det nödvändigt att gruppera de olika behoven för att få fram en lista med unika behov. Slutresultatet presenteras i Tabell 3 och omfattar åtta övergripande behov samt tolv underliggande behov.

Det är värt att notera att identifieringen av ett behov inte säger något om huruvida detta behov är uppfyllt i dagsläget. Ett identifierat behov visar, i detta fall, på vad Försvarsmakten behöver för stöd av en analysmetod för att den ska vara till nytta vid bedömning av sannolikhet och konsekvens för de hot som har identifierats. Behoven relaterar alltså till Försvarsmakten och kan genom vidare analys omvandlas till krav på motsvarande metod (N. Hallberg, Andersson, & Westerdahl, 2005).

Tabell 3: Identifierade behov relaterade till bedömning av sannolikhet och konsekvens för hot mot planerade IT-system.

Övergripande behov	Underliggande behov
Behov av att visualisera alla riskbedömningar gemensamt	
Behov av bedömningsgrund för när risker kan accepteras	
Behov av att bedöma i vilken utsträckning föreslagna skydd minskar specifika risker	
Behov av att bedöma risknivå för hot med låg sannolikhet och hög konsekvens	
Behov av analysmetod som är tillämpbar i praktiken	
Behov av att prioritera risker inbördes	Behov av att jämföra riskers bedömda konsekvenser
	Behov av att jämföra riskers bedömda sannolikheter
Behov av att bedöma sannolikhet att hot realiseras	Behov av underlag vid bedömning av sannolikhet
	Behov av uniformt genomförda sannolikhetsbedömningar
	Behov av sannolikhetsskalor med vedertagen innebörd
	Behov av sannolikhetsskala som kan anpassas utifrån analyserad verksamhet
	Behov av spårbarhet för sannolikhetsbedömningar
Behov av att bedöma konsekvens av att hot realiseras	Behov av att händelsekedjor beaktas vid bedömning av konsekvens
	Behov av anpassningsbar konsekvensskala
	Behov av spårbarhet för konsekvensbedömningar
	Behov av minskat personberoende vid bedömning av konsekvens
	Behov av stöd vid bedömning av konsekvens

2.3 Jämförelsebaserad bedömning

Den genomförda behovsanalysen visar på flera behov som pekar på att det är motiverat att utvärdera om en metod som baseras på jämförande av hot är att föredra framför en metod där absoluta värden sätts för ett hot i taget. Exempel på sådana behov är:

Behov av att jämföra riskers bedömda konsekvenser

Behov av att jämföra riskers bedömda sannolikheter

Behov av spårbarhet för sannolikhetsbedömningar

Behov av spårbarhet för konsekvensbedömningar

På en övergripande nivå består en metod för bedömning av sannolikhets- och konsekvensvärden genom jämförelser av följande två steg.

1. Prioritera hot avseende sannolikhet och konsekvens genom att jämföra dem med varandra och beräkna relativa vikter.
2. Beräkna sannolikhets- och konsekvensvärden för alla hot utifrån erhållna relativa vikter.

En första fråga blir därmed vilken metod som ska användas för att prioritera hot avseende sannolikhet respektive konsekvens. En i litteraturen vanligt förekommande metod som använder relativa bedömningar är *Analytic Hierarchy Process* (AHP) (Saaty, 1990). För att prioritera hot kan den del av AHP som används för att prioritera kriterier och alternativa lösningar nyttjas. AHP:s popularitet och diskussionerna som har förts kring de mekanismer som används för prioriteringen har bidragit till att det finns ett antal varianter av metoden (Ishizaka & Labib, 2011).

Steg 1 *Prioritera hot avseende sannolikhet och konsekvens genom att jämföra dem med varandra och beräkna relativa vikter* kan, utgående från AHP, delas in i följande delsteg.

a. Välj två hot som ska jämföras.
b. Jämför de två valda hoten avseende sannolikhet och/eller konsekvens.
c. Om det behövs fler jämförelser genomförs delsteg a och b igen.
d. Beräkna relativa vikter för alla hot.

Steg 2 *Beräkna sannolikhets- och konsekvensvärden för alla hot utifrån erhållna relativa vikter* kan delas in i följande delsteg.

a. Avgör vilka skalor som ska användas för sannolikhet respektive konsekvens.
b. Beräkna sannolikhets- och konsekvensvärden för alla hot.

Utformningen av dessa delsteg ger upphov till ett antal designval vilka diskuteras i Avsnitt 2.3.1 till 2.3.5. Vilket alternativ som är mest lämpat är i flera av fallen en öppen fråga och det finns stort utrymme för empiriska studier för att klargöra för- och nackdelar med de olika alternativen.

2.3.1 Val av hot att jämföra

Steg 1a i den metod som skissas i avsnittet ovan innebär sammantaget att de par med hot som ska jämföras väljs ut. I den ursprungliga versionen av AHP jämförs alla möjliga par med element direkt med varandra och resultaten förs in i en så kallad bedömningsmatris. Om N stycken element ska jämföras med varandra kommer bedömningsmatrisen att innehålla N gånger N stycken värden. I Figur 1 återfinns en bedömningsmatris för tio stycken element (E_1 till E_{10}). Det innebär att det finns tio gånger tio stycken värden som ska fyllas i.

	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9	E_{10}
E_1	?	?	?	?	?	?	?	?	?	?
E_2	?	?	?	?	?	?	?	?	?	?
E_3	?	?	?	?	?	?	?	?	?	?
E_4	?	?	?	?	?	?	?	?	?	?
E_5	?	?	?	?	?	?	?	?	?	?
E_6	?	?	?	?	?	?	?	?	?	?
E_7	?	?	?	?	?	?	?	?	?	?
E_8	?	?	?	?	?	?	?	?	?	?
E_9	?	?	?	?	?	?	?	?	?	?
E_{10}	?	?	?	?	?	?	?	?	?	?

Figur 1: Bedömningsmatris för tio element (E_1 till E_{10}) vars relativa vikter ska beräknas.

Eftersom alla element (E_1 till E_{10}) är likvärdiga när de jämförs med sig själva kommer diagonalen alltid att innehålla ettor. Dessutom är de enskilda elementens relativa vikter är oberoende av i vilken ordning de jämförs, dvs. om element E_3 jämfört med E_8 ger det relativa värdet v så ger E_8 jämfört med E_3 det relativa värdet $1/v$. Dessa egenskaper hos bedömningsmatrisen illustreras i Figur 2, där alla värden i diagonalen är satta till 1 samt att v och $1/v$ har förts in för de värden som gäller förhållandet mellan E_3 och E_8. Det förhållande som därmed finns mellan de värden som återfinns ovanför diagonalen (markerade med mörkgrått i figuren) och de värden som återfinns under diagonalen gör att det är tillräckligt att ange hälften av de värden som återfinns utanför (ovan eller under) diagonalen.

Vid användning av AHP nyttjas detta faktum ofta så att värdena ovanför diagonalen anges, medan värdena under diagonalen beräknas utifrån de ovan diagonalen införda värdena.

	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9	E_{10}
E_1	1	?	?	?	?	?	?	?	?	?
E_2	?	1	?	?	?	?	?	?	?	?
E_3	?	?	1	?	?	?	?	*v*	?	?
E_4	?	?	?	1	?	?	?	?	?	?
E_5	?	?	?	?	1	?	?	?	?	?
E_6	?	?	?	?	?	1	?	?	?	?
E_7	?	?	?	?	?	?	1	?	?	?
E_8	?	?	1/*v*	?	?	?	?	1	?	?
E_9	?	?	?	?	?	?	?	?	1	?
E_{10}	?	?	?	?	?	?	?	?	?	1

Figur 2: Bedömningsmatris där diagonalens värden har satts till ett, den del av matrisen som återfinns ovanför diagonalen har markerats samt *v* och 1/*v* har förts in som de värden som gäller förhållandet mellan E_3 och E_8.

Sammanfattningsvis behöver långt färre än alla N^2 värden som ska återfinnas i en fullständig bedömningsmatris anges; eftersom diagonalen endast innehåller ettor återstår N^2-N värden att ange; på grund av förhållandet mellan värden ovanför och under diagonalen behöver slutligen (N^2-N)/2 värden anges, vilket motsvaras av det mörkgråa området i Figur 2. Även om det är betydligt färre än N^2 värden som i slutändan behöver anges ökar det totala antalet jämförelser snabbt. Exempelvis ger en uppsättning med tio element (som i Figur 1 och Figur 2) 45 par att jämföra, medan en uppsättning med 100 element ger 4950 par att jämföra.

För att relativa vikter ska kunna räknas ut för en uppsättning med hot måste alla möjliga par med hot kunna jämföras med varandra. Det är dock inte nödvändigt att de är explicit jämförda med varandra; det räcker att de kan jämföras via jämförelser med andra hot. Det minsta antalet jämförelser som medger detta är N-1 stycken, där N är antalet hot. Om exempelvis hot H_1 jämförs med alla andra hot H_2 till H_N, resulterar det i N-1 jämförelser och att alla andra hot kan jämföras med varandra via deras jämförelser med H_1.

Med N-1 jämförelser som är valda så att det går att jämföra alla hotpar direkt eller indirekt finns det dock ingen redundans bland jämförelserna, dvs. det finns endast en möjlig väg när två hot ska jämföras. När fler än N-1 jämförelser

genomförs uppstår redundans, dvs. det kan finnas flera möjliga vägar när två hot ska jämföras. Vid viktning enligt förfarandet i AHP beaktas eventuell redundans och de relativa vikter som erhålls baseras på all tillhandahållen information, vilket medger en högre precision hos de relativa vikterna. Dessutom går det att beräkna mått på hur väl de genomförda bedömningarna överensstämmer med varandra, så kallade konsistensensmått.

Då antalet jämförelser ökar snabbt med antalet hot är det rimligt att endast en delmängd av de möjliga jämförelserna genomförs. Då uppstår frågan om vilken delmängd av de möjliga jämförelserna som är lämpligast att genomföra.

En rättfram lösning är att utförare fritt väljer vilka hot som ska jämföras. Vissa par med hot kan vara enklare för utföraren att vikta än andra. Detta avser såväl hur utföraren upplever svårigheten med att genomföra de nödvändiga bedömningarna som precisionen i de gjorda bedömningarna. Detta talar för att det ska vara upp till utföraren att välja vilka jämförelser som ska genomföras.

Det kan dock vara svårt för utföraren att avgöra vilka hot som ska jämföras för att få en uppsättning med jämförelser som leder till önskvärd redundans och rimligt arbetsinsats. Detta talar för att metoden åtminstone vägleder, alternativt styr, utförarens val.

Vid utveckling av en strategi för att välja vilka par med hot som ska bedömas finns flera alternativ.

1. Strategin ger förslag på vilka par med hot som ska bedömas och kan möjligen begränsa utförarens val, men det är utföraren som väljer.
2. Utföraren får välja en av flera alternativa uppsättningar med jämförelser att genomföra.
3. Strategin avgör vilka bedömningar som ska genomföras dynamiskt beroende på resultatet av de bedömningar som har genomförts.
4. Strategin avgör vilka bedömningar som ska genomföras endast beroende på den givna uppsättningen med hot och påverkas inte av resultatet av de bedömningar som genomförs.

En central fråga är när tillräckligt många viktningar har genomförts. Svaret utgör en avvägning mellan redundans och antalet jämförelser. Med fler jämförelser ökar redundansen och den tillgängliga informationen för att beräkna relativa vikter, men också den totala tid det tar att genomföra jämförelserna.

En enkel ansats för stoppvillkor är att alla hot kan relaterats till varandra direkt eller indirekt; då räcker det med N-1 jämförelser för N stycken hot, om de väljs på rätt sätt. I en studie visades att det finns fördelar med att utgå från jämförelser med det som har det minsta värdet (Wedley, Schoner, & Tang, 1993). Tyvärr är det vid jämförelser av sannolikhet och konsekvens för hot inte på förhand känt vilka värden dessa har. (Ishizaka & Lusti, 2004) argumenterar för att diagonalen

ovanför huvuddiagonalen (dvs. de värden som har markerats med frågetecken i Figur 3) ska användas för att inte något hot ska bli överrepresenterat i jämförelserna.

	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9	E_{10}
E_1	1	?								
E_2		1	?							
E_3			1	?						
E_4				1	?					
E_5					1	?				
E_6						1	?			
E_7							1	?		
E_8								1	?	
E_9									1	?
E_{10}										1

Figur 3: Bedömningsmatris där diagonalen ovanför huvuddiagonalen är markerad.

Alternativt kan konsistensmått användas för att avgöra när tillräcklig precision har uppnåtts. Det innebär att antalet jämförelser avgörs dynamiskt baserat på resultatet av genomförda viktningar. För att möjliggöra beräkning av konsistensmått innan alla möjliga jämförelser har genomförts går det att beräkna saknade bedömningar med hjälp av beräknade relativa vikter (Ishizaka & Labib, 2011).

Vilka par med hot som faktiskt jämförs påverkar den maximala skillnaden mellan de olika hoten. Detta kan medföra att de relativa vikterna kan skilja sig åt beroende på vilka par av hot som jämförs. Vilka som väljs påverkar även möjligheten att särskilja hot som är relativt lika. Detta innebär att hot som via indirekta samband hamnar på samma nivå bör jämföras direkt med varandra för att fånga upp eventuella inbördes skillnader. Detta kräver att urvalet görs enligt den dynamiska strategin.

Sammanfattningsvis kan konstateras att det finns flera olika varianter av strategier för att välja ut vilka par med hot som ska jämföras. Det finns också anledning att anta att urvalet kan påverka resultatet (Wedley et al., 1993). En viktig faktor vid val av strategi bör vara dess komplexitet. I vilken omfattning resultaten påverkas och vilka strategier som är fördelaktiga behöver undersökas genom experiment.

2.3.2 Jämförelse av hot

Vid jämförelse av utvalda par med hot ska värden väljas för att beskriva det bedömda förhållandet mellan de aktuella hoten. Dessa värden väljs från en förutbestämd mängd, en så kallad skala, för viktning av hot med avseende på sannolikhet respektive konsekvens. Den i AHP klassiska skalan innehåller de udda heltalen från och med 1 till och med 9 och deras inverser. Mellanliggande jämna heltal och deras inverser kan användas som kompromisser. En etta betyder att det som jämförs anses vara likvärdigt; tal större än ett betyder att det första av de två element som jämförs har ett större värde (sannolikhet, konsekvens, etc.); tal mindre än ett betyder att det senare elementet har ett större värde. Valet av värden motiveras med att elementen som jämförs inte ska vara alltför olika (Forman & Selly, 2001).

Det har föreslagits ett antal andra skalor, utöver den klassiska, för viktningen inom AHP. Ett exempel är geometriska skalor, där värdena utgörs av geometriska talföljder[1]. Vilken skala som ska användas vid viktning av sannolikheter respektive konsekvenser kopplade till olika hot beror på hur stora skillnaderna mellan hoten är, med vilken precision skillnaderna kan bedömas och vilka skalor som används för sannolikhets- respektive konsekvensvärden. Detta medför att frågan om vilken skala som är bäst lämpad att använda är kontextberoende. Vilka värden som ska användas på skalan är alltså en öppen fråga. Ett alternativ är att använda en skala med färre steg, exempelvis *mindre sannolik*, *lika sannolik* och *mer sannolik*. Färre steg på skalan medför att de enskilda bedömningarna blir enklare att genomföra. En möjlig konsekvens är dock att det kan krävas fler bedömningar för att särskilja hot som inte avses prioriteras lika.

Ofta används AHP med fokus på de värdeladdade ord som används för att beskriva de olika värdena i skalan, snarare än själva värdena. Detta medför att det efter att bedömningarna har gjorts sker en transformation från värdeladdade ord till siffervärden. En fördel med att använda värdeladdade ord snarare än siffervärden är att utföraren inte behöver kvantifiera de relativa skillnaderna mellan hoten. En nackdel är att det blir oklart vad de olika stegen på skalan faktiskt betyder. När skalans siffervärden döljs bakom de värdeladdade orden finns dock möjligheten att utvärdera olika utfall baserat på vilka siffervärden som associeras med de värdeladdade orden.

Vid jämförelser av hot finns det alltså behov av att fastställa en skala, med avseende såväl på hur många steg den ska bestå av som vilka värden dessa steg ska associeras med. Vidare behöver det avgöras huruvida jämförelserna ska utgå från siffervärden eller värdeladdade ord. Det finns inga färdiga svar på dessa

[1] I geometriska talföljder är kvoten mellan intilliggande tal konstant. 1, 3, 9, 27, 81 är ett exempel på en geometrisk talföljd.

frågor och det behövs vidare studier för att utröna vilka alternativ som ger bäst resultat. En startpunkt är att använda den klassiska skalan från AHP och att bedömningarna sker baserat på de värdeladdade ord som den skalan innehåller.

2.3.3 Beräkning av relativa vikter för sannolikhet och konsekvens

Baserat på de parvisa jämförelserna beräknas relativa vikter. Dessa relativa vikter anger hur stor andel av totalen som det aktuella elementet står för. För AHP förordar Saaty (1990) användningen av en metod baserad på beräkning av egenvärden och egenvektorer för bedömningsmatrisen. Det finns dock andra förslag som ger enklare beräkningar (Choo & Wedley, 2004).

När inte alla parvisa jämförelser har genomförts kan de i bedömningsmatrisen saknade värdena beräknas från de som har angetts (i den utsträckning den valda mängden jämförelser medger detta). Dessa beräkningar kan bli omfattande beroende på vilka jämförelser som har genomförts (Ishizaka & Labib, 2011). Harker (1987) har presenterat en metod som medger att de relativa vikterna beräknas utan att de saknade värdena räknas fram, vilket innebär att det finns en rättfram metod för att beräkna relativa vikter för viktade hot så snart alla behov kan relateras till varandra via direkta eller indirekta jämförelser. Harkers metod förutsätter dock att beräkningarna av de relativa vikterna genomförs enligt Saatys beräkningsmetod.

2.3.4 Skalor för sannolikhet och konsekvens

Beräkningen av sannolikhets- och konsekvensvärden för de bedömda hoten beror på vilka skalor som används för sannolikhet respektive konsekvens. Det finns flera olika varianter av skalor. De enklaste skalorna är ordinala, dvs. de anger endast en ordning. Andra skalor kan beskrivas med en matematisk funktion, till exempel linjära skalor, där den absoluta skillnaden mellan två steg är konstant, och geometriska skalor, där den relativa skillnaden mellan två steg är konstant. Även om de olika stegen i en skala definieras med siffervärden kan den vara ordinal om den inte går att beskriva med en matematisk funktion. Ett exempel är den skala för sannolikhet som föreslås i H Säk Grunder (Försvarsmakten, 2013b).

Variationen i vilka skalor som används är stor och det är oklart vilken eller vilka skalor som är bäst att använda vid bedömning av sannolikhet respektive konsekvens.

2.3.5 Beräkning av sannolikhets- och konsekvensvärden

Det sista steget i en metod för beräkning av sannolikhets- och konsekvensvärde baserat på parvisa jämförelser av hot är att koppla hotens relativa vikter till sannolikhets- och konsekvensvärden. Det finns flera olika alternativ för hur denna koppling kan ske.

1. Metoden beräknar sannolikhets- och konsekvensvärden utgående från erhållna relativa vikter och en modell av hur resultaten sprider sig över de olika stegen i skalorna.
2. Utföraren bedömer ett eller flera hot på en absolut skala avseende sannolikhet respektive konsekvens och metoden beräknar resterande absoluta värden för de övriga hoten.

En nackdel med alternativ 1 är att det inte är säkert att hoten ska spridas ut över alla nivåer. Om alla hot anses ha liknande sannolikhet kommer detta att leda till felaktiga värden för en del av hoten då de sprids ut över hela skalan.

Det finns flera olika modeller som kan användas för att bestämma hur resultaten ska sprida sig över stegen i skalorna. En rättfram modell är att det hot som har det högsta prioritetsvärdet erhåller det högsta värdet och därefter erhåller resterande hot värden som motsvarar deras relativa vikters andel av de högsta relativa vikterna. Om skalorna för sannolikhets- och konsekvensvärden är beskrivna med en matematisk funktion kan denna användas för att fördela värdena. Ytterligare ett alternativ är att låta utförare välja vilken fördelning hoten ska ha över de olika stegen i skalorna.

2.3.6 Metodens uppfyllnad av behov

I Avsnitt 2.2 identifierades behov inom Försvarsmakten som relaterar till arbetet med att bedöma sannolikhet och konsekvens för hot mot planerade IT-system. Då bedömning av sannolikhet och konsekvens görs som en del i den mer övergripande uppgiften att bedöma risker innehåller behovsanalysen även behov som egentligen har en vidare omfattning. För dessa behov med vidare omfattning är ett metodstöd för bedömningen av sannolikhet och konsekvens enbart en delmängd av vad som behövs för att möta behovet.

Det finns dock fall där den föreslagna metoden för bedömning av sannolikhet och konsekvens kan vara en lösning som tillgodoser behov vilka den nuvarande metoden inte tillgodoser. Att göra parvisa jämförelser av hot innebär att det kommer att blir möjligt att jämföra både konsekvenser och sannolikheter för alla hot med varandra. Att kunna se den relativa konsekvensen och sannolikheten gör det möjligt att lättare prioritera vilka risker som är viktigast att minska genom fler eller bättre skyddsåtgärder.

När de olika hoten jämförs parvis så skapar detta även en spårbarhet till varför analysresultaten blev som de blev. Om det ifrågasätts varför hot A har bedömts ha högre sannolikhet än hot B så är det möjligt att gå tillbaka till viktningen för att se vilka bedömningar som lett fram till detta resultat. Det skulle även vara möjligt att låta utföraren motivera de olika viktningarna, speciellt i fall där något specifikt antagande har gjorts som kan vara bra att notera för spårbarheten. Den föreslagna metoden bedöms vara en lösning som tillgodoser behoven i Tabell 4 på ett sätt som dagens metod inte gör.

Tabell 4: Behov som tillgodoses av den nya metoden.

Behov	Nuvarande	Föreslagen
Behov av att jämföra riskers bedömda konsekvenser	-	✓
Behov av att jämföra riskers bedömda sannolikheter	-	✓
Behov av spårbarhet för sannolikhetsbedömningar	-	✓
Behov av spårbarhet för konsekvensbedömningar	-	✓

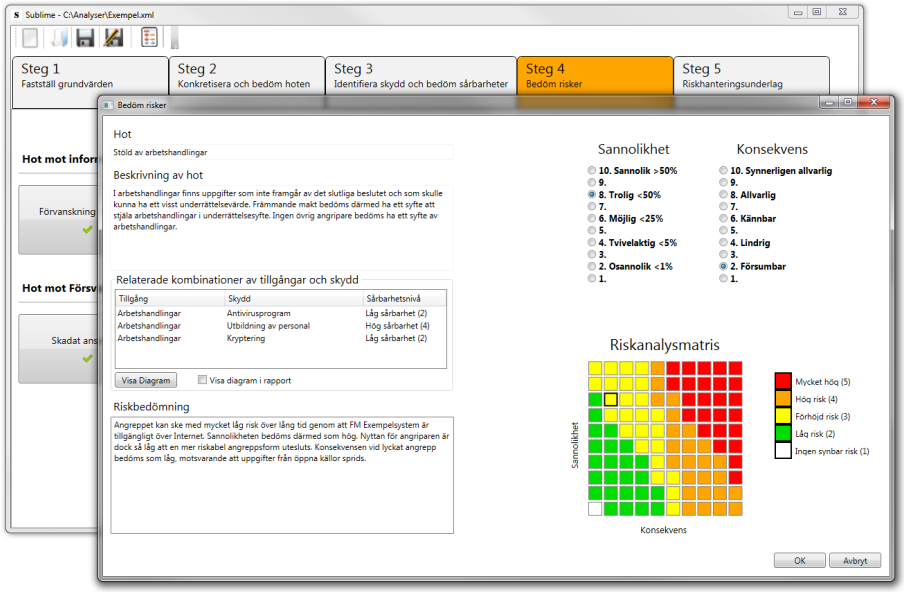
3 Verktygsstöd i Sublime

Som en del i arbetet med att testa den metod som föreslås i Kapitel 2 har den implementerats i Sublime. Att implementera metoden i Sublime ger bra förutsättningar för att genomföra ytterligare experiment i syfte att identifiera hur metoden kan användas på bästa möjliga sätt inom Försvarsmakten för bedömning av sannolikhet och konsekvens för de hot som identifieras.

3.1 Bakgrund

FOI har under ett flertal tidigare projekt arbetat med att utveckla en demonstrator med arbetsnamnet Sublime. Sublime implementerar den metod som beskrivs i Försvarsmaktens gemensamma riskhanteringsmodell (Försvarsmakten, 2009). Syftet med Sublime är att visa hur ett mjukvaruverktyg som stödjer Försvarsmaktens arbete med riskanalyser kan se ut (Figur 4). Målsättningen är att identifiera vad som krävs av ett verktygsstöd för att stödja både utföraren som ska genomföra analysen och de mottagare som ska granska respektive ta beslut utifrån erhållna analysresultat. Att alla parter upplever att verktyget är ett stöd i deras arbete är en viktig framgångsfaktor för att lyckas få hela Försvarsmakten att arbeta på samma sätt med denna typ av analyser.

På en övergripande nivå stödjer Sublime utförare genom att på ett tydligt sätt visa vad som ska göras medan stödet för mottagarna till stor del ligger i att resultaten innehåller för dem nödvändig information och att denna presenteras på ett enhetligt format. Resultaten från analyser genomförda i Sublime presenteras i form av ett rapportunderlag som automatiskt genereras utifrån den information som har matats in i verktyget under analysen. Då rapportunderlaget skapas i form av ett Word-dokument finns möjlighet för komplettering med ytterligare information som behövs för att uppnå en fullgod säkerhetsmålsättning. Målsättningen är dock att så mycket information som möjligt ska matas in direkt i Sublime så att ett nytt rapportunderlag enkelt kan genereras om justeringar har gjorts i den underliggande analysen.



Figur 4: Två fönster som återfinns i Sublime.

Att Sublime är en demonstrator innebär att det inte är ett verktyg som är redo att användas i skarp drift. Sublime kan dock vara ett bra underlag för Försvarsmakten i arbetet med att kravställa ett verktygsstöd av denna typ. Sublime är skapad till fullo utifrån metodbeskrivningen i handboken som beskriver Försvarsmaktens gemensamma riskhanteringsmodell (Försvarsmakten, 2009). Det har inte gjorts några anpassningar för att verktyget ska passa analyser för någon speciell del av Försvarsmaktens verksamhet såsom insatssituationer eller införandet av nya IT-system, vilket medför att Sublime är ett generiskt verktyg för riskanalyser inom olika områden. Anpassning till specifika områden uppnås istället genom återanvändning av exempelvis hot och skyddsåtgärder. Mer information om Sublime går att läsa i (Bengtsson, Hallberg, & Sommestad, 2012; Bengtsson, 2012, 2014a, 2014b, 2014c; J. Hallberg, Bengtsson, & Sommestad, 2013).

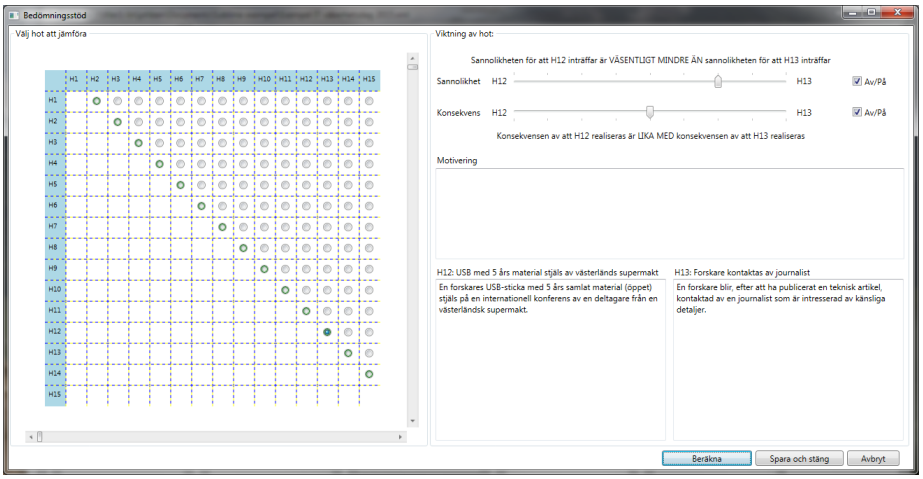
3.2 Relativ viktning

Vid implementationen av ett bedömningsstöd baserat på den föreslagna metoden har fokus legat på att göra ett gränssnitt som är så enkelt och intuitivt som möjligt för utföraren. Fönstret (Figur 5) som utföraren arbetar i är uppdelat i två delar där den vänstra delen av fönstret innehåller en matris som visar de kombinationer av hot som är möjliga att jämföra med varandra. Den högra delen visar detaljer för de två hot som har valts i och med markeringen i matrisen i den

vänstra delen av fönstret. Dessa detaljer omfattar beskrivningar av de två hoten samt ett skjutreglage som används för att göra viktningen avseende sannolikheten att det första hotet realiseras jämfört med det andra och ytterligare ett skjutreglage för att göra samma jämförelse avseende konsekvensen av att det första respektive det andra hotet realiseras. Vilken skala som används för bedömningarna är möjlig att variera, men som standard används den skala som föreslås av Saaty (1990) för användning inom AHP.

Vid designen av fönstret valdes att enbart ha en matris som visar möjliga val av hot att jämföra och sedan ge möjlighet för bedömning av både sannolikhet och konsekvens samtidigt för de valda hoten. Det är dock möjligt att enbart bedöma den ena genom att aktivera eller avaktivera skjutreglagen med den kryssruta som finns till höger om varje skjutreglage.

Fönstret innehåller även en fritextruta som kan användas för att motivera den gjorda viktningen. Motiveringstext kan exempelvis vara lämplig i fall där specifika antaganden om omgivningen har gjorts.



Figur 5: Bedömningsstöd i Sublime för viktning av par med hot.

För att ge utföraren en överblick av vad som är bedömt och vad som är kvar att bedöma markeras de olika alternativen i matrisen med en färg beroende på status. Det finns det fyra olika färgmarkeringar som återges i Tabell 5.

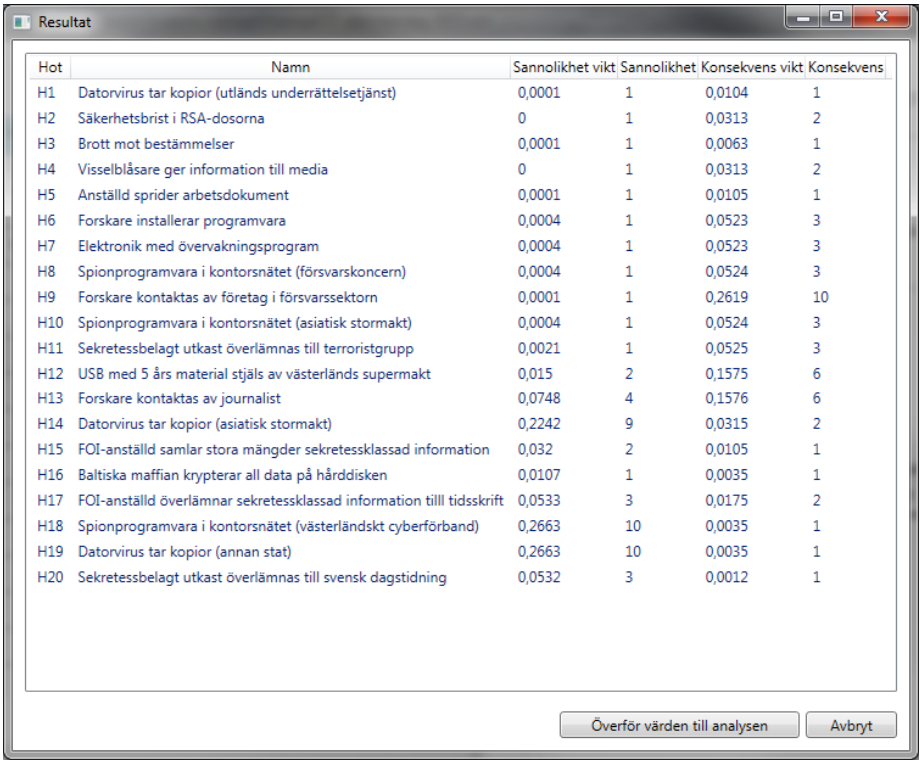
Tabell 5: Färgkodning i bedömningsstödets matris.

Färg	Betydelse
Grön	Viktning av både sannolikhet och konsekvens är genomförd
Gul	Sannolikhet eller konsekvens har viktats
Orange	Förslag på bedömning att göra utifrån aktiverad strategi
Vit	Ingen bedömning har genomförts och alternativet utgör inte ett av de förslag som har markerats med orange färg

För att beräkna de relativa vikterna (en för sannolikhet och en för konsekvens) för varje hot krävs att tillräckligt många jämförelser har gjorts. Det minsta möjliga antalet jämförelser är N-1, d.v.s. en mindre än antalet hot som finns i analysen. Detta uppstår exempelvis om kombinationerna i den övre diagonalen väljs, vilket är de kombinationer som i dagsläget markeras med orange färg i matrisen (i Figur 5 är de gröna eftersom de rekommenderade bedömningarna har genomförts). Det finns många tänkbara strategier för hur valet av jämförelser skulle kunna genomföras, men i dagsläget är endast ovan nämnda strategi implementerad i Sublime. Den motsvarar det som beskrivs som strategi 1 i avsnitt 2.3.1, dvs. *metoden ger förslag på vilka par med hot som ska bedömas och kan möjligen begränsa utförarens val, men det är utföraren som väljer*. Nuvarande implementation i Sublime gör inga begränsningar i utförarens valmöjligheter.

Hur många viktningar som behöver göras innan det går att beräkna de relativa vikterna i Sublime beror på vilka jämförelser utföraren väljer att göra. Det finns ett krav som måste vara uppfyllt för att kunna genomföra beräkningarna och det är att de gjorda bedömningarna skapar ett så kallat *spanning tree*. Om vi gör en parallell till grafteori så är hoten våra noder och jämförelserna blir våra bågar som kopplar ihop noder. När vi har ett *spanning tree* innebär det att det finns minst en väg från varje hot till alla andra hot. Det finns då alltså en kedja av bedömningar som gör att vi kan räkna ut hur två hot förhåller sig till varandra avseende sannolikhet och konsekvens även om de två hoten inte direkt har bedömts. Hur resultatet av en beräkning kan se ut återges i Figur 6. Beräkningarna av vikter följer algoritmen i (Harker, 1987).

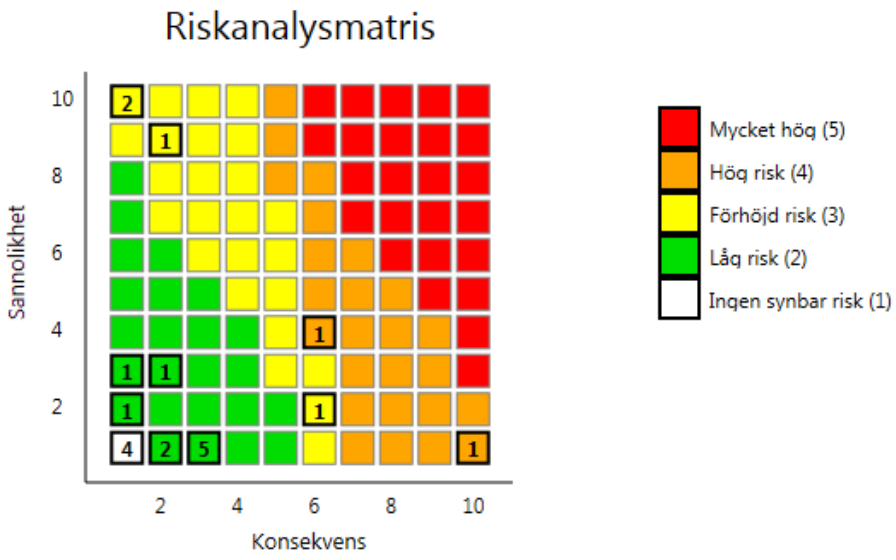
Utgående från de relativa vikterna används den rättframma modell som beskrivs i avsnitt 2.3.5 för att beräkna sannolikhets- och konsekvensvärden. Det innebär att det hot som har den högsta relativa vikten erhåller det högsta möjliga värdet för sannolikhet respektive konsekvens och att resterande hot erhåller värden som motsvarar deras relativa vikters andel av de högsta relativa vikterna. Det finns begränsningar i denna rättframma omräkning och utrymme för att pröva mer avancerade modeller för denna beräkning.



Hot	Namn	Sannolikhet vikt	Sannolikhet	Konsekvens vikt	Konsekvens
H1	Datorvirus tar kopior (utländs underrättelsetjänst)	0,0001	1	0,0104	1
H2	Säkerhetsbrist i RSA-dosorna	0	1	0,0313	2
H3	Brott mot bestämmelser	0,0001	1	0,0063	1
H4	Visselblåsare ger information till media	0	1	0,0313	2
H5	Anställd sprider arbetsdokument	0,0001	1	0,0105	1
H6	Forskare installerar programvara	0,0004	1	0,0523	3
H7	Elektronik med övervakningsprogram	0,0004	1	0,0523	3
H8	Spionprogramvara i kontorsnätet (försvarskoncern)	0,0004	1	0,0524	3
H9	Forskare kontaktas av företag i försvarssektorn	0,0001	1	0,2619	10
H10	Spionprogramvara i kontorsnätet (asiatisk stormakt)	0,0004	1	0,0524	3
H11	Sekretessbelagt utkast överlämnas till terroristgrupp	0,0021	1	0,0525	3
H12	USB med 5 års material stjäls av västerländs supermakt	0,015	2	0,1575	6
H13	Forskare kontaktas av journalist	0,0748	4	0,1576	6
H14	Datorvirus tar kopior (asiatisk stormakt)	0,2242	9	0,0315	2
H15	FOI-anställd samlar stora mängder sekretessklassad information	0,032	2	0,0105	1
H16	Baltiska maffian krypterar all data på hårddisken	0,0107	1	0,0035	1
H17	FOI-anställd överlämnar sekretessklassad information tilll tidsskrift	0,0533	3	0,0175	2
H18	Spionprogramvara i kontorsnätet (västerländskt cyberförband)	0,2663	10	0,0035	1
H19	Datorvirus tar kopior (annan stat)	0,2663	10	0,0035	1
H20	Sekretessbelagt utkast överlämnas till svensk dagstidning	0,0532	3	0,0012	1

Figur 6: Exempel på presentation av resultat efter genomförd beräkning.

De framräknade värdena för sannolikhet och konsekvens kan sedan överföras till analysen. När detta genomförs kommer alla redan genomförda absoluta bedömningar i analysen att ersättas av de värden som räknats fram i och med de parvisa jämförelserna. Efter att bedömningarna har överförts till analysen är tanken att varje riskbedömning gås igenom och motiveras för att på så sätt fastställa den gjorda riskbedömningen. Resultatet av att överföra de framräknade värdena på sannolikhet och konsekvens kan exempelvis se ut som i Figur 7 och Figur 8.



Figur 7: Exempel på spridning av resulterande risknivåer. Siffrorna i riskmatrisens celler anger antalet risker i den aktuella cellen.

Risk	Risknivå
Forskare kontaktas av företag i försvarssektorn	4
Forskare kontaktas av journalist	4
USB med 5 års material stjäls av västerländs supermakt	3
Datorvirus tar kopior (asiatisk stormakt)	3
Spionprogramvara i kontorsnätet (västerländskt cyberförband)	3
Datorvirus tar kopior (annan stat)	3
Säkerhetsbrist i RSA-dosorna	2
Visselblåsare ger information till media	2
Forskare installerar programvara	2
Elektronik med övervakningsprogram	2
Spionprogramvara i kontorsnätet (försvarskoncern)	2
Spionprogramvara i kontorsnätet (asiatisk stormakt)	2
Sekretessbelagt utkast överlämnas till terroristgrupp	2
FOI-anställd samlar stora mängder sekretessklassad information	2
FOI-anställd överlämnar sekretessklassad information tilll tidsskrift	2
Sekretessbelagt utkast överlämnas till svensk dagstidning	2
Datorvirus tar kopior (utländs underrättelsetjänst)	1
Brott mot bestämmelser	1
Anställd sprider arbetsdokument	1
Baltiska maffian krypterar all data på hårddisken	1

Figur 8: Exempel på resulterande risknivåer.

3.3 Framtida utveckling

Sublime kommer att fortsätta användas som en plattform för att genomföra experiment och demonstrera olika metoder och idéer från projektet *Bedömning och analys av IT-system*. Genom vidareutveckling av Sublime är det möjligt att stödja de framtida experiment som planeras under fortsättningen av projektet. Fler tankar kring möjliga framtida experiment återges i Kapitel 5.

Några idéer på förbättringar av Sublime som framkom under årets experiment (se Kapitel 4) följer i punktlistan nedan.

- Den strategi som i dagsläget används för att vägleda utföraren i vilka jämförelser som bör göras är statisk. För att ge ett bättre stöd till utföraren bör strategin uppdateras utifrån de bedömningar som har genomförts. Detta bör fungera på liknande sätt som när en GPS-navigator uppdaterar föreslagen väg på grund av att föraren exempelvis svängt av en avfart tidigare än planerat. Sublime bör även kunna hantera flera olika strategier.
- Att använda olika viktningsskalor är i dagsläget svårt då den valda skalan inte lagras i projektet utan ställs in generellt för hela programmet. Detta resulterar i problem om programmet är inställt på att använda någon annan skala än den skala som användes när hoten i ett projekt

viktades. Sublime bör uppdateras med funktionalitet för att lagra använd skala direkt i projektet. Det bör även bli enklare att hantera valet av viktningsskala direkt när ett nytt projekt skapas.

- Det är inte självklart hur en funktion ska se ut för att gå från framräknade relativa vikter till de absoluta skalor som Försvarsmakten använder. Sublime behöver utökas med alternativa sätt att koppla relativa vikter till de absoluta skalorna samt funktionalitet för att enkelt byta mellan dessa alternativ.

4 Experiment

För att utvärdera vad den i Kapitel 2 föreslagna metoden har för eventuella för- och nackdelar jämfört med den metod som används inom Försvarsmakten genomfördes ett experiment. Försvarsmaktens nuvarande metod innebär att sannolikhet och konsekvens bedöms enskilt med absoluta värden för varje risk. Den föreslagna metoden, som beskrivs i Kapitel 2, utgår istället från att riskernas sannolikhet och konsekvens bedöms genom parvisa jämförelser. Den föreslagna metoden har ett antal parametrar som går att variera. Avsikten med detta första experiment är att utgå från ett så standardiserat val av parametrar som möjligt för att på så sätt få ett basvärde att utgå ifrån i eventuella fortsatta experiment.

Ett första steg i att planera ett experiment är att formulera de hypoteser som experimentet avser pröva. I detta experiment är syftet att undersöka om den föreslagna metoden har några fördelar jämfört med dagens metod avseende tidsåtgång, upplevd arbetsbelastning och samstämmighet mellan försökspersonernas bedömningar. Följande fem hypoteser formulerades för experimentet.

1. Det tar kortare tid att bedöma sannolikhet och konsekvens med hjälp av inbördes viktning.
2. Försökspersonen upplever det som mindre ansträngande att bedöma sannolikhet och konsekvens med hjälp av inbördes viktning.
3. Försökspersonen upplever det som mindre svårt att bedöma sannolikhet och konsekvens med hjälp av inbördes viktning.
4. Bedömningarna av sannolikhet blir mer konsistenta mellan försökspersonerna.
5. Bedömningarna av konsekvens blir mer konsistenta mellan försökspersonerna.

För att kunna genomföra experimentet krävs, förutom formuleringar av de två metoder som ska användas och ett antal försökspersoner, ett antal hot att bedöma sannolikhet och konsekvens för. Under 2014 genomfördes inom ett annat projekt på FOI ett experiment som undersökte hur försökspersonerna tänker kring kopplingen mellan sannolikhet, konsekvens och risk (Sommestad et al., 2015). Det experimentet baserades på två enkäter som försökspersonerna besvarade. I den första enkäten ombads försökspersonerna att bedöma sannolikhet och konsekvens för 105 fiktiva informationssäkerhetsrelaterade incidenter mot deras arbetsplats (FOI). Bedömningarna skulle göras utifrån en metod som till stor del motsvarar den metod som i dagsläget används inom Försvarsmakten. Detta gjorde det tidigare experimentets första enkät till en lämplig utgångspunkt för design av det experiment som beskrivs i detta kapitel. I det tidigare experimentet användes begreppet *incident* istället för hot. Eftersom betydelsen, i detta

sammanhang, är densamma valdes det att även inom ramen för detta experiment använda begreppet incident.

4.1 Upplägg

För att jämföra den föreslagna metoden med den nuvarande metoden används två enkäter som representerar respektive metod. Enkäterna skrivs ut på papper och fylls i med hjälp av bläckpenna. Tanken är att varje försöksperson ska bedöma en och samma uppsättning incidenter, men utifrån de två olika metoder som testas i experimentet. På så sätt kan olika för- och nackdelar med de två metoderna identifieras. Försöket ska genomföras med minst tio personer som väljs genom ett bekvämlighetsurval. Urvalsgruppen består av personer som är fast anställda på FOI som forskare eller chefer.

Båda enkäterna omfattar de 105 incidenter som användes av Sommestad m.fl. (2015). Incidenterna är var och en kortfattat beskrivna med en eller ett par meningar. Omfattningen av beskrivningarna är därför på en nivå som kan tänkas som normal vid analyser av planerade IT-system som alltså sker i ett skede då det ännu inte finns någon design av IT-systemet. Följande två beskrivningar, som representerar två av de 105 incidenterna, är exempel på hur incidentbeskrivningarna kan se ut.

> *Ett datorvirus tar kopior på samtliga dokument kopplade till samarbeten med andra stater som finns i kontorsnätet och delar dessa med en utländsk underrättelsetjänst.*
>
> *En anställd sprider av misstag ofärdiga och icke-kvalitetssäkrade forskningsresultat av undermålig kvalitet till utländska kollegor.*

Båda enkäterna innehåller även de elva inledande frågor som användes av Sommestad m.fl. (2015) och som syftar till att identifiera försökspersonens kognitiva stil samt erfarenhet av att bedöma IT- och informationssäkerhetsrisker. Frågorna relaterade till försökspersonens kognitiva stil avser ge en bild av vad försökspersonen baserar sina beslut på, exempelvis fakta eller magkänsla.

Ett tillägg, som har gjorts på båda enkäter jämför med Sommestad m.fl. (2015), är två avslutande frågor som avser mäta svårigheten att göra bedömningarna samt den mentala ansträngningen som har krävts.

Vid genomförande av experiment är det önskvärt att det sker i en så kontrollerad miljö som möjligt för att minimera faktorer som kan påverka resultaten. De faktorer som försöksledaren försöker kontrollera brukar i experimentsammanhang kallas för *oberoende variabler*. I detta experiment är en av de oberoende variablerna valet av metod. Det är dock inte den enda faktor som bedöms kunna påverka resultaten och därmed behöver kontrolleras. Två

variabler som kan ses som möjliga störvariabler under experimentet är *inlärning* och *kognitiv stil*.

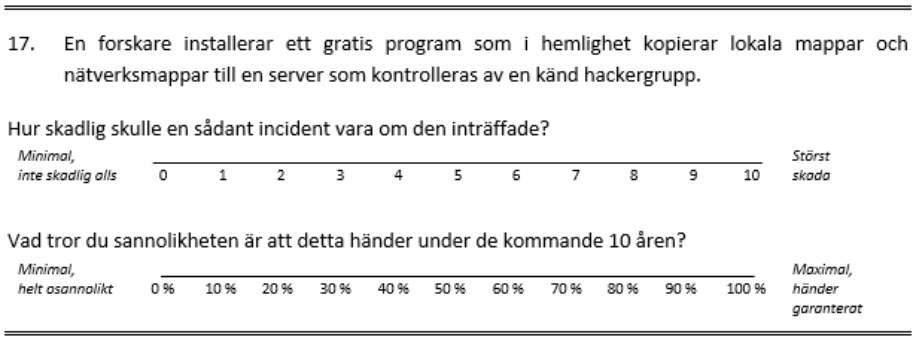
Inlärning innebär att försökspersonen lär sig av att genomföra sin första enkät vilket kan påverka genomförandet av den andra. Det kan alltså spela roll i vilken ordning försökspersonen genomför de två enkäter som beskrivs i 4.1.1 och 4.1.2. För att kontrollera påverkan av inlärning delas försökspersonerna in i två grupper som genomför enkäterna i olika ordning. För att ytterligare minska eventuell påverkan av inlärning krävdes minst en veckas kalendertid mellan varje försökspersons två enkättillfällen.

Försökspersonerna kognitiva stil, det vill säga hur de tar beslut, skulle kunna ha en påverkan på resultatet. Det är exempelvis svårt att påverka huruvida försökspersonerna gör sina bedömningar baserat på fakta eller ren magkänsla. Kännedom om försökspersonens kognitiva stil är värdefull för att i analysen kunna identifiera eventuella samband. För att kunna kontrollera korrelation med kognitiv stil mäts denna med en uppsättning frågor som besvaras av försökspersonen innan det första experimenttillfället.

4.1.1 Enkät 1

Enkät 1 är näst intill identisk med den första enkät som användes i experimentet som beskrivs av Sommestad m.fl. (2015). Det enda som är tillagt är de två avslutande frågorna om svårigheten att göra bedömningarna samt den mentala ansträngningen som har krävts.

Försökspersonen ska bedöma de 105 incidenterna var för sig avseende både sannolikhet och konsekvens. Värdet för sannolikhet avser uppkomst under den kommande tioårsperioden och anges på en linje med ändpunkterna 0% och 100%, där 0% betyder helt osannolik och 100% betyder att incidenten garanterat kommer att inträffa. Värdet för konsekvens anges på en linje med ändpunkterna 0 och 10, där 0 betyder ingen skada alls och 10 är den allvarligaste konsekvensen som någon av incidenterna kan leda till. Trots att det finns markeringar längs linjerna kan deltagarna markera sina svara var som helts längs linjen. Värdena läses av med hjälp av en linjal. Exempel på hur frågorna presenteras i enkäten återges nedan i Figur 9.



Figur 9: Exempel på fråga i enkät 1.

4.1.2 Enkät 2

Parvisa jämförelser av de 105 incidenterna kan genomföras i Sublime (Kapitel 3) av försökspersonerna, men för att inte få ytterligare en variabel som kan påverka utfallet av experimentet ansågs det bättre att genomföra både enkät 1 och enkät 2 med hjälp av papper och penna.

I enkät 2 återanvänds incidenterna och terminologin från enkät 1, men bedömningarna görs parvis enligt den metod som beskrivs i Kapitel 2. För att ta fram en enkät utgående från den metoden behöver det fastställas vilka jämförelser som ska göras samt vilka skalor som ska användas när incidenterna jämförs.

De jämförelser som ska genomföras utgör den så kallade övre diagonalen i jämförelsematrisen (Figur 3). Detta för att alla incidenter ska förekomma i maximalt två jämförelser så att ingen incident bli överrepresenterad. Dessutom minimeras antalet jämförelser som behöver genomföras för att kunna beräkna de relativa vikterna för incidenterna. De par med incidenter som ingår i övre diagonalen jämförs via den klassiska skalan (Tabell 6) från AHP (Saaty, 1990). En justering som har gjorts är dock att de mellanliggande jämna heltalen och deras inverser, som enligt Saaty kan användas för kompromisser, inte används i detta experiment.

Tabell 6: Svensk översättning av den klassiska skalan från AHP.

Värde	Beskrivning
1	Lika
3	Något större
5	Väsentligt större
7	Väldigt mycket större
9	Extremt mycket större

I och med att incidenterna ska jämföras parvis istället för var för sig är det nödvändigt att ändra presentationen av frågorna jämfört med enkät 1. Frågeformuleringarna behöver förändras så att två incidenter beskrivs i varje fråga samtidigt som bedömningarna av den relativa sannolikheten och konsekvensen ska anges på en annan skala. Exempel på hur frågorna presenteras i enkät 2 återges i Figur 10.

ID	Beskrivning
H16	En anställd sprider av misstag ofärdiga och icke-kvalitetssäkrade forskningsresultat av undermålig kvalitet till utländska kollegor.
H17	En forskare installerar ett gratis program som i hemlighet kopierar lokala mappar och nätverksmappar till en server som kontrolleras av en känd hackergrupp.

Vikta incidenterna avseende skada.

H16	9	7	5	3	1	3	5	7	9	**H17**

Vikta incidenterna avseende sannolikhet.

H16	9	7	5	3	1	3	5	7	9	**H17**

Figur 10: Exempel på fråga i enkät 2.

De resultat som erhålls via frågorna i enkät 2 matas in i demonstratorn Sublime (Kapitel 3) för beräkning av relativa vikter för varje incident.

4.2 Genomförande

Försökspersoner till experimentet valdes genom ett bekvämlighetsurval bland heltidsanställda forskare och chefer på FOI Linköping. Att bekvämlighetsurval nyttjades innebär att en grupp av möjliga deltagare valdes ut på förhand. Totalt identifierades 23 personer som, via slump, placerades i en ordnad lista. Personerna kontaktades enligt ordningen i listan. Om en person inte var anträffbar eller avböjde deltagande togs nästa person på listan. När tio personer hade accepterat att delta avbröts rekryteringen.

En fördel med att göra urvalet bland medarbetare på FOI är att de som del av sitt dagliga arbete värderar olika typer av risker. För att bevara deltagarnas anonymitet samlades inga personuppgifter in. De svar som lämnades i enkäterna ska inte kunna knytas till någon av deltagarna. Eftersom det är nödvändigt att kunna knyta samman de två enkäter som har besvarats av samma person används

en kod som deltagarna själva valde vid första tillfället och sedan återgav vid det andra tillfället.

För varje försöksperson genomfördes följande steg.

1. Tillfälle 1
    a. Försöksledaren delar ut frågor avseende kognitiv stil.
    b. Försöksledaren tar emot ifyllda papper avseende kognitiv stil.
    c. Försöksledaren delar ut ena enkäten och noterar klockslag.
    d. Försöksledaren tar emot den ifyllda enkäten och noterar klockslag.
2. Tillfälle 2
    a. Försöksledaren delar ut den andra enkäten och noterar klockslag.
    b. Försöksledaren tar emot den ifyllda enkäten och noterar klockslag.

När alla försökspersoner har fyllt i två enkäter var genomförs en statistisk analys av underlaget. Analysen görs med hjälp av en programvara som heter *Statistical Package for the Social Science* (SPSS).

4.3 Resultat

Resultaten från experimentet redovisas i förhållande till var och en av de fem hypoteserna. Därefter diskuteras de andra variabler som har mätts för att se huruvida de kan ha påverkat resultaten. Två av hypoteserna relaterar till samstämmigheten hos de olika försökspersonernas bedömningar. Beräkningarna av samstämmighet utgår från de absoluta värden som angavs i enkät 1 (Avsnitt 4.1.1) samt de relativa vikter som beräknas utifrån de relativa värden som angavs i enkät 2 (Avsnitt 4.1.2).

Sammanfattningsvis kunde ingen av de fem hypoteserna bekräftas och den konkretisering av den föreslagna metoden som användes i experimentet har inte någon påvisad fördel jämfört med nuvarande metod (där absoluta sannolikhets- och konsekvensvärde anges direkt för varje hot). De kontrollerade variablerna hade inte någon statistiskt signifikant påverkan på bedömda sannolikheter och konsekvenser.

4.3.1 Test av hypoteser

Det tar kortare tid att bedöma sannolikhet och konsekvens med hjälp av inbördes viktning.

Försökspersonerna behövde inte lika lång tid för att besvara enkät 1 som enkät 2. Skillnaden är statistiskt signifikant med en genomsnittlig skillnad på knappt 16 minuter. Därmed faller den första hypotesen.

Försökspersonen upplever det som mindre ansträngande att bedöma sannolikhet och konsekvens med hjälp av inbördes viktning.
Det finns också en statistiskt signifikant skillnad avseende försökspersonernas upplevda ansträngning, som var större för enkät 2. Därmed faller den andra hypotesen.

Försökspersonen upplever det som mindre svårt att bedöma sannolikhet och konsekvens med hjälp av inbördes viktning.
Avseende den upplevda svårigheten är det genomsnittliga värdet något högre för enkät 2, skillnaden är inte statistiskt signifikant. Därmed kan den tredje hypotesen varken bekräftas eller förkastas.

Bedömningarna av sannolikhet blir mer konsistenta mellan försökspersonerna.
Samstämmigheten avseende bedömningar av sannolikheter mäts utgående från de parvisa korrelationerna mellan de svar försökspersonerna angav. Resultaten visar att korrelationerna är starkare mellan svaren i enkät 1 än vad de är mellan svaren i enkät 2. Därmed faller den fjärde hypotesen.

Bedömningarna av konsekvens blir mer konsistenta mellan försökspersonerna.
Samstämmigheten avseende bedömningar av konsekvenser mäts på samma sätt som för sannolikhet. Resultaten visar att korrelationerna är starkare mellan svaren i enkät 1 än vad de är mellan svaren i enkät 2. Därmed faller den femte hypotesen.

4.3.2 Påverkan av störvariabler

För att kontrollera att resultaten inte påverkats av någon annan variabel än valet av metod ställdes även frågor gällande försökspersonernas kognitiva stil och expertis. Dessutom kontrollerades huruvida den ordning i vilken enkäterna genomfördes har en påvisbar påverkan på resultaten.

Frågorna gällande kognitiv stil och expertis hade hög reliabilitet, dvs. de mäter samma sak. Däremot har de ingen statistiskt signifikant påverkan på resultaten avseende sannolikhet och konsekvens. I vilken ordning enkäterna genomfördes hade inte heller någon statistiskt signifikant påverkan på bedömda sannolikheter och konsekvenser.

5 Diskussion

Inom ramen för årets projekt genomfördes två studier. Den första studien utgjordes av en behovsanalys. Resultaten från behovsanalysen visar på att det finns ett antal behov relaterade till bedömning av sannolikhet och konsekvens för identifierade hot. Behov av stöd för genomförandet indikerar att det inte anses vara rättframt att genomföra bedömningarna direkt på egen hand. Vidare finns behov kopplade till uniformitet, minskat personberoende, spårbarhet och att jämföra bedömda sannolikheter respektive konsekvenser. Det ska noteras att existensen av ett behov inte säger något om huruvida detta behov är uppfyllt eller inte. Sammantaget utgör ändå dessa behov ett motiv till att formulera och pröva alternativa metoder för bedömning av sannolikhet och konsekvens.

Årets andra studie resulterade i ett förslag till metod som utgår ifrån ett jämförelsebaserat bedömningsförfarande. I ett första experiment jämförs den föreslagna metoden med en metod som motsvarar den som i dagsläget används inom Försvarsmakten. Som grund för experimentet formulerades fem hypoteser. Experimentet resulterade dock i att fyra hypoteser föll och en hypotes varken kunde bekräftas eller förkastas, vilket inte var i linje med förväntningarna när experimentet planerades. Baserat på resultaten kan det ifrågasättas om det är värt att fortsätta forska på denna typ av jämförelsebaserade bedömningar för bedömning av hot mot Försvarsmaktens planerade IT-system. I syfte att utröna alla möjligheter gjordes även en alternativ analys. Som ett alternativ till att testa hypoteserna baserat på erhållna absoluta värden från enkät 1 och beräknade relativa vikter från enkät 2 användes de värden som angavs direkt i enkät 2. Detta innebär att istället för att utgå från den resulterande relativa vikten för varje hot så jämfördes svarsalternativen som försökspersonerna angav i enkät 2 för att se om detta kunde ge andra indikationer för hypotes 4 och 5 som avser samstämmigheten mellan försökspersonerna i bedömningarna.

Detta alternativa sätt att analysera underlaget ger följande resultat avseende hypotes 4 och 5.

- Sannolikhetsbedömningarna är mer samstämmiga när den föreslagna metoden används än när nuvarande metod används. Dock är skillnaderna små, men det skulle innebära att hypotes 4 bekräftas.
- Konsekvensbedömningarna är fortfarande mer samstämmiga med nuvarande metod, men skillnaderna jämfört med den föreslagna metoden är små.

Sammantaget visar detta analyssätt på att samstämmigheten (hypotes 4 och 5) mellan försökspersonerna är ungefär lika för den nuvarande metoden och den nya metoden. Bristen på redundans i bedömningarna är en möjlig anledning till att resultaten för samstämmighet blir olika beroende på om analysen utgår från de beräknade relativa vikterna eller de svarsalternativ som försökspersonerna har

angett. I experimentet gjordes minsta möjliga antal jämförelser, vilket leder till att en ändring i en bedömning direkt kan påverka alla relativa vikter. Med redundanta bedömningar (dvs. fler än enbart den övre diagonalen) skulle dessa skillnader minska alternativt ge utslag i ett dåligt konsistensmått.

Självklart är det samstämmighet mellan försökspersonerna utgående från de resulterande relativa vikterna som är önskvärt, men denna alternativa analys tyder på att ett annat val av parametrar (viktningsskala och val av hot att jämföra) skulle kunna ge upphov till ett annat resultat. Denna typ av relativa jämförelser används primärt inom andra områden än prioritering av hot, vilket gör det nödvändigt att testa sig fram till vilken uppsättning som ger rimliga resultat. Ytterligare experiment är alltså nödvändiga innan detta bedömningsförfarande kan förkastas avseende bedömning av sannolikhet och konsekvens för hot.

Kommande arbete inom projektet föreslås inriktas på fortsatta studier av jämförelsebaserade bedömningsmetoder och som ett stöd för dessa studier bör de förändringar av Sublime som föreslås i Avsnitt 3.3 genomföras. Detta för att på ett enklare sätt kunna genomföra ytterligare experiment med avseende på följande tre parametrar i den föreslagna metoden.

- Utvärdering av olika skalor för jämförelse av hot
- Strategier för val av vilka hot som ska jämföras
- Beräkning av absoluta sannolikhets- och konsekvensvärden utifrån de relativa vikterna

6 Referenser

Bengtsson, J. (2012). *Användarhandledning för Sublime (FOI Memo 4320)*.

Bengtsson, J. (2014a). *Visualisering av risker i Sublime (FOI Memo 5218)*.

Bengtsson, J. (2014b). *Workshop om säkerhetsanalysverktyg (FOI Memo 4485)*.

Bengtsson, J. (2014c). *Workshop: Nytt säkerhetsanalysverktyg (FOI Memo 4484)*.

Bengtsson, J., Hallberg, J., & Sommestad, T. (2012). *Verktygsstöd för hot-, risk- och sårbarhetsanalyser - realiseringsförslag. FOI-rapport FOI-R--3552--SE*. Linköping, Sverige.

Choo, E. U., & Wedley, W. C. (2004). A common framework for deriving preference values from pairwise comparison matrices. *Computers & Operations Research*, *31*(6), 893–908.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, *22*, 410–430.

Forman, E. H., & Selly, M. A. (2001). *Decision by Objectives: How to Convince Others that You are Right*. World Scientific Publishing Company.

Försvarsmakten. (2004a). *Direktiv för Försvarsmaktens informationsteknikverksamhet (DIT 04)*.

Försvarsmakten. (2004b). *Krav på säkerhetsfunktioner - Grunder (ver. 2.0, HKV 10 750: 78976)*.

Försvarsmakten. (2006). *Handbok för Försvarsmaktens Säkerhetstjänst, Informationsteknik (H SÄK IT)*. Försvarsmakten.

Försvarsmakten. (2009). Försvarsmaktens gemensamma riskhanteringsmodell, Handbok (M7739-350012).

Försvarsmakten. (2013a). Fastställande av processhandbok IT-processen (FM2013-4411:1).

Försvarsmakten. (2013b). *Handbok Säkerhetstjänst Grunder (H Säk Grunder, M7745-734011)*. Försvarsmakten.

Försvarsmakten. (2013c). *Handbok Säkerhetstjänst Informationssäkerhet (H Säk Infosäk, M7739-352056)* (Ändring 1). Försvarsmakten.

Försvarsmakten. (2013d). *Processhandbok IT-processen, Handbok*.

Försvarsmakten. (2014a). *KSF, Krav på IT-säkerhetsförmågor hos IT-system, v3.1, Ordlista och definitioner av begrepp*. Försvarsmakten.

Försvarsmakten. (2014b). *KSF: Krav på IT-säkerhetsförmågor hos IT-system, v3.1*.

Försvarsmakten.

Hallberg, J., Bengtsson, J., & Sommestad, T. (2013). *Effektivare hot-, risk- och sårbarhetsanalyser: Vad blev det för resultat? (FOI-R--3785--SE)*.

Hallberg, N., Andersson, R., & Westerdahl, L. (2005). Quality-driven process for requirements elicitation: the case of architecture driving requirements (FOI-R--1576--SE), 12.

Harker, P. T. (1987). Alternative modes of questioning in the analytic hierarchy process. *Mathematical Modelling*, *9*(3-5), 353–360.

Ishizaka, A., & Labib, A. (2011). Review of the main developments in the analytic hierarchy process. *Expert Systems with Applications*, *38*(11), 14336–14345.

Ishizaka, A., & Lusti, M. (2004). An expert module to improve the consistency of AHP matrices. *International Transactions in Operational Research*, *11*(November), 97–105.

ISO International Organization for Standardization. (2009). *Guide 73 Risk management — Vocabulary*. *ISO Guide 73:2009*.

Saaty, T. L. (1990). How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, *48*(1), 9–26.

SIS. (2007). *SIS HB 550: Terminologi för informationssäkerhet, utgåva 3*.

Sommestad, T., Karlzén, H., Nilsson, P., & Hallberg, J. (2015). Perceived information security risk as a function of probability and severity. In *Human Aspects of Information Security, Privacy, and Trust*.

Thurstone. (1927). A law of comparative judgment. *Psychlogical Review*, *34*, 273–286.

Wedley, W. C., Schoner, B., & Tang, T. S. (1993). Starting rules for incomplete comparisons in the analytic hierarchy process. *Mathematical and Computer Modelling*, *17*(4-5), 93–100.

Yokoyama, M. (1921). The Nature of the Affective Judgment in the Method of Paired Comparisons. *The American Journal of Psychology*, *32*(3), 357–369.