Övning, träning och prövning inom logganalys

Översikt över olika alternativ

PATRIK LIF, MIRKO THORSTENSSON, TEODOR SOMMESTAD

FOI-R--4149--SE
ISSN 1650-1942 December 2015

Patrik Lif, Mirko Thorstensson,
Teodor Sommestad

Övning, träning och prövning inom logganalys

Översikt över olika alternativ

Titel	Övning, träning och prövning inom logganalys
Title	Exercise, training and test within log analysis
Rapportnr/Report no	FOI-R--4149--SE
Månad/Month	December
Utgivningsår/Year	2015
Antal sidor/Pages	59
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	1. Beslutsstödssystem och informationsfusion
FoT-område	Ledning och MSI
Projektnr/Project no	E36083
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Syftet med denna rapport är att beskriva hur träning för logganalytiker bör genomföras effektivt genom framtagande av övningsscenarier och beskriva designen av sådana träningsupplägg. Detta kräver kunskap och förståelse av logganalytikers arbete, mänskliga förmågor och hur träning bör genomföras. Logganalytikerns arbete inkluderar att samla in information och genomföra automatisk och manuell analys. Uppgifter som genomförs är bland annat att konfigurera sensorer för datainsamling, övervakning för att identifiera avvikelser, analysera utvalda händelser och vidta lämplig åtgärd när hot identifieras. Utifrån dessa arbetsuppgifter identifieras viktiga faktorer inom forskningsområdet *Human factors* för att tydliggöra mänskliga förmågor, begränsningar och metoder för att mäta prestation. Utifrån en modell om situationsmedvetande beskrivs bland annat hur logganalytiker påverkas av omgivning, uppgift och miljö, individuella faktorer (t.ex. minne och uppmärksamhet). Dessutom beskrivs individens agerande med utgångspunkt från teorier om situationsmedvetande (perception, förståelse och prediktion), beslutsfattande och agerande. Vidare beskrivs hur övning, träning och prövning bör bedrivas, där återkoppling till deltagarna är en viktig framgångsfaktor för positiv inlärning. Avslutningsvis presenteras sju exempel på träningsdesign för logganalytiker.

Nyckelord: Logganalytiker, human factors, situationsmedvetande, träning.

Summary

The purpose of this report is to describe how training for log analysts should be effectively conducted through development of exercise scenarios and design of training. This requires knowledge and understanding of the log analyst's work, human abilities, and how training should be conducted. The analysts work includes gathering information and carrying out automatic and manual analysis. In these three stages they typically perform four tasks: configure sensors for data collection, monitor the system to identify anomalies, analyze selected events, and take appropriate action when threats are identified. Based on these tasks key areas of human factors research were identified to clarify human abilities, limitations and methods for measuring performance. From the model of situational awareness we described how log analysts were affected by the environment, task, and individual factors such as memory and attention. We also described the individual's behavior with situational awareness (perception, understanding and prediction), decision making and action. Then training and testing were explained, with feedback to participants as a key factor for positive learning. Finally, seven examples of training design for the log analyst were proposed.

Keywords: Log analyst, human factors, situation awareness, and training.

Innehållsförteckning

1 Inledning 9

1.1 Cyberförsvarsförmåga och logganalysförmåga 9

1.2 Övning, träning och prövning inom cybersäkerhet 10

1.3 Rapporten syfte och disposition 12

2 Logganalysuppgifter 13

2.1 Konfiguration av logginsamling och analys 14

2.2 Övervakning av tillstånd, händelser och larm 15

2.3 Analys av händelsers orsak 15

2.4 Val och utförande av åtgärd 16

3 Mänskliga förmågor och färdigheter inom logganalys 18

3.1 Uppgifter och miljöfaktorer 21

3.1.1 Stressfaktorer 21
3.1.2 Mental arbetsbelastning 22
3.1.3 Systemutformning 23

3.2 Faktorer som påverkar individ och grupp 24

3.2.1 Färdigheter 24
3.2.2 Kognitiva förmågor och begränsningar 28
3.2.3 Mentala modeller och inlärda handlingsmönster 30
3.2.4 Attityd och motivation 31

4 Övning, träning och prövning 32

4.1 Typer av kunskap och färdighet 35

4.2 Hur man lär sig 37

4.3 Planering av övningar 39

4.4 Reflektion och återkoppling 41

5 Förslag på övning, träning och prövning för logganalytiker 45

5.1 Manuell analys av logghändelser 45
5.2 Prioritera loggposter för vidare analys 46
5.3 Identifiera påverkade systembehörigheter och systemresurser 47
5.4 Identifiera utnyttjad sårbarhet och föreslå åtgärd 48
5.5 Skapa en signatur som identifierat ett angrepp 49
5.6 Procedurträning 50
5.7 Beredskapstest 50

6 Diskussion och sammanfattning 52

7 Referenser 53

1 Inledning

Denna rapport har producerats under det första året av det treåriga projektet Övning och Experiment för operativ förmåga inom cybermiljön (ÖvExCy). ÖvExCy finansieras av Försvarsmaktens Forskning och Teknikutveckling (FoT) och ska bland annat svara på vilka övningar och experiment som är passande för att utveckla, pröva och utvärdera förmåga till logganalys inom cyberdomänen.

I rapportens första kapitel ges kort översikt över hur logganalysfråga relaterar till mer allmän cyberförsvarsförmåga, en överblick över träning och en översikt över övning och prövning inom cybersäkerhet. Dessutom förklaras rapportens syfte och disposition.

1.1 Cyberförsvarsförmåga och logganalysförmåga

Cyberförsvar saknar en tydlig och etablerad definition, både i Försvarsmakten och i andra sammanhang. Det finns dock flera allmänna idéer om vad cybersäkerhetsarbete består av. Den mest omfattande sammanställningen är det ramverk som har skapats av Amerikanska National Institute of Standards and Technology (NIST) och kallas Cybersecurity Workforce Framework (NICE, 2015). I det ramverket beskrivs 31 specialområden inom 7 övergripande kategorier av arbete. Inom dessa 31 specialområden listas 456 uppgifter, 65 kompetenser och 399 kunskaper/färdigheter/förmågor. Ramverket anger till exempel specialområdet *System Administration* inom kategorin *Operate and maintain* som innefattar 17 uppgifter och 36 kunskaper/färdigheter/förmågor. Ett exempel på en av dessa 17 uppgifter är *Att genomföra funktionell och förbindelsetestning för att säkerställa fortsatt operabilitet* och ett exempel på en av dessa 36 kunskaper/färdigheter/förmågor är *Kunskap om operativsystem för server och klient* (inom kompetensen *Operativa System*).

Cyberförsvarsförmåga förutsätter att många olika uppgifter löses, förutsätter ett stort antal kompetenser inom organisationen. FoT-projektet *Övning och Experiment för Operativ Förmåga i Cybermiljön* (ÖvExCy) kommer att fokusera på test och utveckling av en del av Försvarsmaktens cyberförsvarsförmåga. Nämligen den logganalysförmåga som upprättas i Försvarsmaktens nya centrala logganalysenhet FM SOC. Skälet till att denna förmåga sattes i fokus var att:

1. Det är en ny förmåga som byggs upp och ökad kunskap om lösningar och olika träningsmetoder inom detta område ligger väl i tiden.

2. FOI har sedan tidigare en övnings- och testanläggning vid namn Cyber Range And Training Environment (CRATE)[1] som är lämplig att använda för tester och träning kopplat till lägesbild i cybermiljön.

I de termer som används i NIST:s National Cybersecurity Workforce Framework så kommer denna centrala logganalysenhet främst att syssla med specialområdet *Computer Network Defense Analysis.* Enligt NIST:s ramverk finns det inom detta specialområde 25 uppgifter att utföra och det behövs hela 61 kunskaper, färdigheter och förmågor.

Det har gjorts en hel del forskning kopplat till de 25 typerna av uppgifter som listas i NIST:s National Cybersecurity Workforce Framework. Stor del av denna forskning har handlat om intrångsdetektion – att identifiera elakartad aktivitet utifrån loggar. Ett stort antal lösningsförslag har presenterats i litteraturen, men det finns lite kunskap om hur bra dessa lösningar fungerar i praktiken. När tester gjorts av föreslagna lösningar så har det i regel gjorts mot det femton år gamla datasetet Knowledge Discovery Dataset (KDD) Cup (Lippmann, Haines, Fried, Korba, & Das, 2000), som sedan länge varit kritiserat för betydande brister (McHugh, 2000; Tavallaee, Bagheri, Lu, & Ghorbani, 2009). Det finns även forskning inom cybersäkerhet kopplat till det bredare begreppet lägesförståelse. Men det är ont om kunskap om vad som fungerar och vad som är viktigt. Efter en genomgång av publicerad forskning konstaterade Franke och Brynielsson (2014) att det finns lite empirisk forskning och att mer sådan forskning behövs. Samtidigt konstateras att det finns potential att göra sådana forskning, inte minst i samband med att förmågor övas och prövas.

1.2 Övning, träning och prövning inom cybersäkerhet

Övning, träning och prövning av cybersäkerhet, och logganalysförmåga sker redan. Det har det under de senaste åren tagits fram förslag på övningar (t. ex. ENISA, 2015) och tankar om hur övningar borde utformas (t.ex. handböcker från MSB (2012) och NIST (Wilson & Hash, 2003). Det finns också kataloger med kurser som erbjuds professionella logganalytiker, men övning, träning och prövning inom cybersäkerhet är inte något som getts stor uppmärksamhet av forskare och det finns lite validerad kunskap om hur det bäst görs. Det gäller särskilt när det kommer till övning, träning och prövning av professionella inom cybersäkerhet. Det går till exempel inte att hitta någon studie i den vetenskapliga litteraturen som mäter hur kunskap, förmåga eller färdighet har förändrats hos professionella efter det att de genomgått en övning, träning eller prövning.

[1] www.foi.se/crate

I orienterande syfte ges nedan en kort genomgång av hur begreppen utbildning övning, träning och prövning används i denna rapport. Mer utförliga beskrivningar av hur lärande, utbildning, övning, träning och prövning kan tillämpas och användas inom logganalys ges i kapitel 4.

Övning är ett begrepp som ofta används i generella ordalag för att ange en tillämpad verksamhet där en eller flera individer gör något som relaterar till deras profession. Ibland används övning som begrepp när det handlar om försök med ny utrustning eller nya metoder och ibland används begreppet för att verifiera eller validera kompetens hos personal eller att utrustning fungerar som den ska. I denna rapport utgår vi från den definition för utbildning, övning och träning som Försvarsmakten (FM) använder i Handbok Utbildningsmetodik (2013). Det innebär att begreppet övning används i vid bemärkelse till att omfatta allt från lektion inomhus till färdighetsträning utomhus, och begreppet träning sätts som synonymt med övning. Syftet är dock att lära något.

Övning och träning av cybersäkerhet kan ske på olika sätt och ha olika syften. Övningarna kan till exempel vara inriktade på lärande med syftet att utveckla rutinbaserat handlande eller vara inriktade på lärande med fokus på reflektivt handlande. En faktor som bör beaktas vid planering av övningar är att definiera lärandemål som kopplas till lärnivåer och den kunskapsnivå som målgruppen för övningen behöver ha för att kunna möta sina uppgifter. Den kunskapsnivå som behövs är beroende av den typ av handlingar som uppgiftens lösande bygger på. I FM Pedagogiska grunder (2006) görs definitionen av dessa nivåer enligt Tabell 1 nedan.

Tabell 1: Samband mellan handlings-, kunskaps- och lärnivå (Pedagogiska grunder 2006, sid. 152)

Handlingsnivå	**Kunskapsnivå**	**Lärnivå**
Rutinbaserat handlande	Implicit (tyst) kunskap	Reproduktivt lärande
Regelbaserat handlande	Procedurkunskap (”knowing-how”)	Metodstyrt lärande
Kunskapsbaserat handlande	Teoretisk kunskap (”knowing that”)	Problemstyrt lärande
Reflektivt handlande	Metakognitiv kunskap	Utvecklingsinriktat (kreativt) lärande

Uppgifter som kan förekomma inom cybersäkerhetsarbete ställer krav på både enskilda användare och grupper att tillämpa samtliga fyra nivåer av handlande. En komplett katalog av övningar bör därför belysa alla de olika lärnivåerna.

För cybersäkerhetsområdet, som för de flesta andra områden inom FM, är det centralt att ingen enskild individ ensam kan lösa förestående uppgifter. Det är gruppen, arbetslaget, som är det centrala när problem och uppgifter ska lösas. Detta bör has i åtanke när övningar sätts upp inom cybersäkerhet. Arbetsgruppen kan definieras som en samling individer med gemensamt mål eller syfte, vilken dels är beroende av respektive individs kunskaper och färdigheter, men även av gruppens förmåga att samarbeta (Lind & Skärvad, 1997). Detta är ännu en viktig faktor som kommer att beaktas vis sammansättningen av olika övningar och träningstillfällen.

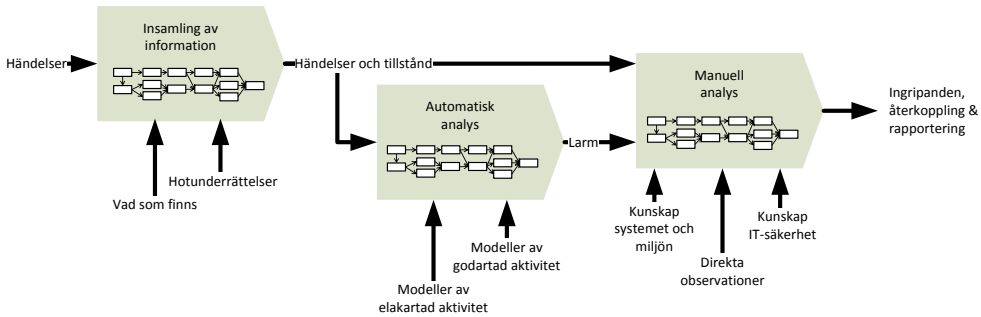
Ett syfte som ofta förekommer vid övningar är att *pröva* nuvarande förmåga hos ett förband eller hos viss personal. En faktor som blir extra viktig i en övning med syftet att pröva förmågan hos förband eller viss personal är den utvärdering som genomförs. Syftet är nämligen att mäta prestationen och inte att ge lärande återkoppling. FM Handbok Utbildningsmetodik (2013) beskriver begreppet utvärdering: ”Med utvärdering av en övning menar vi en sammanvägd värdering av övningens utfall och vägen fram till detta utfall. Med värdering menas de bedömningar och mätningar vilka görs för att vara underlag i utvärderingen”.

1.3 Rapporten syfte och disposition

Syftet med denna rapport är att beskriva hur träning för logganalytiker bör genomföras effektivt genom framtagande av övningsscenarier samt att beskriva hur sådana träningsupplägg bör designas. För att detta ska göras krävs förståelse för incidenthantering och logganalytikers arbete (Kapitel 2), mänskliga förmågor som är relevanta för logganalys (Kapitel 3), samt hur träning och övning bör bedrivas (Kapitel 4). Utifrån dessa tre områden presenteras exempel på träningsdesign för logganalytiker (Kapitel 4).

2 Logganalysuppgifter

Inom ÖvExCy producerades under 2015 en rapport med titeln *Variabler av vikt för förmågan att analysera cybersäkerhetsloggar* (Sommestad & Holm, 2015). I den rapporten ges en översikt över de variabler som tros vara av betydelse för att utföra logganalys på ett bra sätt. På den högst nivån bröts förmågan ner i de tre steg som visas i Figur 1: insamling av information, automatisk analys och manuell analys.



Figur 1. Översikt över logganalysarbete och den input och output som hanteras.

Denna rapport fokuserar på träning och övning av mänskliga logganalytiker. Dessa har en roll att spela i alla de tre steg som visas i Figur 1:

- de bestämmer konfigurationer för insamling av information och automatisk analys
- de utför övervakning i den manuella analysen
- de analyserar händelsers orsak i den manuella analysen
- de väljer och utför åtgärder i den manuella analysen

För att ge en grund till följande avsnitt i denna rapport presenteras nedan en beskrivning av vad logganalytiker gör i dessa steg. Avsnitt 2.1 beskriver konfiguration av logginsamling och analys; avsnitt 2.2 beskriver den manuella övervakningen; avsnitt 2.3 beskriver den manuella orsaksanalysen; och avsnitt 2.4 beskriver hur val av åtgärd görs.

Det finns ingen beskrivning av detta slag som är giltig för samtliga logganalytikers arbete generellt och texten nedan bör endast ses som en skiss på vad deras arbete typiskt omfattar. Det bör också poängteras att det kan finnas flera logganalytiker som samarbetar för att lösa logganalysuppgifterna eller som

har delat upp uppgifterna mellan sig. Det kan även finnas organisatoriska regler som begränsar logganalytikernas arbete, exempelvis att de inte kan utföra åtgärder själva utan att de får föreslå dem till andra inom organisationen.

2.1 Konfiguration av logginsamling och analys

Sensorer kan placeras på olika platser och konfigureras på olika sätt. Hur de placeras och konfigureras påverkar vad de registrerar och därmed vilka analyser som kan göras automatiskt och manuellt. Fördelar och nackdelar finns med olika val. En maskinbaserad sensor behöver till exempel installeras på alla maskiner som ska övervakas medan en nätverksbaserad sensor enbart behöver placeras på knutpunkter för nätverksbaserad kommunikation. Men en maskinbaserad sensor kan registrera både vilken kommunikation som maskinerna är involverade i och vad som händer lokalt på maskinen (t.ex. användande av USB-stickor). Eftersom logginsamling i regel kostar både tid, prestanda och pengar behöver en logganalytiker välja en datainsamlingsstrategi som är lämplig för systemet. För att göra detta optimalt kan det krävas att logganalytikern tar hänsyn till sådant som: hotbild, olika tillgångars exponering, tillgångars värde, behörighetsregler i systemet, användningsmönster och de sårbarheter som systemet har. Förslag på hur formella analyser kan optimera insamlingen med utgångspunkt från tänkbara angrepp finns bland annat i (Noel & Jajodia, 2008). Inom Försvarsmakten begränsas friheten för valen av logginsamling för närvarande av de *Krav på Säkerhetsfunktioner* (Försvarsmakten, 2012) som MUST tagit fram för system. Dessa fastslår en lägsta nivå för logginsamling.

Arkitekturen och tillståndet i det övervakade systemet tillsammans med hotbilden kan användas för att konfigurera logginsamling. Arkitekturbeskrivningar och hotinformation kan också vara av stort värde för att konfigurera den automatiska analysen. Information om vad som är vanligt beteende i systemet kan till exempel användas för att ta bort vissa signaturer för att slippa stora mängder falsklarm. Information om hotbilden kan användas för att prioritera upp andra signaturer och för att skapa egenutvecklade signaturer.

Den manuella analys som logganalytiker gör kan i regel ge information som indikerar sensorernas bästa konfiguration och den bästa lösningen för automatisk analys. Till exempel kan en orsaksanalys fastslå att ett larm är en följd en ofarlig konfiguration i systemet som i framtiden borde ignoreras i den automatiska analysen. Sådan trial-and-error-baserad intrimning har identifierats som en viktig men tidskrävande uppgift för logganalytiker. I Figur 1 motsvarar detta den ”återkoppling” som kommer ur den manuella analysen.

2.2 Övervakning av tillstånd, händelser och larm

Övervakning är ofta en monoton och långtråkig uppgift som syftar till att identifiera avvikelser, oregelbundna mönster och andra tecken på verkliga hot i en omfattande mängd larm. Arbetet innebär att visuellt kontrollera listor på händelser i loggsystem. Det är inte ovanligt att analytiker i större center för cybersäkerhet delar upp arbetsuppgifterna så att vissa tar hand om rena övervakningsuppgifter och andra utför de övriga stegen i manuell analys (Zimmerman, 2014).

Arbetet innebär i huvudsak att värdera, inspektera händelser och larm och att prioritera vilka händelser som utgör potentiella hot och kräver djupare analys. Det vill säga att klassificera händelserna. Inspektionen av händelser kan ske instinktivt enligt inlärda heuristiker eller göras mer genomtänkt. För att bestämma om en eller flera händelser bör analyseras djupare använder logganalytiker information om aktuella hot (t.ex. vanliga angreppssätt) och situationsrelaterad information om egna system (t.ex. kända sårbarheter) (Goodall, Lutters, & Komplodi, 2004).

Logganalytikerns prestation i övervakningsfasen utgörs primärt av förmågan att identifiera faktiska hot (larm som bör utredas vidare) utan att ägna för mycket tid åt felaktiga larm som inte utgör ett hot. Antalet experimentella studier som undersöker logganalytikerns förmåga i denna fas är få. I ett experiment med simulerad data undersökte Sommestad och Hunstad (2013) en logganalytikers förmåga att filtrera ut relevanta larm. Resultaten visar att logganalytikern kan reducera antalet falska larm utan att missa många riktiga attacker genom att bland annat använda kunskap om nätverkstopologin. Intrångsdetektionssystemet larmade om sex av tio angrepp och gav tio falsklarm för varje riktigt larm; logganalytikern larmade för fem av tio angrepp och gav drygt ett falsklarm för varje korrekt larm. I ett annat experiment undersökte Sawyer m.fl. (2014) mental arbetsbelastning när en logganalytiker gavs uppgiften att matcha IP-adresser i tabell med två kolumner. Slutsatserna från studien visade att det var svårare att matcha kolumner när tabellen med IP-adresser arrangerades om kontinuerligt och när attacker förekom sällan. Vilka slutsatser det går att dra från denna studie är något oklart eftersom uppgiften som genomfördes inte överensstämmer med de uppgifter som faktiskt genomförs i övervakningsfasen – logganalytiker sitter sällan och stirrar på tabeller med IP-adresser i väntan på att de ska stå samma sak två gånger i rad.

2.3 Analys av händelsers orsak

Under en orsaksanalys utgår logganalytikern från händelser som prioriterades i övervakningsfasen och som bedömts behöva analyseras ytterligare för att avgöra

om det är nödvändigt att vidta någon form av åtgärd. Till skillnad från övervakningsfasen, som ofta har ett konstant flöde med input i form av händelser, så är starten av en orsaksanalys irreguljär. Dessutom varierar analyserna både till frekvens och tidsomfattning.

Informationen som identifierades som viktig övervakningsfasen (t.ex. larm från en sensor) sammanvägs under orsaksanalysen med annan information för att bättre kunna avgöra varför systemet larmar. Enligt Goodall m.fl. (2004) så använder systemadministratörer generellt kunskap relaterat till intrångsdetektion (t.ex. sensorerna), allmän cybersäkerhetsexpertis och lokal kännedom om de egna systemen när detta görs. Thompson m.fl. (2006) visar även andra typer av systemloggar kan användas för denna typ av arbete (Ramona Su Thompson, Rantanen, & Yurcik, 2006). Det är inte ovanligt att logganalytiker i den manuella analysen använder verktyg för automatisk analys som är fristående från logganalyssystemet. Till exempel kan filer hämtas in från maskiner som är kopplade till händelserna och analyseras.

Logganalytikerns förmåga i denna fas är att identifiera faktiska attacker och förståelse för av hur dessa genomförs under en begränsad tidsrymd. Endast två experiment kopplade till orsaksanalys har identifierats i litteraturen. Ben-Asher and Gonzalez (2015) gav experimentdeltagare uppgiften att bedöma om ett systems status (t.ex. specifika nätverkslaster och aktiva tjänster) utgjorde en säkerhetsrisk i ett förenklat scenario. Deltagarna som hade god kunskap om cybersäkerhet var bättre på upptäckt av skadliga händelser, bättre på att sortera bort av ofarliga händelser och hjälpte logganalytikerna att identifiera vilken typ av hot som skapade den aktuella situationen. Thompson m. fl. (2007) testade hur väl deltagare kunde att identifiera och klassificera angrepp med ett visuellt- respektive ett textbaserat gränssnitt. Aningen förenklat fann de att förbestämda uppgifter utfördes bättre med textbaserat gränssnitt medan mer explorativa uppgifter som att se anomalier i nätverket löstes bättre med det visualiseringsstöd som gavs av det visuella gränssnittet visualiseringsstöd.

2.4 Val och utförande av åtgärd

I responsfasen vidgas lämpliga åtgärder utifrån arbetet som genomförts under övervakningen och orsaksanalysen. De vanligaste typerna av respons är: ingripanden, återkoppling och rapportering (Goodall et al., 2004). Exempel på ingripanden är att dra ur nätverkssladden, ominstallera en dator, uppdatera programvara eller ändra användares behörigheter. Återkoppling innebär vanligen att anpassa signaturernas regler i automationssystemet eller att välja ny data att samla in. Det vill säga, återkoppling ger input till den konfiguration som beskrevs i avsnitt 2.1. Rapportering innebär att sprida informationen om hotet till andra eller att fördjupa analysen av hotet (t.ex. insamling av forensiska data för analys och vidta juridiska åtgärder tack var genomförd analys).

Valet av åtgärd(er) beror på inte enbart på den aktuella händelsen utan även på logganalytikerns roll i organisationen och logganalytikerns mandat/ansvar/behörighet. Eftersom rätt respons är beroende av tillgången som angrips och logganalytikerns mandat/ansvar/behörighet så är det svårt att fastslå en allmän mall för vilken åtgärd som bör genomföras vid olika angrepp. Cichonski m.fl. (2012) menar att strategin för att välja rätt strategi för att begränsa skadeverkningarna bör ta hänsyn till: potentiell skada, krav på att bevara bevis, tillgänglighetskrav, samt kostnaden och effektiviteten. Dessa bedömningar kan vara svåra. Att bedöma hur effektiv en lösning är kräver till exempel en god teori om säkerhet som går att använda med den information som är tillgänglig.

Trots att det är fullt möjligt att studera människor och deras agerande i responsfasen så verkar det inte finnas någon publicerad forskning som empirisk testar vad som påverkar logganalytikers prestation under åtgärdsfasen. Ben-Asher and Gonzalez (2015a) har dock testat hur detaljnivå i återkoppling till tidigare analyser (som ju skapas i åtgärdsfasen) påverkar framtida övervakningsförmåga. De fann som väntat att detaljerad återkoppling om vad som var korrekt ökade förmågan att identifiera vanliga angrepp, men också att det gav sämre förmåga att detektera nya typer angrepp jämfört med när återkopplingen var mer abstrakt.

3 Mänskliga förmågor och färdigheter inom logganalys

Logganalytiker samlar in information och genomför analyser, vilket delvis görs med automationsstöd. Både datainsamling och analys kräver mänskligt handhavande av systemet, exempelvis konfigurera automatiska funktioner, övervakning och beslut om åtgärder i den manuella analysen och ständigt analyserande av enstaka händelser eller processer. För att genomföra en effektiv träning är det nödvändigt att förstå uppgifterna, förstå hur logganalytiker genomför uppgifterna och hur de tänker. Inom Human factors finns det en lång forskningstradition om mänskliga förmågor och begränsningar. Human factors definieras av International Ergonomics Association och har accepterats av Human Factors and Ergonomics Society:

"Ergonomics (or human factors) is the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance. Ergonomists contribute to the design and evaluation of tasks, jobs, products, environments and systems in order to make them compatible with the needs, abilities and limitations of people."

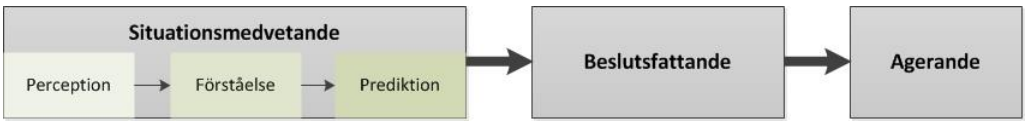
(HFES, 2015)

Syftet med detta kapitel är att utifrån logganalytikers arbetsuppgifter identifiera relevanta koncept och metoder inom Human factors området. Endsley (1995) har sedan mitten på 90-talet skapat begreppet situationsmedvetande och framtagit en välkänd modell som beskriver situationsmedvetande. Även om situationsmedvetande används av många så är det inte alltid uppenbart vad som menas eftersom begreppet används på olika sätt. Den mest etablerade synen på begreppet är den som presenterades av Endsley (1995) för tjugo år sedan. Situationsmedvetande definieras av Endsley som:

"the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future"

Endsley, 1998, p. 97.

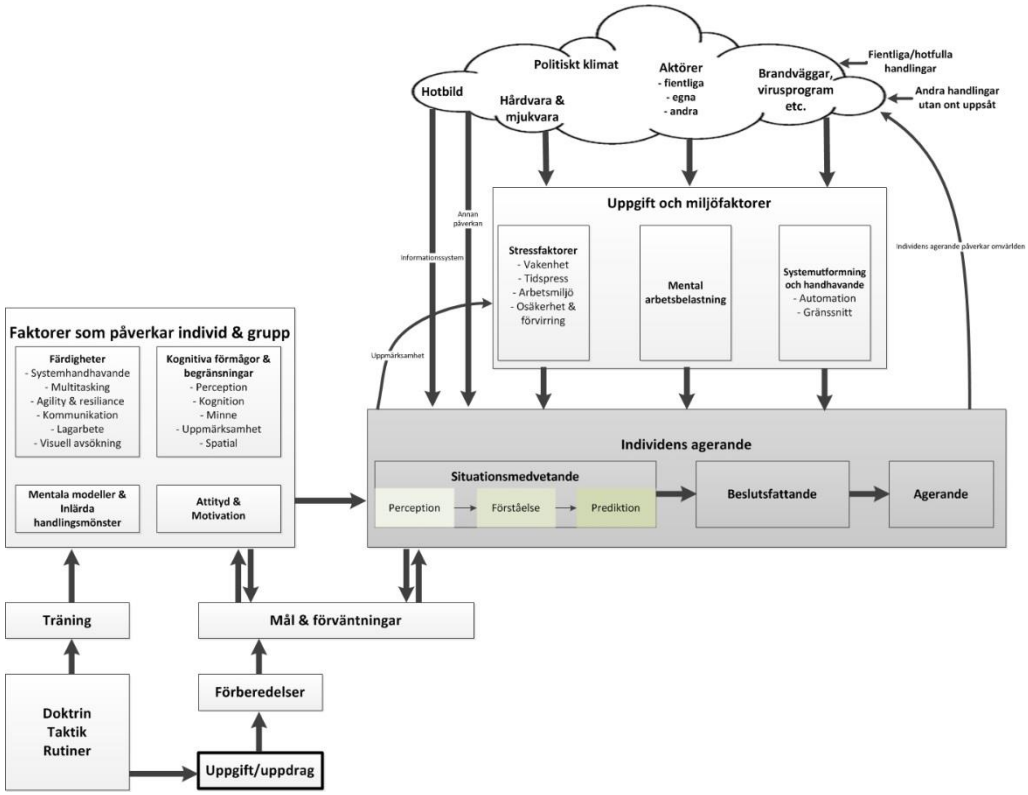
I denna modell beskrivs de tre stegen situationsmedvetande, beslutsfattande och agerande. Situationsmedvetande delas vidare in i perception, förståelse och prediktion.



Figur 2. Den centrala delen i situationsmedvetande (perception, förståelse och prediktion), beslutsfattande och agerande.

Situationsmedvetande är ett begrepp som bl.a. kan användas för att bättre förstå komplexa situationer och system. Situationsmedvetande formas bland annat genom påverkan av omgivning, tekniska systems kapacitet, gränssnitt, stress, mental arbetsbelastning, komplexitet, grad av automation och mänskliga resurser såsom erfarenhet, träning och olika förmågor. Situationsmedvetande kan ses som en integrerad lägesbild som användaren har och fattar beslut efter. Eftersom de flesta situationer och system är dynamiska så måste lägesbilden ständigt uppdateras för att bra beslut ska kunna fattas. Dåligt situationsmedvetande kan ge katastrofala effekter i form av olyckor för flygplan, trafik och kärnkraftsanläggningar (Endsley, 1999; Endsley & Smolensky, 1998; Hogg, Folles, Strand-Volden, & Torralba, 1995).

Brist på situationsmedvetande kan vara ett problem inom cybersäkerhet eftersom logganalytiker övervakar stora datamängder i mycket komplexa nätverk som dessutom ofta är geografiskt distribuerade. För att förstå en logganalytikers arbete och identifiera lämpliga övningssituationer är det nödvändigt att ta hänsyn till alla de faktorer som kan ha en betydande påverkan på prestationen. Med utgångspunkt från en modell framtagen av Endsley m.fl. (2000) presenteras en anpassad modell i Figur 3 för att beskriva logganalytikernas arbete.



Figur 3. Modell av situationsmedvetande om omgivande faktorer, modifierad efter Endsley m.fl. (2000).

Enligt Endsley m.fl. (2000) finns både miljöfaktorer (t.ex. stressfaktorer) och faktorer i omgivningen (t.ex. fientligt agerande) som påverkar användares agerande. Varje användares prestation påverkas även av individuella färdigheter, förmågor och begränsningar, inställning och tidigare erfarenheter (Figur 3). Exempel på färdigheter är systemhanterande, multitasking, anpassningsbarhet, kommunikation, lagarbete och visuell färdighet att söka information. Kognitiva förmågor och begränsningar inkluderar perception, kognition, minne, uppmärksamhet och spatial förmåga. Erfarenhet från tidigare händelser och arbete med aktuell problematik påverkar i direkt mening genom inlärda handlingsmönster men också genom att användaren redan innan händelsen har en mental modell om vad det är som sker. Användarens motivation och attityd till att vilja lösa problemet är ytterligare en individuell faktor som påverkar utfallet. Dessutom påverkas användaren av tidigare träning, möjligheten till förberedelser, uppsatta rutiner för att lösa problemet och vilka mål och förväntningar som finns.

Metoder för att bedöma situationsmedvetande kan delas in i: behovs- och kravanalys, frysa scenario, realtidsundersökningar, subjektiva skattningar efter försök, observatörsprotokoll och processanalyser Två av de populäraste mätmetoderna är Situation Awareness Global Assessment Technique (SAGAT) och Situation Awareness Rating Technique (SART) som beskrivs utförligt av Stanton m.fl. (2013). Vid användande av SAGAT så avbryts en simulering vid en slumpmässig tidpunkt och användaren ombeds att besvara frågor om specifika parametrar på en display eller predicera framtiden utifrån den senast tillgängliga informationen. För en logganalytiker så kan det till exempel innebära att man fryser och döljer informationen på skärmarna för att sedan fråga användaren vilka som är inloggade i det aktuella systemet eller om det finns någon specifik dator som nämnts i larm upprepade tillfällen de senaste tio minuterna. SART bygger på självskattningar och används vanligen efter en övning (ibland efter del av övning) och innehåller 10 dimensioner för att mäta situationsmedvetande där varje dimension mäts med en sjugradig skala. För en logganalytiker kan det till exempel innebära att efter genomförd övning skatta upplevd komplexitet, engagemang, fokus på uppgiften och hur mycket mental kapacitet som upplevs finnas över för att lösa andra uppgifter.

Nedan beskrivs ett urval av såväl uppgifts- och miljöfaktorer och individuella faktorer mer ingående. Urvalet har gjorts med utgångspunkt från vad som bedöms speciellt viktigt för logganalytiker.

3.1 Uppgifter och miljöfaktorer

Uppgiften och miljöfaktorer påverkar möjligheterna att erhålla bra situationsmedvetande och bör följaktligen beaktas. Nedan beskrivs hur stressfaktorer, mental över- och underbelastning och systemutformning kan påverka situationsmedvetandet för en logganalytiker.

3.1.1 Stressfaktorer

Det finns både fysisk social/psykologisk stress som påverkar prestationen. Fysisk stress orsakas av rådande arbetsmiljö, t.ex. ljud, vibrationer, ljus, trötthet och utmattning. Social och psykologisk stress syftar på oro, till exempel på grund av oklara arbetsuppgifter, konsekvensen av att göra fel i viktiga situationer och tidspress. Logganalytiker riskerar att utsättas för både fysisk och psykologisk stress.

Arbetsmiljön för logganalytiker är generellt bra i meningen att de oftast arbetar i kontorslokaler. Men ett uppenbart problem kan vara att de sitter lång tid framför skärmar där de ska upptäcka och analysera larm. Logganalytiker sitter ofta framför flera skärmar och genomför ofta ett monotont och oregelbundet arbete där stora mängder data ska övervakas och det endast är ett fåtal incidenter som

ska tillvaratas (Mancuso et al., 2014). Denna typ av arbete kräver både delad och selektiv uppmärksamheten, effektiv skanning av mönster, bibehållen uppmärksamhet och stor minneskapacitet (Donald, 2008). Det är ett välkänt fenomen att uppmärksamheten försämras över tid (Baker, 1962). Vakenhet kan testas för att förstå logganalytikernas arbetssituation i övervakningsfasen för att optimera systemet från Human factors perspektiv. Även om vakenhet kan vara ett generellt problem för logganalytikerna så är detta speciellt kritiskt under övervakningsfasen där användaren hanterar loggar och arbetet riskerar att bli monotont.

Tidspress i situationer där uppgifter måste genomföras på kort tid är inte ovanliga och aktuella för logganalytiker, t.ex. i samband med att en allvarlig attack inträffar. Forskning har visat att ökad stress begränsar uppmärksamhet och förmågan att ta in perifer information (Bacon, 1974; Weltman, Smith, & Engstrom, 1971). Dessutom finns det en tendens att främst samla in och använda den information som är mest vanligt, eller som vid en första anblick verkar passa in (Broadbent, 1971). Detta kan vara problematiskt eftersom det kan leda till felaktigt situationsmedvetande. Stress kan även leda till att arbetsminnets kapacitet begränsas och försvårar åtkomst av tidigare förvärvad kunskap som lagrats i långtidsminnet (Hockey, 1986; Mandler, 1979). För en logganalytiker kan detta innebära att förmågan att korrelera information från olika källor och förmågan att inhämta ny information reduceras.

För att mäta vakenhet kan psykofysiologiska metoder såsom hjärtslag, pulsvariabilitet, hudkonduktans och blinkfrekvens användas. Även responstid vid sökande efter objekt eller tid att upptäcka och agera vid larm kan användas. Subjektiva skattningar av mental arbetsbelastning, till exempel med NASA-TLX, kan även användas som en indikator på vakenhet.

3.1.2 Mental arbetsbelastning

Mental arbetsbelastning är ett etablerat begrepp som används av många inom Human factors (t.ex.Tsang & Wilson, 1997). Det underliggande teoretiska antagandet är att människor har en begränsad förmåga att processa information (Kahneman, 1973). När en uppgifts svårighet och komplexitet ökar så innebär det ökad mental arbetsbelastning. Om kraven överstigen förmågan så klarar inte användaren att genomföra den aktuella uppgiften.

Mental arbetsbelastning är ett komplext begrepp som inte har en enhetlig definition, men ett förslag på definition av Gopher och Donchin (1986) är:

> "... mental workload may be viewed as the difference between the capacities of the information processing system that are required for task performance to satisfy performance expectations and the capacity available at any given time."
>
> (Gopher and Donchin 1986, p. 41-3)

Förmågan att rikta uppmärksamhet mot något är ett exempel på en förmåga som påverkas negativt när den mentala arbetsbelastningen ökar. Det finns många alternativa metoder med olika känslighet så det är inte givet vilken metod som passar till vilken situation (Matthews, Reinerman-Jones, Barber, & Abich, 2015). Exempel på metoder är: (1) mätning av prestation på sekundäruppgift som indikator för mental arbetsbelastning när en primäruppgift genomförs, (2) psykofysiologisk mätning (t.ex. variabilitet i hjärtfrekvens), och (3) subjektiva självskattningar som är en delskala av NASA-TLX (Hart & Staveland, 1988), modifierad Cooper Harper skala (Wierwille & Casali, 1983) och SWAT(Reid & Nygren, 1988). Ofta kombineras metoder, t.ex. genom att mäta puls och subjektiva självskattningar av sin mentala arbetsbelastning. En del av metoderna är omfattande och därför finns det i vissa fall förenklade versioner för att det under ett försök ska vara praktiskt genomförbart att mäta mental arbetsbelastning.

3.1.3 Systemutformning

Gränssnitt ger ofta visuell information och ibland även auditiv information till logganalytikern. Möjligheten att interagera med gränssnittet på ett logiskt och intuitivt sätt är avgörande för att logganalytikern ska kunna fatta bra beslut snabbt och effektivt. Logganalytikern klarar typiskt inte att manuellt hantera alla inkommande larm, vilket medför att automation är nödvändigt. En bra implementerad automation kan ge stora fördelar i övervakningsprocessen; en dåligt implementerad automation kan leda till stora negativa effekter, t.ex. att logganalytikern missar viktiga larm eller attacker. En uppgiftsanalys (Stanton et al., 2013) är ofta lämpligt för att tydliggöra möjliga vinster och risker med automation. Ett vanligt problem i komplexa system är att användare inte vet hur automationen fungerar, t.ex. vilka regler som styr om intrångsdetektionssystem ger olika larmar. Erfarenheter från andra domäner visar att det är viktigt att användare av automatiserade analyser kan stänga av eller påverka nivån automation manuellt (Olson & Sarter, 1998). Användarens tillit till systemet och dess automation är en annan viktig faktor som påverkar hur användaren arbetar med systemet. Beroende på systemets prestation, korrekta larm och missar så påverkas användarens förtroende för systemet (Hoff & Bashir, 2015; Lee & See, 2004). Förtroendet byggs upp över tid och om ett system larmar för ofta eller missar viktiga händelser finns risken att användaren helt ignorerar larm och istället söker alternativa lösningar på problemet, t.ex. genom att söka annan information. Detta är ett känt problem också inom i cybersäkerhetssammanhang (Axelsson, 2000). Automation sker enligt ett kontinuum från helt manuellt till helt automatiserat. Sheridans och Verplank (1978) har till exempel utvecklat en mätskala med tio nivåer och förtroende mellan människa/användare och system där en checklista som tagits fram av Jian, Bisantz, Drury och Llinas (2000) används.

3.2 Faktorer som påverkar individ och grupp

Med utgångspunkt från modellen i Figur 3 beskrivs här faktorer som påverkar individen och gruppen på ett övergripande sätt. Fyra områden beskrivs: (1) färdigheter, (2) kognitiva förmågor och begränsningar, (3) mentala modeller och inlärda handlingsmönster, och (4) attityd och motivation. Alla dessa faktorer går att träna på olika sätt, vilket i slutändan kan påverka situationsmedvetande och agerande positivt.

3.2.1 Färdigheter

När det kommer till färdigheter kopplat till logganalys är många indelningar tänkbara. Exempelvis skulle de 25 uppgifterna kopplat till *Computer Network Defense Analysisi* NIST:s National Cybersecurity Workforce Framework (NICE, 2015) användas. I denna rapport delas färdigheterna in i systemhandhavande, multitasking, agility och resiliens, kommunikation, lagarbete och visuell avsökning.

3.2.1.1 Systemutformning och handhavande

System idag är ofta mycket komplexa och det krävs träning för att använda dem på ett effektivt sätt. Dessutom ger många system olika möjligheter, dvs. de går att anpassa till olika behov och olika användare. Olika konfigurationer ger olika möjligheter och det är inte givet att användaren förstår potentialen i de många alternativ som finns. Det krävs erfarenhet och kunskap för att nyttja system effektivt, vilket oerfarna användare oftast inte har. Det finns i många kurser på marknaden som syftar till att öka förmågan att hantera olika system som används inom logganalys. Vissa av dessa erbjuder certifiering, vilket kan användas som en indikation på hur väl en person kan hantera systemet. Mer generella mätmetoder finns också att tillgå, Till exempel genom enkäter för att mäta egenskattad förmåga (Murphy, Coover, & Owen, 1989).

3.2.1.2 Multitasking

Människor utför ofta flera uppgifter simultant, t.ex. äter frukost, lyssnar på musik och läser tidningen samtidigt. Multitasking är relaterat till förmågan till delad uppmärksamhet, men handlar mer om själva utförandet av en uppgift. Det handlar om interaktionen mellan perception, kognition och motoriska färdigheter, t.ex. att analysera ett larm och samtidigt övervaka nya larm.

Multitasking, dvs. utförande av flera uppgifter simultant, är relevant i samtliga logganalysuppgifter som beskrivs i kapitel 2. Det finns en uppenbar risk att logganalytiker inte klarar att genomföra alla arbetsuppgifter samtidigt eftersom kapaciteten att processa information är begränsad. Om logganalytikern utför flera uppgifter simultant och tvingas avbryta en aktuell uppgift för att lösa en annan kan det vara problematiskt att återgå till den första uppgiften. Det finns olika

typer av avbrott som kan inträffa. Vid perceptuella avbrott så tvingas logganalytikern ofta söka information mellan flera skärmar och källor, vilket kan ta tid. Vid motoriska avbrott så handlar det ofta om att flytta datormusen och trycka på olika knappar, t.ex. för att en dialogruta dyker upp. Både perceptuella och motoriska avbrott kan vara tidskrävande och frustrerande, men mest problematiskt är ofta kognitiva avbrott där personen måste börja om med en uppgift. Är avbrottet någon eller några sekunder så kan det vara enkelt att återgå till uppgiften, men om avbrottet är längre så minns ofta inte personen det hon gjorde innan, eller hur hon tänkte för att lösa uppgiften. Våra resurser för att handskas med perceptuella, kognitiva och motoriska uppgifter är begränsade. Som Salvucci och Taatgen (2011) föreslår så kan uppgifter placeras in enligt ett kontinuum från uppgifter som endast tar några sekunder till uppgifter som tar lång tid. Som Stanton m.fl. (2013) har beskrivit att det är svårare att återuppta arbete under hög arbetsbelastning. På motsvarande sätt kan korrelationsanalys användas för att undersöka sambandet mellan logganalytikers prestation och mätningar av deras mentala arbetsbelastning. Det råder delade meningar om hur prestation för multitasking bör mätas. Tid att utföra en uppgift och antal fel är två exempel på metoder som kan användas. Två exempel på enkäter som används är Polychronic Values (IPV) and Modified Plychronic Attitude Index 3 (MPAI3) (König & Waller, 2010; Poposki & Oswald, 2010) medan nylig forskning istället föreslår mätning av arbetsminneskapacitet för att prediktera multitasking-förmåga (Colom, Martínez-Molina, Shih, & Santacreu, 2010).

3.2.1.3 Agility och resiliens

Osäkerhet och förändring har identifierats som en faktor som bidrar till stress, vilket innebär att användares förmåga att hantera detta är viktig. Forskningsområdet om agility inkluderar frågor om hur individer och grupper att hantera situationer som man inte förväntat sig och därför riskerar att försämra prestationen. Agility är ett sätt att hantera kombinationen av komplexitet och osäkerhet och definieras som:

> *"Agility is the capability to successfully cope with changes in circumstances."*
>
> Alberts, 2011, p. 66

För att beskriva agilitet så har sex koncepts identifieras (NATO, 2014): (1) lyhördhet/mottaglighet, (2) mångsidighet, (3) flexibilitet, (4) resiliens, (5) öppenhet för nya idéer och (6) anpassningsförmåga. Lyhördhet syftar på tiden det tar att upptäcka och respondera på något som sker eller som användare förutspår kommer att hända (t.ex. ett larm som uppstår eller agerande när det finns information om att något kommer inträffa). Mångsidighet syftar på att kunna

bibehålla en acceptabel prestation eller effektivitet även när uppgifter eller uppdrag skiftar. Flexibilitet syftar på att en enhet ska kunna lösa en given uppgift på mer än ett sätt och uppmuntrar att prova nya åtgärder på uppkomna problem istället för att åtgärda dem som man alltid gjort. Flexibilitet kräver förståelse för det faktiska problemet och kunskap om hur man kan nyttja alternativa åtgärder. Resiliens ses ofta av de som arbetar med agility som en del av agility medan andra betraktar resiliens som ett eget forskningsområde. Fyra koncept har identifierats av hur begreppet resiliens används: (1) återställande till utgångsläget, (2) robusthet, (3) tillförande av adaptiva resurser och (4) arkitektur som är flexibelt (Woods, 2015). Kan logganalytikern återställa systemet efter en attack? Behöver logganalytikern vara förberedd på att agera på olika sätt? Är logganalytikern medveten om vilka resurser som behöver tillföras vid olika typer av attacker? Är systemarkitekturen uppbyggd på ett sådant sätt att det finns viss flexibilitet att klara av vissa typer av attacker? Öppenhet för nya idéer innebär att logganalytikern utvecklar en ny taktik för att lösa nya problem. Anpassningsbarhet syftar på att förändra organisationen eller processerna för att bättre möta de krav som finns. I militära sammanhang kan agility delas i fysisk (t.ex. plattformens hastighet, miljö och vapensystem) och information (sensorer upptäcksavstånd och kvalité på uppmätt data) (Dekker, 2006).

Agility kan delas in manifest- (engelska: manifest) och möjlig (engelska: potential) agility. Manifest agility mäter hur en individ eller grupp hanterar förändringar. Det är ett relativt mått, t.ex. skillnaden mellan hur en situation ser ut och hur situationen kan utvecklas. Potentiell agility är ett relativt mått som jämför individers eller gruppers beredskap, men även den relativa effekten av alternativa lösningar eller processer (Alberts, 2011). Andra exempel på mått är att använda komplexitet (Arteta & Giachetti, 2004). Eftersom agility är ett relativt nytt forskningsområde så finns det goda möjligheter för utveckling av både konceptet och mätmetoderna.

3.2.1.4 Kommunikation

Bra kommunikation är avgörande för effektivt och säkert arbete. Det finns många teoretiska angreppssätt, t.ex. informationsprocess, strukturellt, och målorienterat synsätt. Begreppet ”Common ground” (Clark & Brennan, 1991) kombinerar kognitiva och sociala aspekter av kommunikation. Språket och icke-verbala signaler används implicit (t.ex. ansiktsuttryck och kroppshållning), explicit (t.ex. nicka med huvudet). Genom analys av hur individer, grupper eller organisationer arbetar kan förståelsen av arbetssituationen ökas (Morrow & Fischer, 2013). Analysen kan inkludera och eventuellt fokusera på specifika områden, t.ex. beslutsfattande och situationsmedvetande. Beroende på aktuell frågeställning så kan kommunikation avseende kvantifiering, fördelning, användande av tekniska system och hur logganalytiker sprider informationen analyseras. Logganalytikers kommunikation kan analyseras för att förstå hur de interagerar med det tekniska

systemet och medarbetare. Sedan kan detta jämföras med hur effektivt arbete bör bedrivas, t.ex. enligt en instruktion.

Diskursanalys innebär att det naturligt förekommande språket, t.ex. mellan logganalytiker, analyseras i den faktiska miljön. Det beskriver vem som pratar med vem, roller och vad som sägs givet den aktuella situationen (Winther-Jörgensen & Phillips, 2000).

3.2.1.5 Lagarbete

En grupp är en två eller fler individer som tilldelats roller eller uppgifter, interagerar med varandra och arbetar för att nå ett specifikt mål under en begränsad tidsperiod (Salas, Dickinson, Converse, & Tannenbaum, 1992). Varje medlem i gruppen har individuellt situationsmedvetande som delvis är överlappande med andra gruppmedlemmars situationsmedvetande (Kaber & Endsley, 1998; Salas, Prince, Baker, & Shrestha, 1995). Beroende på arbetets art så är det ofta mer effektivt att ta ansvar för olika delar i arbetet och komplettera varandra. Logganalytiker interagerar både med tekniska system och andra människor. Arbetet kan ske individuellt, men ofta sker samarbete med andra gruppmedlemmar och chefer. Individens situationsmedvetande påverkas dessutom bl.a. av gruppens processer och arbetsmetoder, t.ex. delge information till andra vid en cyber-attack. Gruppens situationsmedvetande representerar mer än att bara addera enskilda gruppmedlemmars situationsmedvetande (Schwartz, 1990). Gruppens situationsmedvetande definieras av Salas, m.fl (Salas et al., 1992) på följande sätt:

”a destinguishable set of two or more people who interact dynamically, independently, and adaptively toward a common and valued goal/object/mission, who have each been assigned specific roles or functions to perform, and who have limited life span of membership.”

Salas, m.fl., s. 4.

Gruppens medlemmar har oftast olika ansvar som inte delas av de andra gruppmedlemmarna, vilket innebär att individens situationsmedvetande endast delvis överlappar andra gruppmedlemmars situationsmedvetande (Salas et al., 1995). Logganalytiker som arbetar i grupp behöver ofta samla information från olika källor för att lösa en gemensam uppgift och bidra till skapandet av delat situationsmedvetande mellan gruppmedlemmar.

3.2.1.6 Visuell avsökning

Visuell sökning som begrepp kan användas för att beskriva visuella aktiviteter för både människor och tekniska system. Mänskligt visuell sökning innebär att en individ med ögonrörelser och genom att vrida på huvudet söker efter och förstå information, t.ex. på en display. I tekniska system kan visuell sökning innebära att en sensor på motsvarande sätt söker efter objekt, t.ex. en flygande farkost som

automatiskt försöker upptäcka människor på marken (Brogan, Gale, & Carr, 1993). Eftersom system idag är komplexa och innehåller mycket information så måste användaren ofta leta efter information i omgivningen eller på en eller flera displayer. För att underlätta för användare används t.ex. färg som informationsbärare eller lägga information som hör samman fysiskt nära varandra för att användaren inte ska behöva söka efter information på olika delar av displayen. Logganalytiker behöver ständigt söka efter och förstå viktig information som finns i stora mängder data. Deras arbete inkluderar ständigt visuell sökning som ofta är tidskrävande men kan underlättas om system designas och konfigureras på lämpligt sätt.

3.2.2 Kognitiva förmågor och begränsningar

Kognitiva förmågor och begränsningar inkluderar de mänskliga förmågorna perception, kognition, minne, uppmärksamhet och spatial förmåga. Dessa förmågor kan tränas, men samtidigt är det viktigt att notera att det finns medfödda begränsningar avseende hur information kan processas i den mänskliga hjärnan. Dessa begränsningar sätter gränser för hur arbete kan utföras och hur arbetsuppgifter bör utformas.

3.2.2.1 Perception

Perception inkluderar uppfattning av information med samtliga sinnen, men vid design av tekniska system förmedlas oftast information endast visuellt och auditivt. Forskning inom perception har en lång tradition där det finns många inriktningar, t.ex. gestalpsykologi, informationsprocessande och direkt eller ekologisk perception (Bruce, Green, & Georgeson, 1996). Det ekologiska synsättet som av många är det mest tilltalande framhäver bl.a. kopplingen mellan omgivningen och det som betraktaren ser, två delar som inte går att separera. Perception är det första av de tre stegen i den ovan beskrivna modellen av situationsmedvetande (Figur 3). För logganalytiker innefattar detta att upptäcka vad som sker på skärmen och i viss mån direkt dra slutsatser utifrån given information (som inom ekologiskt perspektiv kallas affordance).

3.2.2.2 Kognition

Kognition är ett brett begrepp som syftar på mentala processer som handlar om kunskap, tänkande och hantering av information. Begreppet är tätt sammankopplat med perception såtillvida att människor uppfattar information via sina sinnen (perception) och utifrån given information drar slutsatser från tidigare kunskap och erfarenheter och utifrån det fattar beslut. I modellen av situationsmedvetande (Figur 3) kan kognition primärt kopplas till förståelse och prediktion, men även till beslutsfattande. Logganalytikers arbete med analys och sökande av samband i informationen är kognitivt mycket krävande.

3.2.2.3 Minne

Vår minneskapacitet är begränsad avseende att temporärt hålla information i arbetsminnet och att mentalt bearbeta informationen (Baddeley, 1983). Steg två, förståelse i SA-modellen, involverar att hålla information i minnet och bearbeta information för att skapa förståelse. Denna process innefattar att integrera tidigare inlärd information för att skapa en helhetsförståelse, vilket kan vara en mycket krävande process. För logganalytiker kan det handla om att vid inkomna larm bedöma om det är ett alvarligt hot genom att mentalt jämföra informationen med tidigare larm, dvs. nyttja information som redan finns lagrad i långtidsminnet. Det finns en uppenbar risk att användare överbelastas och inte har mental kapacitet att uppfatta eller analysera andra inkommande larm. Logganalytiker förväntas predicera vad som kommer ske om en åtgärd verkställs och bedöma risker om åtgärder inte sätts in tidigt. Även detta är minneskrävande och med begränsad kapacitet så är risken uppenbar att det inte finns reservkapacitet för att upptäcka andra hot eller utföra andra uppgifter.

3.2.2.4 Uppmärksamhet

Vid beskrivningen av uppmärksamhet används ofta *filter* och *bränsle* som metaforer (Fernandez-Duque & Johnson, 1999). Filter beskriver det sensoriska systemets begränsningar (speciellt syn och hörsel) för att acceptera och processa information. Denna metafor syftar på att vi selektivt väljer bort viss information eftersom möjligheten att processa information är begränsad. Bränsle används för att beskriva begränsningen i informationsprocessen (perception, arbetsminne, beslutsfattande och agerande). Uppmärksamhet beskrivs enligt denna metafor som mental energi eller resurser som fördelas och anpassas till den aktuella uppgiften eller uppgifterna. Metaforerna är inte motstridiga utan uppmärksamhet kan allokeras på två nivåer. På den övre nivån (bränsle) riktas uppmärksamheten mot uppgiften, där flera uppgifter kan konkurrera om samma uppmärksamhet, t.ex. en logganalytiker som ständigt övervakar loggar, bedömer risker på uppkomna larm och ibland interagerar med andra. Analytikern behöver fatta beslut om vilken av uppgifterna som är viktigast. På den lägre nivån så behöver personen filtrera information, t.ex. välja vilka larm som är prioriterade och skicka viss information vidare till andra logganalytiker för djupare analys eftersom en logganalytiker kan fördjupa sig i ett specifikt problem och samtidigt hålla uppmärksamhet till den ständig uppdaterade listan med systemloggar.

Wickens m.fl. (2013) beskriver förmågan till uppmärksamhet är begränsad och kan beskrivas med hjälp av begreppen: selektiv-, fokuserad- och delad uppmärksamhet. Selektiv uppmärksamhet syftar på förmågan att välja vilken information som ska processas. Fokuserad uppmärksamhet syftar på förmågan att fokusera på en uppgift även när vi blir ditraherade av andra uppgifter. Delad uppmärksamhet syftar på förmågan att fokusera på flera uppgifter samtidigt trots att det inta alltid är möjligt (t.ex. en logganalytiker som försöker handskas med information från flera källor simultant).

Uppmärksamhet kan mätas genom responstid, t.ex. för att mäta hur lång tid det tar när en deltagare söker efter ett objekt på en display. För en logganalytiker kan tiden för upptäckt av ett larm mätas. Blickpunktsregistrering och analys av detta är en annan värdefull metod som kan ge information om var en logganalytiker tittar, vilket inte innebär att de ser och förstår informationen. Analyser från blickpunktsregistrering mäter även ögonrörelser visar kan visa avsökningsmönster, vilket kan öka logganalytikers medvetenhet om hur de arbetar, men det kan också ge viktig information till systemutvecklare på vad i ett system och gränssnitt som behöver förändras. En studie (McIntire, McKinley, McIntire, Goodyear, & Nelson, 2013) visas att bl.a. blinkfrekvens, pupillhastighet och pupillens diameter förändras över tid vid en simulerad cyberuppgift. Sambandet mellan dessa mått och arbetsbelastning finns dessutom beskrivet i en rapport av Castor m.fl. (2003).

3.2.2.5 Spatial förmåga

Den spatiala förmågan förutsätter att syn, hörsel och känsel fungerar normalt och handlar om upplevelsen av det tredimensionella rummet. Kopplingen till visuell perception är tydlig och förmågan inkluderar att uppfatta form, storlek, riktning, linjers lutning för att därigenom skapa en bra omvärldsuppfattning. Även tid är en viktig faktor i den spatiala förmågan. Tosto, m.fl. (2014) beskriver även hur spatial förmåga kan predicera prestation i matematik och expertis inom bl.a. vetenskap och teknologi. För en logganalytiker kan det handla om att sammanlänka information från t.ex. flera larm, sekvenser av larm som kan uppträda på olika platser vid olika tidpunkter i ett nätverk. Analytikerns uppgift blir att tolka och dra slutsatser och eventuellt upptäcka hot som annars skulle förbises.

3.2.3 Mentala modeller och inlärda handlingsmönster

Mentala modeller skapas från erfarenhet och underlättar problemlösning i olika situationer. De definieras som:

> ”våra konceptuella uppfattningar om hur saker fungerar, händelser äger rum och hur människor beter sig.”
>
> Norman (1988)

Mentala modeller kan hjälpa oss förklara något som inträffat eller förstå orsaken till ett problem utan att egentligen veta exakt vad som skett. Från tidigare kunskap och erfarenhet så tror sig en person veta bakomliggande orsak och fattar ofta beslut utifrån detta. I många situationer underlättar mentala modeller problemlösning eftersom de vanligen ger en bra övergripande bild av bakomliggande orsaker, men risken finns att ny felaktig information adderas till en redan befintlig mental modell, eller att den befintliga mentala modellen är felaktig. Oerfarna användare som interagerar med datorer har till exempel ofta en mycket begränsad förståelse för hur en dator fungerar (begränsad eller felaktig mental modell). Risken är stor att

personen inte söker det verkliga problemet utan gör felaktiga antaganden eftersom de tror sig känna igen eller förstå ett problem. Logganalytiker som har en bra övergripande mental modell över nätverket har sannolikt en ökad förståelse och förmåga att predicera (steg tre i modellen av situationsmedvetande, se Figur 2) hur ett virus riskerar spridas i ett nät.

3.2.4 Attityd och motivation

Motivation och attityd har en direkt påverkan på inlärning och därigenom en indirekt påverkan på prestation i faktiska situationer. Motivation kan beskrivas som viljan eller önskan att engagera sig i en uppgift. Motiverade personer engagerar sig och visar stort intresse vilket ofta leder till att de lägger mer tid på träning (Garris, Ahlers, & Driskell, 2002). Inneboende drivkrafter såsom viljan att utforska, upptäcka och lära leder till positiv inlärning, medan yttre faktorer såsom belöningar och betyg, i stället kan hämma inlärningen genom att den som tränar skiftar fokus från själva inlärningsuppgiften till belöningen (Deci & Ryan, 1985). Attityd och motivation är viktigt för logganalytiker.

4 Övning, träning och prövning

Inom FM syftar all utbildning ytterst till att höja förbandens insatsförmåga (Försvarsmakten, 2013). Alla handlingar i ett militärt sammanhang genomförs för att lösa uppgifter och utbildning ska därför bedömas efter hur den bidrar till att lösa dessa uppgifter. FM definierar begreppet övning i vid bemärkelse till att omfatta allt från lektion inomhus till färdighetsträning utomhus, och begreppet träning sätts som synonymt med övning.

Övningar kan ändå ha olika eller flera syften. Ibland används begreppet övningar även för sådant som borde benämnas försök eller prov. Övningar kan således ha flera, eller andra, syften än att utbilda den deltagande personalen. Enligt FM (Försvarsmakten, 2013) är inlärning eller befästande av kunskap och färdigheter det som i första hand avses med den verksamhet som genomförs under begreppet övning. Men ibland är syftet att utveckla nya metoder eller att pröva hur ny teknik skulle kunna användas i verksamheten. Ibland benämns sådan verksamhet för utvecklingsövning, men ofta används helt enkelt begreppet övning även här. Ibland finns också flera olika syften kopplade till en och samma övning. För viss personal kan det vara en klassisk övningsverksamhet, medan annan personal genomför ett försök med ny organisation. Ibland finns flera olika syften inblandade med olika krav på hur verksamheten genomförs och på vilka scenarier som används, vilket kan medföra utmaningar för de som har att planera och genomföra övningen. Ett annat syfte som ofta förekommer är att pröva nuvarande förmåga hos ett förband eller hos viss personal. En faktor som blir extra viktig i en prövande övning är den utvärdering som genomförs med mätning av prestation och förmåga, i kontrast till att endast ge lärande återkoppling.

En viktig faktor att beakta vid övningar inom cybersäkerhet är vem som ska övas och vad som ska läras. Som uttrycks i kapitel 1.2 är det gruppen – arbetslaget – som är den centrala lösaren av problem och uppgifter. Men gruppens förmåga är beroende av den kunskap som varje individ besitter, vilket ger att olika typer av övningar med olika inriktning och syfte kommer att vara nödvändiga för att utveckla cybersäkerhetsförmåga. Olika utbildningsmetoder kommer att behöva tillämpas och nedan beskrivs kort några exempel, hämtade ur FM Pedagogiska grunder (2006). Definitionerna är breda och många delar kan vara gemensamma för olika metoder. En exakt gränsdragning kan därför vara svår, men översiktligt finns till exempel följande metoder:

- *Formella metoder*: syftar till att lära ut ett exakt och korrekt handlande i en klart definierad situation, ett så kallat slutet problem.
- *Tillämpade metoder*: syftar till att utveckla förmåga att agera i oklara situationer, att hantera så kallade öppna problem.

- *Problembaserad inlärning (PBL)*: är ett grupparbete där 7-8 personer ges uppgiften att kring ett definierat avgränsat problem skaffa den kunskap som behövs för att åstadkomma en lösning.
- *Case metoden*. Liknar PBL men gruppen kan vara större (60-80 personer) och instruktören har en aktiv roll. Ett praktikfall gås igenom stegvis och komplikationer diskuteras som en motor för lärande.
- *Förmedling*. Den klassiska undervisningssituationen där en lärare beskriver, förklarar och instruerar för att öka elevernas kunskaper. Föreläsning, föredrag och förvisning är exempel där förmedling har stor del.
- *Enskild övning*. Syftar till att ge en individ ökad kunskap för att sedan kunna lösa uppgifter i grupp.
- *Grupparbete*. Handlar i huvudsak om att flera personer (3-6) tillsammans arbetar kring en problemställning.
- *Taktisk beslutsövning*. Är en övning under tidspress där deltagaren får en kort tid (vanligen 5 minuter) på sig att identifiera en situation och skriva ner sina beslut och plan för lösning.
- *Drill*: En utbildningsmetod som syftar till att utveckla automatiserade handlingar för att säkerställa att dessa kan utföras i pressade situationer.
- *Psykisk beredskapsträning (PBT)*. Är FM benämning på den träning av psyket som syftar till att ge utövaren bästa möjliga beredskap att utföra förväntade handlingar.

En faktor som ofta behandlas inom FM är just förmågan att kunna agera och utföra handlingar i psykiskt och fysiskt belastande situationer, det vill säga under stress. I utbildningssituationer måste däremot stress bemötas och hanteras beroende på vad som ska övas. En effekt av stress är att tankebanorna för lärande blockeras, vilket är direkt kontraproduktivt för lärande övningar. Den ursprungliga innebörden av stress omfattade både fysisk och psykisk påverkan ”*det fysiologisk-hormonella tillstånd, som inträder då organismen utsätts för skadlig påverkan*” (Nationalencyklopedin, 1995). Begreppet har använts på olika sätt för att beskriva olika typer av påverkan, vilket innebär att när begreppet används är det lämpligt att inkludera den definition man avser. Ofta avses psykisk belastning och då används ofta begreppet *press* för att särskilja den delen från fysisk belastning (Albrecht, 1980). Det är viktigt att inse att vad som är press för en individ kan vara stimulans för en annan och ge upphov till stress hos en tredje, beroende på vilka förutsättningar som finns. Stimulans är viktigt för att erhålla en lagom utmanande utbildningssituation, men med bibehållen balans är nödvändigt för att undvika oönskad belastning och stress.

I FM Pedagogiska grunder (2006) ges 10 perspektiv på övningen vilka även bör beaktas vid upprättande av träning för cybersäkerhet. Nedan redogörs för begreppen:

1. *Mål med övningen.* Varje övning måste ges ett tydligt mål som beskriver vad man ska kunna utföra efter övningen.
2. *Övningsdynamik*. Lärande är en dynamisk process som är omöjlig att förutsäga i detalj, vilket medför att utbildning kan ske med ”*undan-för-undan planering*”. Varje steg i en utbildning eller övningsserie bygger på resultaten av föregående moment.
3. *Tid för övningen*. Det är viktigt att den studerande får arbeta med den aktuella övningen utan avbrott och splittring. Tillräcklig tid måste allokeras för respektive övning för att maximera lärandet.
4. *Sammanhang*. Det är centralt att elever förstår vad slutmålet och syftet med en övning är för att kunna lära sig effektivt. Detta innebär att vissa grundläggande övningar kan genomföras efter att en sammansatt övning som visar slutmålet genomförts. Lärande sker inte alltid stegvis med ökande svårighetsgrad, utan beroende på sammanhang så kan ordningen på komplexitet och svårighetsgrad alterneras.
5. *Förståelse*. Det är mycket viktigt att alla övade förstår syfte, sammanhang och mål med övningen, och denna förståelse kan variera med bakgrund och tidigare utbildning.
6. *Organisation*. Det är viktigt att övningen är tydligt organiserad och att detta kommuniceras till deltagarna på ett anpassat sätt.
7. *Aspekter av kunskap*. De tre olika aspekterna av kunskap som nämnts tidigare, *konstruktiv, kontextuell och funktionell,* måste behandlas inom varje övning. Växelspelet mellan kunskap som redan finns, problem som upplevs och erfarenheter som görs (den konstruktiva aspekten) är motorn i lärandet och bör integreras i övningen. Kontexten måste vara relevant för att lärande ska uppstå vilket kan åstadkommas med en miljö och ett nätverk som motsvarar den övades normalbild. Den funktionella aspekten som består av att den övade ser mening och sammanhang i det som ska läras måste också integreras och belysas.
8. *Planering*. Övningen måste planeras utifrån ett helhetstänkande där faktorer som innehåll, ramfaktorer, metoder, mål, utvärdering och förutsättningar beaktas.
9. *Frågan*. En väsentlig del i lärandet är reflektion vilket kan stimuleras med frågor från läraren eller instruktören. Att utforma relevanta, bra och välformulerade frågor en väsentlig del av övningen.

10. *Läraren på estraden*. I vissa delar av en övning kommer läraren eller instruktören att hamna i centrum av all uppmärksamhet. En mängd olika faktorer bör beaktas inför denna situation som i militära sammanhang har mycket gemensamt med ledarskap och att vara en föregångsman. En väsentlig del är kunskap om området och kunskap om lärande, samt rättrådighet, rättvisa, saklighet och ärlighet.

För mer information kring dessa faktorer listar Pedagogiska grunder (2006) 16 olika erfarenheter. Ovanstående beskrivningar ger initial information om begreppen övning träning och olika utbildningssituationer och faktorer att beakta vid framtagning av övningar och träningssituationer. Nedan följer beskrivningar av typer av kunskap och lärande (avsnitt 4.1), sätt att lära sig (avsnitt 4.2) och planering av övningar (avsnitt 4.3) och reflektion och återkoppling (avsnitt 4.4).

4.1 Typer av kunskap och färdighet

Övningar används för att ge personal och förband möjligheter att lära sig lösa de uppgifter de tilldelats. Ett övergripande syfte är således att deltagarna, eller eleverna, ska erhålla kunskap kring lösandet av dessa uppgifter. Vad kunskap är beskrivs i ett resonemang i Pedagogiska grunder (2006) och vi beskriver några faktorer som bedöms relevanta för arbetet med logganalys.

Kunskap kan i en förenklad modell beskrivas som en produkt eller en process. Synen på kunskap som *produkt* innebär att individen tar till sig en mängd tidlösa sanningar; synen på kunskap som *process* inriktade synen innebär att lärande är en ständigt pågående aktivitet starkt kopplad till de yttre omständigheter i vilken kunskapen ska tillämpas. En annan indelning gäller ytkunskap och djupkunskap. *Ytkunskap* ses som en kvantitet, att kunna minnas och återge vad andra skrivit eller sagt, utan att fokusera på tolkning och koppling. *Djup kunskap* är istället inriktad på innebörd och mening, som en kvalitet där individen sätter in fakta och erfarenheter i ett sammanhang. En annan indelning som görs gäller teoretisk kunskap respektive praktisk kunskap. Den *teoretiska* kunskapen meddelas i ord; den *praktiska* kunskapen är förmågan att lösa problem och utföra uppgifter i verkligheten, men kan vara svår att beskriva. Praktisk kunskap kan även delas in i *uttalad* och *tyst* kunskap. Den uttalade kan beskrivas i tal och text, men den tysta är mer sådan man gör utan att reflektera över det.

Vid diskussioner kring kunskap och lärande används ofta begrepp som faktakunskap, förståelse, färdighet och förtrogenhet. Begreppen är inte heltäckande men förenklar diskussioner och de samspelar inbördes utan rangordning. *Faktakunskap* är att veta hur saker och ting förhåller sig. *Förståelse* är en insikt om sammanhang och innebörd. När vi kan omsätta vår kunskap för att göra någonting är det en *färdighet*. *Förtrogenhet* är när individen har förmåga

att handskas med ett fenomen utan stöd och hjälp och förstår konsekvenser av olika ageranden.

Tre aspekter på kunskap som är viktiga för att förstå hur kunskap utvecklas och används är den konstruktiva aspekten, den kontextuella aspekten och den funktionella aspekten. Den kontextuella aspekten betonar att inlärning sker i ett sammanhang. Den *konstruktiva* aspekten menar att utveckling av kunskap är en aktiv och skapande process hos den enskilda människan som bygger på vad individen vill uppnå i förhållande till redan innehavd kunskap, erfarenheter, och problem med nuvarande kunskapsnivå. Lärandet bygger till stor del på individens egna ambitioner och utmaningen för en utbildare blir att skapa och främja det egna initiativet. För att kunskapen ska bli meningsfull är det viktigt att sammanhanget i lärandet är relevant, både det fysiska och det sociala sammanhanget. Den fysiska miljön bör vara tillräckligt lik den verkliga miljön och samspelet med omgivande människor måste finnas. Den *funktionella* aspekten innebär att den inlärda kunskapen betraktas som ett redskap för att åstadkomma någonting, för att lösa uppgifter.

En ofta använd beskrivning av detta resonemang kring kunskap är Blooms taxonomi (Tabell 2). Taxonomin har använts sedan 1950-talet (Bloom, 1956), men en revision med ambitionen att göra modellen mer användbar för att planera utbildningsprogram och lärande gjordes 2001 av Anderson & Krathwohl (2001).

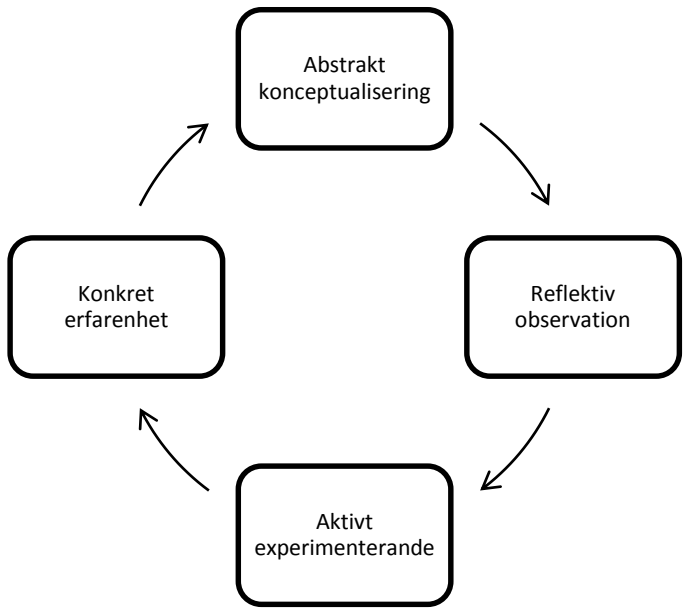
Tabell 2. Beskrivning av de begrepp som används i Blooms taxonomi.

Nivå	*Inlärd kunskap och färdighet*
Skapa	Sätta samman kunskapsdelar för att skapa en funktionell helhet. Omorganisera kunskapselement i nya strukturer och mönster genom skapande, planerande eller produktion. Sätta samman saker, för samman olika delar, presenterar innehåll, planerar försök, sätter ihop information på nya kreativa sätt.
Utvärdera	Göra bedömningar baserade på kriterier och standarder genom kontroller och kritiskt tänkande. Definiera standarder, bedöma med hjälp av bevis och rubriceringar, acceptera eller förkasta utifrån kriterier.
Analysera	Dela upp information i beståndsdelar. Avgöra hur delar hänger ihop inbördes och i helhet genom att differentiera, organisera och beskriva. Bryta ner koncept, analysera strukturer, bedöma antaganden och värdera relevans.
Tillämpa	Genomföra och använda procedurer. Tillämpa praktiska teorier, lösa problem och använda information i nya situationer.
Förstå	Skapa meningsfullhet från muntlig, skriva eller grafisk information genom att tolka exemplifiera summera, jämföra och förklara. Förstå tillämpning och konsekvenser.
Minnas	Återkalla, känna igen och minnas relevant kunskap från långtidsminnet. Lära sig och komma ihåg begrepp, fakta, metoder, processer och koncept.

4.2 Hur man lär sig

Generellt sätt finns två perspektiv på lärande för FM:s personal: individuellt lärande eller lärande i grupp (Försvarsmakten, 2013). Dessa två perspektiv kompletterar varandra och bör kombineras för att stödja effektivt lärande. Individuellt lärande handlar om individens intag av information och utformning av beteende. Lärande i grupp belyser vikten av sociala relationer och externa förutsättningar. Denna typ av lärande lägger vikt på interaktioner och deltagande som skapar ett sammanhang. Lärande sker genom deltagande utförande av arbetsuppgifter samt interaktion och samverkan med andra. Erfarenhet och reflektion är två nyckelfaktorer för lärande i båda två ansatserna. Erfarenhet är kopplat till upplevelser från handlingar som sker individuellt eller i grupp och reflektion är en process av tolkning och skapande av förståelse av denna erfarenhet.

Hur vuxna människor lär sig och bygger erfarenhetsbaserad kunskap bygger till stor del på teorier grundade av Kurt Lewin under 1940-talet (Brehmer, 2015) men som fördjupats och vidareutvecklats av bland annat (Kolb, 1984). Enligt Kolb är reflektion över genomförd verksamhet grunden för att erfarenheter omvandlas till professionell kunskap och förmåga vilket när det sätts in i ett sammanhang kan beskrivas som en cirkulär och kontinuerlig modell, Kolbs cykel för erfarenhetsbaserat lärande (Figur 4).



Figur 4. Kolbs cykliska modell för erfarenhetsbaserat lärande.

Kolbs lärandecykel innehåller fyra steg för att lära från erfarenheter och en individ kan gå in i en cykel vid vilket steg som helst, men stegen måste genomföras i sekventiell ordning för att ett framgångsrikt lärande ska vara möjligt. Förloppet är även kontinuerligt där en lärandecykel följs av fler i en kontinuerlig process. Modellen beskriver också att det inte är tillräckligt att var med om en upplevelse för att man ska lära sig något. Man måste reflektera över erfarenheten för att sedan dra slutsatser och formulera nya begrepp som sedan tillämpas i en ny situation. Individen måste kunna göra kopplingen mellan teori och handling genom att planera, agera, reflektera och koppla tillbaka till teorin. Denna modell är en tvåvägsprocess där handling leder till kunskap som leder till förbättrad handling. Modellen är en grundteori för lärande som tillämpas idag vid olika läroanstalter, till exempel vid Polishögskolan i Umeå som bakgrund till praktiska övningar och utbildningssituationer.

Transfer av träning syftar på vilken effekt träningen har på agerande i verkligheten (Gestrelius, 1998). Det har föreslagits att transfer endast äger rum när det finns identiska element mellan träning och verklighet(Laktasic, 1976). Detta innebär att träning och verklighet åtminstone bör efterlikna varandra i så stor utsträckning som möjligt. Transfer av träning kan vara positiv, noll eller negativ. Positiv transfer innebär en förbättrad prestation i den verkliga miljön, noll att det inte finns någon effekt, och i vissa fall kan träningen leda till negativ transfer med försämrad prestation i den verkliga miljön som resultat (Hammar, Bergström, Åkerström, Thorstensson, & Oskarsson, 2012). Begreppet horisontell och vertikal transfer används också. Horisontell innebär att kunskap och färdigheter överförts till den lärande, medan vertikal transfer innebär att informationen kan användas på ett mer automatiserat sätt i verkliga miljöer.

För att träningen ska bli effektiv är det nödvändigt att identifiera vilka *kompetenser* utbildningen gäller, i vilka *situationer* dessa ska kunna användas och vilka *kriterier* som används för att utvärdera utbildningen. Genom att kartlägga vilka arbetsuppgifter som inkluderas i en befattning så kan sedan kompetenser matchas för att individen eller gruppen ska kunna genomföra sina uppgifter på bästa sätt. kompetenser kan beskrivas på olika sätt, bl.a. med utgångspunkt från Bloom (1956) och Krathwohl, Bloom och Masia (1964) med mekaniska, kognitiva och sociala förmågor. Vilka kompetenser som är nödvändiga eller önskvärda för logganalytiker är i nuläget inte utrett.

Under övning och träning av specialister på cybersäkerhet måste särskild hänsyn tas till förmågan att abstrahera och generalisera erhållen kunskap. Tidigare studier visar att under träning och övning är detaljerad återkoppling grundläggande för att lära sig hur arbetet fungerar och vilken struktur som funnits på hot och arbetsuppgifter. Men som Ben-Asher & Gonzales (2015b) beskriver så måste en kvalificerad logganalytiker även lära sig att hantera övergripande återkoppling och abstrahera information och data för att se sammanhang och på så sätt öka sin förmåga att möta nya, icke tidigare upplevda hot Kärnan i det resonemang som förs gäller att detaljeringsgraden av viss typ av återkopplad information är mycket viktig för viss typ av inlärning av strukturer och mönster, medan en lägre detaljeringsgrad för den typen av återkoppling av data stimulerar den övade att själv analysera strukturer och mönster. Detta innebär att vid övning av logganalytiker bör olika typer information och innehåll under återkoppling varieras och nyttan och effekten noggrant utvärderas.

4.3 Planering av övningar

Övningar i olika typer av anläggningar är idag en viktig del i att utveckla och vidmakthålla förmågan vid FM:s förband. Övningar kan genomföras som momentövningar eller mer sammanhängande insatslika övningar. Övningarna är uppbyggda för att vara lärandemiljöer för medverkan och faktiska upplevelser

där olika representationer av omgivningen är centrala. Olika grad av simuleringar av den fysiska och sociala miljön är väsentliga för att belysa och förstärka handlingsmönster och tankemönster i skapade situationer. Det krävs både individuella färdigheter och organisatorisk förmåga för den enhet som övas för att på ett effektivt sätt lösa uppkomna uppgifter.

Problemlösning är en central förmåga för personal som arbetar med logganalys enligt Oser, Gualtieri, Cannon-Bowers och Salas (1999) som beskriver en metod för att angripa problemlösningsövningar för team; händelsebaserad approach till träning (EBAT) där följande punkter är centrala: (1) definition av lärandemål; (2) utveckling av utlösande händelser; (3) specifikation av mätpunkter för effektivitetsmätning; (4) scenariogenerering; (5) övningsledning; (6) datainsamling; (7) genomgång efter övning; samt (8) databashantering och arkivering. En faktor som författarna hänvisar till som en central funktion för att kunna öva lösning av komplexa problem är den miljö som är karakteriserar naturalistiskt beslutsfattande (Klein, 2008), vilket i princip är en modell för att beskriva hur människor fattar beslut i verkliga situationer, ofta under tidspress, och där informationsunderlaget är bristfälligt. Orasanu och Conolly (1995) listade åtta faktorer att beakta i naturalistiska miljöer, det vill säga miljöer som till stor del liknar verkligheten (har hög grad av realism i viktiga aspekter), och dessa är i olika grad relevanta för logganalys: (1) illa strukturerade problem; (2) föränderlig omgivning; (3) skiftande eller motstridiga mål; (4) loopar för återkoppling; (5) tidsbrist (stress); (6) risk för stora förluster; (7) många aktörer; samt (8) tvingande organisatoriska mål. Dessa faktorer är centrala för logganalytiker och bör beaktas när övningar planeras och genomförs. Inom projektet finns stora möjligheter att i övningsmiljön CRATE särskilt betona dessa faktorer, med olika vikt vid olika tillfällen för att möte behovet av att öva i realistiska miljöer. Genom att belysa någon eller några faktorer vid respektive övningstillfälle kan svårighetsnivån anpassas efter aktuella kunskapsnivåer och lärmål.

Wickens, m.fl. (2013) anser att det viktigt att planera övningars innehåll och delmoment så att dessa inte blir för sekvenserade och tagna ur sitt sammanhang. Noggrann analys av vilka moment som ska övas, hur dessa hänger ihop och hur svårigheter i övningar anpassas till rådande färdighetsnivå är centralt för att erhålla god effekt av träning och övning. Om dessa analyser görs och övningar anpassas till identifierade tränings- och övningsbehov kan goda resultat för organisatoriskt lärande och förmåga erhållas (Winfred, Winston, Edens, & Bell, 2003). Det är också viktigt att i förväg definiera vilka mätbara parametrar som indikerar att förmågan inom enheten ökat och att personalen blivit mer kunnig om utvärdering av övningars utformning, stegring och sammanhang ska vara möjlig (O'Connor et al., 2008).

Avgörande för att lära från erfarenhet och problemlösningssituationer är den reflektion som genomförs efter en händelse eller ett förlopp. I en pedagogisk

situation är det en av instruktörens eller lärarens viktigaste uppgifter att stödja den processen för att säkerställa ett positivt och effektivt utfall. Denna process beskrivs mer i detalj nedan.

4.4 Reflektion och återkoppling

Enligt Kolb (1984) är reflektionen en nyckelfaktor för att omsätta upplevelser till kunskap och färdigheter. En viktig del för lärandet från övningar är därför reflektionsfasen och det utbyte som där kan ske, både internt hos respektive deltagare, men också mellan deltagare och mellan deltagare och handledare. Forskningen som belyser hur mycket lärandet kan ökas genom systematisk och metodisk återkoppling är spridd över olika områden, men en studie gör gällande att individer och arbetsgrupper kan öka sin prestation med 20 till 25 procent med hjälp av strukturerad reflektion i samband med övningar eller insatser (Tannenbaum & Cerasoli, 2013). I synnerhet i situationer när datorer och simuleringar används finns stora möjligheter att dra nytta av metoder och verktyg för att förstärka reflektionsprocessen, eftersom datainsamling (loggning) oftast är relativt enkel att göra – händelseförloppets ”sanning” är ju i den simulerade världen inne i datorer. Teori kopplat till reflektion och återkoppling samt tillhörande datainsamling beskrivs nedan.

En etablerad metod för att genomföra återkoppling är after-action review (AAR), som ursprungligen utvecklats för tillämpning vid militär stridsträning (Morrison & Meliza, 1999; Rankin, Gentner, & Crissey, 1995) men numera vidareutvecklats och används brett vid olika typer av övningar, försök och insatser som beskrivs av Wikberg m.fl. (2005). Metoden går ut på att strukturerat gå igenom händelseförloppet i en övning eller insats och fokusera på hur händelser upplevts och vad som kan läras från det. Metoden är ursprungligen tänkt att användas tillsammans med verktyg för återuppspelning av händelseförlopp men AAR kan även användas som en diskussionsmetod utan inspelat material. Händelseförloppet gås igenom i kronologisk ordning och fokus läggs på vad som förväntats, vad som hände och varför det hände och vad som kan förbättras.

Med avstamp i AAR och med stöd av datoriserade verktyg för att visualisera händelseförlopp har en metod för rekonstruktion och utforskning (Reconstruction & Exploration: R&E) utvecklats (Jenvald, 1999; Morin, 2002). R&E bygger på att använda ett datorverktyg för att bygga en uppspelningsbar modell av ett händelseförlopp vilken sedan kan visualiseras och användas för olika syften, bland annat för att stödja lärande genom att genomföra AAR med pedagogiskt fokus (Jenvald, 1999). Metoderna för den uppspelningsbara modellen (mission history) beskrivs ingående av Morin (2002). Den uppspelningsbara datormodellen över ett händelseförlopp kan även användas på fler sätt med olika syften och sju olika alternativ har föreslagits (Thorstensson, 2008):

1. Planering. Som underlag för att planera en övning kan tidigare övningars dokumentation användas. Syften, övningsmål och krav definieras med utgångspunkt i övergripande målsättningar. Utifrån syfte med övningen definieras även en datainsamlingsplan.
2. Presentation före övning. Tidigare övningar är en källa till mycket kunskap och som förberedelse för den egna kommande övningen bör de övade förevisas tidigare inspelade övningar.
3. Under pågående övning. Om loggning av data genomförs under en övning på ett sådant sätt att den är visualiseringsbar kan övningsledningen använda detta för att styra och kontrollera händelseförloppet.
4. After-action review (AAR). Den strukturerade genomgången efter övning är en väsentlig del av inlärningsprocessen vid en övning.
5. Post-mission analys. Om insamlad data från övningen innehåller delar som medger analys av händelseförlopp, prestation och utfall finns stora möjligheter att dra djupare slutsatser från genomförandet än vad som kan åstadkommas vid en AAR. Det är viktigt att de erfarenheter som görs vid AAR återförs till modellen och används vid de efterföljande analyserna.
6. Lessons learned. Processen att organisatoriskt lära från de erfarenheter som görs vid övningar, incidenter och insatser brukar benämnas lessons learned. Här kan den dokumenterade datormodellen över händelseförloppet vara en viktig del.
7. Kunskapsöverföring. En viktig del med en övning är att sprida erhållen kunskap från olika aktörer eller organisationer till andra berörda parter. Här är det viktigt att ta hänsyn till de säkerhetsrestriktioner som kan finnas i samband med CS-övningar.

Den datainsamling som ligger till grund för R&E kan varieras stort utifrån vilket syfte övningen har, vilka resurser som finns tillgängliga och vilken ambition övningen har givits. Den datainsamling som genomförs bör ha både tekniskt och humant fokus och bygga både på subjektiva och objektiva metoder (Lif & Oskarsson, 2012). Vilken data som ska samlas fån en specifik övning beror alltid på syftet med datainsamlingen men en huvudpoäng är ofta att kunna sätta aktörers upplevelser i samband med det faktiska händelseförloppet. På så sätt kan diskussioner föras kring vad som faktiskt hände, hur detta upplevdes och hanterades och vilka resultat som faktiskt erhölls. Tekniska loggar från använda system tillsammans med observatörsprotokoll och användarenkäter bör vara återkommande datakällor.

Grunden för att samla data vid träningstillfällen är att stödja förmågeutvecklingen vid den tränade enheten. Med hjälp av insamlad data kan

inlärningen stärkas genom att data används som grund i kvalificerad återkoppling efter övning (AAR), men även genom att data kan ligga till grund för analys och utveckling av de metoder, procedurer och rutiner enheten arbetar efter. Djupanalys av hur operatörer angriper problem och vilka effekter detta får kan baseras på stora mängder insamlad data som kan visualiseras och analyseras med hjälp av olika typer av verktyg. En förutsättning för att fördjupa dessa analyser är att insamlad data innehåller både teknisk information om händelseförloppet i nätverket, och data om åtgärder och beteende både från angripare och övade. Hur människor uppfattat det som hände måste kunna sättas i förhållande till vad som faktiskt hände. Ofta finns skillnader mellan hur människor uppfattar ett händelseförlopp och hur det faktiskt var. Ibland är dessa skillnader stora och ofta finns skillnader mellan olika individers uppfattningar. För att kunna genomföra de fördjupade analyserna behöver således objektiva data kombineras med subjektiva data, både från observatörer och deltagare. Datainsamling behöver alltså ske både utifrån ett tekniskt perspektiv och ett humanperspektiv.

Data från det tekniska perspektivet syftar framför allt till att få kunskap om *vad* operatören gör i nätverket och *hur* han/hon agerar. Exempel på frågor som besvaras är: vilka verktyg används och vilka delar av nätverket undersöks? I humanperspektivet är fokus på *varför* operatörer agerar som de gör. Frågor såsom arbetsbelastning, situationsförståelse och förståelse av automation kan besvaras, se kapitel 3. Datainsamling inom dessa två perspektiv ger möjlighet till en bra analys av agerande och arbetsprocesser samt förståelse av hur experter inom logganalys arbetar och möjliggör även en bra återkoppling till de som tränas. Exempel på information som kan samlas in presenteras i Tabell 3. Viss del av denna information kan samlas in genom olika logginsamlingsverktyg, men annan information bör smalas in med hjälp av kvalificerade observatörer som följer specifika observationsprotokoll. Denna information kan även användas för att ställa subjektiva frågor till operatörerna. Även loggning av operatörsbeteenden bör göras genom dokumentation med film och ljudinspelning. Datainsamlingen från nätverket kan sedan matchas med logganalytikernas subjektiva uppfattning. Det kan även vara värdefullt att genomföra datainsamling i form av expertintervjuer för att öka förståelsen för varför operatörerna agerat på ett specifikt sätt. Dessa frågor ska betraktas som ett exempel på sådan data och trafik som kan samlas in snarare än en färdig lösning. Valet av datainsamling måste alltid anpassas till den aktuella frågeställningen. En genomgång på olika typer av data som kan användas presenteras i Lif och Oskarsson (2012).

Tabell 3. Exempel på data som kan samlas in och protokoll som kan användas under träningen. Från D'Amico m.fl. (2005).

IP-adresser
• Är IP-adressen extern eller intern? • Är IP-adressen på en lista av ”heta adresser”? • Är IP-adressen kopplad till en misstänkt enhet eller känd antagonist? • Är IP-adressen spoofad?
Portar/protokoll
• Är det ökad aktivitet vid en specifik port? • Sker något som inte borde ske via en port/protokoll? • Är det någon avvikelse från det normala protokollbeteendet? • Sker det någon aktivitet på en port som borde vara stängd/blockerad?
Pakets innehåll
• Överskrider pakets innehåll den förväntade storleken? • Finns det strängar i paketets innehåll som matchar icke önskvärda signaturer (från tidigare kända attacker)? • Är antalet bytes ovanligt konsistent?
IP beteende
• Finns det andra larm som kan associeras med ursprungs-IP, mål-IP eller subnet? • Skickar en intern IP information externt i samband med skannande eller en attack (eller försök till attack)? • Skickar en intern IP ut mycket information? • Vem talar käll-IP med? • Vilka tjänster kör en IP? • Finns det förändringar över tid avseende typen/antalet av protokoll och kopplingar? • Antar en IP flera roller (t.ex. agerar som både klient och server)?
Temporala aspekter
• Tid: När skedde aktiviteten och vad skedde samtidigt? • Varaktighet: Hur snabbt skedde det inträffade? Kan man dra några slutsatser om det fanns människor involverade, eller var det en helt automatiserad process? • Upprepning: Finns det tecken på att detta upprepas över tid?
Förståelse mellan incidenter
• Delar skilda incidenter några gemensamma faktorer (IP eller subnet adresser, portnummer, tid på dygnet, mm)?

5 Förslag på övning, träning och prövning för logganalytiker

Det finns en stor mängd tänkbara alternativ för övning, träning och prövning för logganalytiker. I detta kapitel beskrivs sju alternativ för övning, träning och prövning. Dessa sju relateras till viktiga faktorer som tagits upp tidigare i rapporten. Nämligen:

- Vilken (eller vilka) av de fyra typer av uppgifter en logganalytiker kan behöva lösa som adresseras (kapitel 2).
- Vilka mänskliga förmågor och färdigheter (kapitel 3) är i fokus. Detta inkluderar betydelsen av faktorer kopplade till uppgiften och miljön, faktorer kopplade till individen och situationsmedvetande.
- Typ av övning, träning och prövning (kapitel 4) kopplat till olika typer av kunskap och färdighet, olika sätt att lära sig, planering av övningar och betydelsen av reflektion och återkoppling för lärande.

De lösningar som presenteras nedan beskriver inte alla tänkbara alternativ för övning, träning och prövning av logganalytiker. Inte heller individuella- och gruppfaktorer är uttömmande beskrivet för allt som kan beaktas vid konstruktion av lösningsalternativ. Nedan beskrivs uppgift (kapitel 2), mänskliga förmågor och färdigheter (kapitel 3), och övning, träning och prövning (kapitel 4) övergripande för respektive övningsförslag. De sju övningarna som presenteras nedan ska ses som intressanta alternativ som anses relevanta för projektet ÖvExCy.

5.1 Manuell analys av logghändelser

Uppgift: Den manuella analysen omfattar tre övergripande moment: inspektera händelser i loggar för att identifiera potentiella hot, genomföra en orsaksanalys och föreslå en åtgärd. Dessa utförs, som kapitel 2 beskrev, delvis överlappande med varandra. Övervakning görs i regel kontinuerligt medan orsaksanalys och en eventuell åtgärd utförs när det bedöms vara nödvändigt. I denna övning ges deltagarna i uppgift att utföra hela den manuella analysen för att hantera en serie angrepp som har skett och som pågår under övningen. Detta innebär inte bara att deltagarna behöver utföra flera aktiviteter i följd, utan också att de behöver prioritera mellan olika aktiviteter och sannolikt utföra flera parallellt. Till exempel utföra slagningar i loggar och i väntan på att de blir klara analysera andra loggar. Det övergripande syftet med den manuella analysen är att rekommendera lämpliga åtgärder. Hur väl deltagarna lyckas med detta kan avgöras av en expert som känner till de faktiska angreppen. Men eftersom flera

deluppgifter ingår i den manuella analysen kan flera sätt att mäta deltagarnas prestation vara aktuella.

Mänskliga förmågor och färdigheter: Systemet och framför allt gränssnittet som används bör vara detsamma eller snarlikt som det logganalytikern är van vid. Uppgiften är komplex och kräver bra situationsmedvetande för att analytikern ska kunna fatta bra beslut. Deltagarnas mentala arbetsbelastning kommer sannolikt kommer vara hög. För att lösa uppgiften så måste logganalytikerna framför allt tillämpa och analysera logghändelser med utgångspunkt från de mentala modeller logganalytikerna har. Används realistiska scenarier så kan logganalytikernas mentala modeller användas och utvecklas till att mer efterlikna hur faktiska angrepp genomförs. Logganalytikernas förmåga att söka efter information och förmågan att klara flera uppgifter simultant (multitasking) kommer tränas. Dessutom kommer kognitiva förmågor såsom minne, uppmärksamhet och spatial förmåga tränas och vid upprepad mätning över tid så kan individens utveckling kartläggas.

Övning, träning och prövning: Uppgiften innefattar framförallt individuellt lärande och kan betraktas som en sammanhängande insatsövning där hela kedjan med situationsförståelse, beslutsfattande och agerande inkluderas. Även om uppgiften inte kommer att vara helt realistisk möjliggörs träning av beslutsfattande i en komplex situation som påminner om den verkliga situationen. Återkoppling ges till deltagarna genom automatiserad statistik på hur väl åtgärder fungerar mot angreppen och mer pedagogiskt genom kvalitativ återkoppling från en instruktör. Analytikernas föreslagna åtgärder kan också testas för att utvärdera hur effektiva de hade varit mot en verklig attack.

5.2 Prioritera loggposter för vidare analys

Uppgift: Övervakningen av tillstånd, händelser och larm handlar i stor utsträckning om att filtrera ut loggposter som är symptom på elakartat beteende eller annat som kan orsaka IT-säkerhetsrisk. Detta kan göras i takt med att loggposter kommer in i systemet, i efterhand mot en databas av loggar eller båda i kombination. I denna övning förses deltagarna med en ackumulerad mängd historiska loggar där såväl godartade som elakartade händelser har övervakats. Bland loggarna kan till exempel godartat beteende som epostanvändning och applicering av systemuppdateringar blandas med spridning av skadlig kod. Deltagarnas uppgift är att identifiera vilka loggposter som bör undersökas noggrannare, beskriva varför de valts ut och eventuellt prioritera vilka som bör undersökas först.

Mänskliga förmågor och färdigheter: Övervakning sker vanligtvis under viss mental arbetsbelastning och kräver att ett stort antal loggposter gås igenom under kort tid där den mentala arbetsbelastningen kan varieras genom ökad tidspress eller genom ökad komplexitet. Då prioritering under tidspress är kognitivt

krävande bedöms individens allmänna kognitiva förmåga (t.ex. korttidsminne) och förmågan att avsöka stora datamängder (bl.a. loggar) vara av stor vikt. Detta arbete kan underlättas av en bra mental modell av hur elakartat beteende yttrar sig. En initial analys kräver inte att analytikern förstår hela händelsekedjan, men däremot bör analytikern efter genomförd övning kunna sammanfatta vad loggposterna beskrev för händelser.

Övning, träning och prövning: Denna uppgift handlar framför allt om att tillämpa eller analysera tidigare kunskaper. Tillämpa syftar på att en metod eller heuristik som lärts ut och analysera syftar i detta fall till att logganalytikern ska göra egna bedömningar. Även om djup kunskap oftast eftersträvas kan ytlig kunskap vara tillräcklig i den initiala delen av denna uppgift. Både individuellt lärande och sociala aspekter i grupp, det senare genom arbeta i par. För att förstärka analytikernas positiva handlingsmönster är det av stor vikt att den typ av prioriteringar som görs i uppgiften är av samma typ som görs i praktiken. Återkopplingen bör knytas till deltagarnas kunskap om systemet och förståelse för vad som är normalt.

5.3 Identifiera påverkade systembehörigheter och systemresurser

Uppgift: Att identifiera vilka behörigheter och resurser en angripare har kommit över kan vara av stor vikt för att på ett bra sätt hantera ett pågående angrepp och för att hantera skadereduktion i efterhand. I denna övning ges logganalytikern en rapporterad anomali att starta med, till exempel ett antiviruslarm eller onormalt datoranvändande, och uppgiften att reda ut vilka delar systemet som har blivit komprometterade. I uppgiften ingår inte att rekommendera åtgärder för att hantera incidenten utan enbart att regelbundet reda ut vilka systembehörigheter och datorresurser som redan har påverkats av angreppet. Detta görs genom att rapportera korrekta beskrivningar av vilka systembehörigheter och systemresurser angriparna har kommit över. Till sitt förfogande har deltagaren historiska loggar av olika slag och detaljerad information om det övervakade systemet.

Mänskliga förmågor och färdigheter: Denna uppgift genomförs primärt utan tidspress för att efterlikna den verkliga situationen. System med gränssnitt och funktioner bör efterlikna de som används i praktiken för att färdigheter i att hantera systemet och söka efter information i loggar ska kunna tränas. Förståelsen av vilka delar i systemet som påverkas underlättas av bra mentala modeller, vilka kan tränas och uppdateras med ny erfarenhet. För att lösa uppgiften behöver analytikern kombinera teoretisk och praktisk kunskap. Den teoretiska kunskapen är nödvändig för att förstå själva anomalin och den praktiska kunskapen fås med erfarenhet för att veta vad som kan betraktas normalt i ett system.

Övning, träning och prövning: Logganalytikern ska identifiera loggposter, förstå vad angriparna har gjort och göra kvalificerade bedömningar angående systembehörigheter och systemresurser angriparen tillskansat sig. I denna process tränas framför allt individuella egenskaper och alla tre nivåerna av situationsmedvetenhet är inblandade (perception, förståelse och prediktion). Detta är en momentövning med en delmängd av orsaksanalysen som en logganalytiker kan tänkas göra i driftmiljöer. För att förstärka den positiva inlärningen i form av handlingsmönster bör både den anomali som startar processen, de övervakade systemen och angreppen vara realistiska. Analytikern kommer efter övningen vara bättre på att bedöma när en analys av detta slag kommer att vara träffsäker. Då sekvensen av angrepp kan bestämmas i förhand finns goda förutsättningar att ge tydlig och detaljerad återkoppling. Denna återkoppling kan till exempel ges i form av detaljerade beskrivningar av angreppen och de loggposter de genererade.

5.4 Identifiera utnyttjad sårbarhet och föreslå åtgärd

Uppgift: I orsaksanalysarbetet är en central uppgift att identifiera hur incidenter uppstått och vilken väg/vektor som använts i angreppet. Det är i många fall en förutsättning för att kunna täppa till de säkerhetsbrister som utnyttjas i angreppet, och liknande brister som inte utnyttjas ännu. I denna övning ges deltagaren i uppgift att identifiera vilken sårbarhet som nyttjas i ett angrepp och föreslå en konkret åtgärd för att hantera sårbarheten. Övningen inleds med att deltagaren ges information om ett eller flera tydliga symptom på ett angrepp, till exempel i form av en anomali rapporterad av en användare. Utifrån denna anomali ska deltagaren med hjälp av loggar identifiera sårbarheten eller sårbarheterna som utnyttjats och föreslå en kostnadseffektiv åtgärd.

Mänskliga förmågor och färdigheter: Uppgiften genomförs primärt utan tidspress och den mentala arbetsbelastningen bedöms vara låg. Systemet som används bör vara det samma eller likvärdigt med det som används i praktiken för att handhavande av systemet ska kunna tränas realistiskt. Analytikerns mentala modell om aktuella sårbarheter kommer tränas och eventuellt förändras. Uppgiften kan i praktiken behöva genomföras parallellt med andra analyser eller övervakning och multitasking är därför en viktig individuell faktor som kan tränas. Uppgiften inkluderar perception och förståelse men inte nödvändigtvis att predicera hur systemet påverkas över tid. Även beslutsfattande och förslag om agerande i form av kostnadseffektiv lösning är väsentligt.

Övning, träning och prövning: Syftet med denna övning är både att ge deltagaren praktisk erfarenhet av orsaksanalyser av olika slag och att ge deltagaren en allmän uppfattning om sin förmåga/möjlighet att identifiera vilken sårbarhet som utnyttjas under olika förutsättningar. Dessa förutsättningar kan till

exempel vara angrepp av olika typ eller informationsresurser av olika slag. Det är alltså inte bara analytisk förmåga som är i fokus, utan också deltagarens förmåga att utvärdera vad som är möjligt under olika förutsättningar. Analytikerna måste förstå på djupet och sätta in informationen i ett sammanhang för att förstå sårbarheter och föreslå åtgärder. Detta är en momentövning som kan upprepas för olika sårbarheter eller delsystem. Fokus är på det individuella lärandet och återkoppling bör bestå i en detaljerad beskrivning av det korrekta svaret och en expertbedömning av hur detta svar skulle kunnat identifieras med befintliga resurser. I ett mer ambitiöst fall görs också en bedömning av deltagarens arbetssätt för att bedöma om existerande resurser (t.ex. loggar) har utnyttjas på ett bra sätt.

5.5 Skapa en signatur som identifierat ett angrepp

Uppgift: Att konfigurera den automatiska analysen så att den kan känna igen de angrepp som kommer är en central del av logganalytikerns uppgifter. I denna övning ges deltagaren i uppgift att själv skapa och justera regler så att de ger larm för angrepp som beskrivs på olika sätt. Angreppen kan till exempel beskrivas textuellt i fritext, utifrån en exploit (åtgärd som utnyttjar svaghet i dator för att åstadkomma skada), en payload (lasten som utför den skadliga aktiviteten i dator), en regel skriven för ett annat logghanteringssystem, information om de logghändelser som angreppet orsakar eller en kombination av ovanstående. Uppgiften består av att skapa en regel eller liknande som larmar för angreppet, och som inte larmar för andra händelser i systemet.

Mänskliga förmågor och färdigheter: Systemutformningen bör efterlikna verkligheten, i synnerhet bör loggar som används i övningen vara av den typ som finns att tillgå i praktiken. Eftersom systemhandhavande (i form a regelskapande) övas så är det önskvärt att den formalism/syntax som används för att ange regler är snarlik den som deltagaren använder i praktiken. Uppgiften handlar om att förstå vilka avtryck ett angrepp gör i system, dvs. analytikern ska predicera påverkan på systemet baserat på abstrakt information och rimliga antaganden. Uppgiften genomförs inte under tidspress och den mentala arbetsbelastningen bedöms vara låg.

Övning, träning och prövning: Denna uppgift kräver djupkunskap där analytikern verkligen måste förstå angreppet för att kunna utveckla och justera regler för att upptäcka det aktuella hotet utan att larma för icke-hotfulla beteenden. Det individuella lärandet är i fokus men kan alterneras genom att analytikerna löser uppgiften i grupp. I denna uppgift kan en djupare kognitiv analys av hur analytikerns arbete avseende det aktuella hotet och skapandet av ny regel vara lämpligt. Återkoppling där regeln testas mot hot och en mer detaljerad återkoppling från instruktörer ökar sannolikheten för positiv inlärning.

5.6 Procedurträning

Uppgift: Det finns flera tänkbara delar av logganalysarbetet som kan struktureras upp genom processer med tydliga gränssnitt. Det är till exempel vanligt att övervakning av tillstånd, händelser och larm görs i en separat process av vissa personer medan orsaksanalys och åtgärder utförs av andra personer. Särskilt när ytterligare data, som en hårddisk, behöver samlas in för att kunna utföra orsaksanalysen. Det är också tänkbart att fastslå procedurer för olika typer av analyser, till exempel genom att ange vad som ska antecknas under en orsaksanalys eller vilken information som ska tas i beaktande innan åtgärd föreslås. Procedurer och förfaranden som dessa övas under ledning av instruktörer.

Mänskliga förmågor och färdigheter: I denna momentövning förväntas analytikerna följa förutbestämda procedurer, antingen för att lära från grunden eller för att förändra ett tidigare inte effektivt handlingsmönster. En viktig faktor kommer vara deltagarnas attityd och motivation till att följa angivna procedurer. Arbetet bör ske med realistiska system. Uppgiftens komplexitet bör vara låg för att minimera stress och mental arbetsbelastning.
Övning, träning och prövning: Inlärningen i denna uppgift handlar om att lära in processer för att arbetet ska ske effektivt. Det är viktigt att framtagna procedurer är tillämpbara i den aktuella situationen för att undvika negativ inlärning. Återkoppling sker bäst med en erfaren instruktör som är väl insatt i framtagna procedurer. Genomgång av analytikerns agerande bör inte bara bedöma om uppsatta procedurer följts, utan även reflektioner om procedurernas användbarhet och beskrivning av eventuella avvikelser från procedurerna. På så sätt kan både individen och procedurer utvecklas.

5.7 Beredskapstest

Uppgift: En serie koordinerade angrepp utförda av en ihärdig motståndare är ett tänkbart scenario som logganalytiker kan behöva handskas med. Logganalysförmågan kommer då att sättas under press och logganalytiker kommer sannolikt behöva samarbeta med varandra, prioritera mellan aktiviteter och arbeta under kraftig tidspress. För att öva på att hantera en sådan situation utsätts en grupp av logganalytiker för en serie sofistikerade angrepp som pågår under flera timmar. Uppgiften är att i enlighet med fastslagna procedurer identifiera vilka angrepp som sker, vilka men som uppstått, lämpliga åtgärder och angreppens övergripande syfte (t.ex. vilken information angriparen eftersöker).

Mänskliga förmågor och färdigheter:

Fokus i denna uppgift är att utsätta deltagarna för extrema situationer med mycket hög stress och mental arbetsbelastning. Arbetsmiljön bör vara familjär

för analytikerna som måste ges möjlighet att fokusera på problemlösning utan att lära sig nya verktyg. Förkunskapen om system och gränssnitt kommer vara avgörande för att denna övning ska kunna genomföras. Deltagarnas motivation förväntas vara hög eftersom denna övning kommer pressa deltagarnas gränser. Förmåga att klara flera saker samtidigt och förmåga att anpassa sig efter situationen kommer tränas. Deltagarnas kognitiva förmågor kommer testas och begränsningar kommer tydliggöras. Hela kedjan av situationsmedvetande, beslutsfattande och agerande inkluderas och både individens- och gruppens beteende kan utvärderas.

Övning, träning och prövning:

Denna övning syftar till att ge deltagarna insikt i hur de hanterar stress och tydliggöra deras begränsningar snarare än att lära dem faktakunskap eller nya procedurer. Uppgiften bör endast genomföras med erfarna deltagare. Analytikerna bör innan denna övning ha genomgått momentövningar där de tränat de olika delar som i denna situation sätts samman till en mer komplex övning med tidspress. Tid för reflektion och återkoppling, t.ex. genom AAR (after-action-review) är viktigt.

6 Diskussion och sammanfattning

Genom att beskriva hur logganalytiker arbetar, nyttja kunskap från Human factors området och pedagogisk kunskap presenteras i denna rapport sju förslag på hur logganalytiker bör genomföra träning. Respektive förslag inkluderar en beskrivning av uppgiften, mänskliga förmågor och färdigheter, och pedagogiska aspekter att beakta vid design av framtagna förslag. En genomgång och förståelse av logganalytikers arbete i verkliga miljöer med verkliga system har varit utgångspunkten för detta arbete. Därefter har en modifierad version av Endsleys modell om situationsmedvetande används för att beskriva faktorer som bedöms vara speciellt viktiga för logganalytiker, påverka av miljöfaktorer och typ av uppgift, och hur individen erhåller situationsmedvetande, fattar beslut och slutligen agerar. Exempel på faktorer som beskrivs och kopplas till logganalytikers arbete är mänskliga förmågor (t.ex. minne och uppmärksamhet), färdigheter (t.ex. klara flera uppgifter samtidigt och söka efter information), motivation och nyttjande av mentala modeller. Analytikerna påverkas dessutom av faktorer som stress, mental arbetsbelastning, systemets utformning och uppgiftens komplexitet. Samtliga dessa faktorer påverkar logganalytikerns arbete när situationsmedvetande eftersträvas för att kunna fatta bra beslut och slutligen vidta lämplig åtgärd för att förhindra att hot orsakar skada i viktiga system. För att de framtagna övningsförslagen ska ge önskad effekt (positiv inlärning) så beskrivs även välkända metoder för lärande, t.ex. Kolbs erfarenhetsbaserade lärande. Förslagen är beskrivna kortfattat och det återstår att i mer detalj utveckla dessa sju träningsförslag, bland annat att beskriva hur prestation värderas i respektive situation. Nästa steg är att utifrån mer detaljerade designförslag genomföra träning med logganalytiker, vilket planeras kunna genomföras under 2016.

7 Referenser

Alberts, D. S. (2011). *The Agility Advantage A Survival Guide for Complex Enterprises and Endeavers*. Washington D.C.: Department of defense, U.S.

Albrecht, K. (1980). *Chefen och stressen*. Stockholm: Liber läromedel.

Andersson, L. W., & Krathwohl, D. (2001). *A Taxonomi for Learning. Teaching, and Assessing: A Revision of Bloom's Taxonomi of Educational Objectives*. New York: Longman.

Arteta, B. M., & Giachetti, R. E. (2004). *A measure of agility as the complexity of the enterprise system*. Paper presented at the Robotics and Computer-Integrated Manufacturing, Toronto, Canada.

Axelsson, S. (2000). The Base-Rate Fallacy and the Difficulty of Intrusion Detection. *ACM Transactions on Information and System Security, 3*(3), 186-205. doi: 10.1145/357830.357849

Bacon, S. J. (1974). Arousal and the range of cue utilization. *Journal of Experimental Psychology, 102*, 81-87.

Baddeley, A. D. (1983). Working Memory. *Philosophical Transaction of the Royal Society of London. Series B, Biological Sciences, 302*(1110), 311-324.

Baker, C. H. (1962). *Man and radar displays*. New York, U.S.: Macmillan.

Ben-Asher, N., & Gonzalez, C. (2015a). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51-61.

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*(0), 51-61. doi: http://dx.doi.org/10.1016/j.chb.2015.01.039

Ben-Asher, N., & Gonzalez, C. (2015b). Training for the unknown: The role of feedback and similarity in detecting zero-days attack. *In Proceedings of 6th Internatinal Conference on Applied Human Factors and Ergonomics (AHFE 2015)*.

Bloom, B. E. (1956). *Taxonomy of educational objectives. Handbook 1: cognitive domain*. New York. US.: McKay Company.

Brehmer, B. (2015). Kurt Lewin *Nationalencyklopedin*: NE.

Broadbent, D. E. (1971). *Decision and stress*. London: Academic Press.

Brogan, D., Gale, A., & Carr, K. (1993). *Visual Search 2*. London: Taylor & Francis.

Bruce, V., Green, P., & Georgeson, M. (1996). *Visual Perception*. Hove, UK: Psychology Press Taylor & Francis group.

Castor, M., Hansson, E., Svensson, E., Nählinder, S., Le Blaye, P., MacLeod, I., . . . Ohlsson, K. (2003). *Handbook of Mental Workload Measurememnt*. Garteur Group for Aeronautical Reserach and Technology in Europe.

Cichonski, P., & Scarfone, K. (2012). *Computer Security Incident Handling Guide Recommendations of the National Institute of Standards and Technology (SP 800-61)*. Gaithersburg, MD, USA.

Clark, H., & Brennan, S. (1991). Grounding in Communication. In L. B. Resnick, J. M. Levine, & S. D. Teasley (Eds.), *Perspectives on Socially-Shared Cognition*. Washington, D.C.: APA.

Colom, R., Martínez-Molina, A., Shih, P. C., & Santacreu, J. (2010). Intelligence, working memory, and multitasking performance. *Intelligence, 38*(6), 543-551. doi: http://dx.doi.org/10.1016/j.intell.2010.08.002

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 49*(3), 229-233. doi: 10.1177/154193120504900304

Deci, E. L., & Ryan, R. M. (1985). *Intrinsic motivation and self-determination in human behaviour*. New York: Plenum.

Dekker, A. H. (2006). Measuring the agility of networked military forces. *Journal of battlefield technology, 9*(1), 1-6.

Donald, F. M. (2008). The classification of vigilance tasks in the real world. *Ergonomics, 51*(11), 1643-1655.

Endsley, M. (1995). Toward a Theory of Situational Awareness in Dynamic Systems. *Human Factors, 37*(1), 32-64.

Endsley, M. (1999). Situation Awareness In Aviation Systems. In D. J. Garland, J. A. Wise, & V. D. Hopkin (Eds.), *Handbook of Aviation Human Factors*. Mahwah: lawrence Erlbaum Associates.

Endsley, M., Holder, L., Leibrecht, B., Garland, D. J., Wampler, R., & Mathews, M. (2000). *Modeling and measuring Siuation awareness in the infantry operational environment* (1753). U.S. Army Research Institute for the Behavioral and Social Sciences.

Endsley, M., & Smolensky, M. W. (1998). Situation awareness in air traffic control: The picture. In M. W. Smolensky & E. S. Stein (Eds.), *Human factors in air traffic control*. San Diego, CA: US: Academic Press.

ENISA. (2015). from https://www.enisa.europa.eu/activities/cert/support/exercise

Fernandez-Duque, D., & Johnson, M. L. (1999). Attention Metaphors: How Metaphors Guide the Cognitive Psychology of Attention. *Cognitive Science, 23*(1), 83-116. doi: 10.1207/s15516709cog2301_4

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security, 46*(0), 18-31. doi: http://dx.doi.org/10.1016/j.cose.2014.06.008

Försvarsmakten. (2006). *Pedagogiska grunder*. Stockholm: Jure AB.

Försvarsmakten. (2012). *Krav på IT-säkerhetsförmågor hos IT-system v3.0*. Sverige: Högkvarterat.

Försvarsmakten. (2013). *Handbok Utbildningsmetodik*. Stockholm, Sweden: FMV, FSV, Grafisk Produktion.

Garris, R., Ahlers, R., & Driskell, J. (2002). Games, motivation, and learning. *Simulation & Gaming, 33*(4), 441-467.

Gestrelius, K. (1998). *Simulering och utbildningsspel*. Malmö, Sweden.: Institutionen för pedagogik och specialmetodik, Lärarhögskolan i Malmö, Lunds Universitet.

Goodall, J., R., Lutters, W., G., & Komplodi, A. (2004). *The Work of Intrusion Detection: Rethinking the Role of Security Analysts*. Paper presented at the Proceedings of the Tenth Americas Conference on Information Systems, New York, US.

Gopher, D., & Donchin, E. (1986). Workload – An examination of the concep. In K. Boff, L. Kaufman, & J. Thomas (Eds.), *Handbook of Perception and Human Performance* (Vol. 2): John Wiley and Sons Inc.

Hammar, P., Bergström, G., Åkerström, J., Thorstensson, M., & Oskarsson, P.-A. (2012). *Spel för träning av soldater* (FOI-R--3540--SE). Stockholm: FOI-R--3540--SE.

Hart, S. G., & Staveland, L. E. (1988). Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. In P. Hancock & N. Meshkati (Eds.), *Human Mental Workload*. Amsterdam: North Holland Press.

HFES, H. F. a. E. S.-. (2015). Definitions of Human Factors and Ergonomics. from http://www.hfes.org/Web/EducationalResources/HFEdefinitionsmain.html

Hockey, G. R. J. (1986). Changes in operator efficiency as a function of environmental stress, fatigue and cicadian rhythms. In K. Boff, L. Kaufman, & J. Thomas (Eds.), *Handbook of perception and performance* (pp. 44/41 - 44/49). New York: John Wiley.

Hoff, K. A., & Bashir, M. (2015). Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 57*(3), 407-434. doi: 10.1177/0018720814547570

Hogg, D. N., Folles, K., Strand-Volden, F., & Torralba, B. (1995). Development of a situation awareness measure to evaluate advanced alarm systems in nuclear power plant control rooms. *Ergonomics, 38*(11), 2394-2413. doi: 10.1080/00140139508925275

Jenvald, J. (1999). *Methods and Tools in Computer-Supported Taskforce Training.* (Dissertation), Linköping University, Linköping, Sweden. (No. 598)

Jian, J.-Y., Bisantz, A. M., Drury, C. G., & Llinas, J. (2000). *Foundations for an empirically determined scale of trust in automated systems*. Dayton, OH, US.: Wright-Patterson Air Force Base.

Kaber, D., & Endsley, M. (1998). Team Situation Awareness for Process Control Safety and Performance. *Process Safety Progress, 17*(1), 43-48.

Kahneman, D. (1973). *Attention and effort*. Englewood, NJ: Prentice Hall.

Klein, G. (2008). Naturalistic decision making. *Human Factors, 50*(3), 456-460.

Kolb, D. A. (1984). *Experiential Learning experience as a source of learning and development*. New Jersey, US.: Prentice Hall.

Krathwohl, D., Bloom, B. E., & Masia, B. (1964). *Taxonomy of educational objectives*. New York, Us.: McKay Company.

König, C. J., & Waller, M. J. (2010). Time for Reflection: A Critical Examination of Polychronicity. *Human Performance, 23*(2), 173-190. doi: 10.1080/08959281003621703

Laktasic, S. (1976). *Achieving Transfer of Learning Through Simulation*. Washington: US Department og Health, education and wellfare. National institute of education.

Lee, J. D., & See, K. A. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 46*(1), 50-80. doi: 10.1518/hfes.46.1.50_30392

Lif, P., & Oskarsson, P.-A. (2012). *Metoder för insamling av objektiva och subjektiva data* (FOI-R--3626--SE). Stockholm, Sverige: FOI - Totalförsvarets Forskningsinstitut.

Lind, J.-I., & Skärvad, P.-H. (1997). *Nya team i organisationernas värld*. Malmö: Liber AB.

Lippmann, R., Haines, J. W., Fried, D. J., Korba, J., & Das, K. (2000). The 1999 DARPA on-line intrusion detection evaluation. *Comput. Networks, 34*.

Mancuso, V. F., Christensen, J. C., Cowley, J., Finomore, V., Gonzalez, C., & Knott, B. (2014). Human Factors in Cyber Warfare II: Emerging Perspectives. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58*(1), 415-418. doi: 10.1177/1541931214581085

Mandler, G. (1979). Thoght process, consciousness and stress. In V. Hamilton & D. M. Warburton (Eds.), *Human stress and cognition: An information-processing approach*. Chichester: Wiley and Sons.

Matthews, G., Reinerman-Jones, L. E., Barber, D. J., & Abich, J. (2015). The Psychometrics of Mental Workload: Multiple Measures Are Sensitive but Divergent. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 57*(1), 125-143. doi: 10.1177/0018720814539505

McHugh, J. (2000). Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory. *ACM Trans. Inf. Syst. Secur, 3*(4), 262-294.

McIntire, L., McKinley, R. A., McIntire, J., Goodyear, C., & Nelson, J. (2013). Eye metrics: An alternative vigilance detector for military operators. *Military Psychology, 25*(5), 502-513. doi: 10.1037/mil0000011

Morin, M. (2002). *Multimedia Representation of Distributed Tactical Operations.* (Dissertation), Linköpings Universitet, Linköping, Sweden. (No. 771)

Morrison, J. E., & Meliza, L. L. (1999). *Foundation of the after action review process*. Alexandria, U.S.: United States Army Research Institute for the Behavioral and Social Sciences.

Morrow, D. G., & Fischer, U. M. (2013). Communication in Socio-Technical Systems. In D. N. Lee & A. Kirlik (Eds.), *The Oxford Handbook of Cognitive Engineering*. Oxford: Oxford University Press.

MSB. (2012). *Handbok – Tekniska informations- och cybersäkerhetsövningar*. Stockholm, Sweden.

Murphy, C. A., Coover, D., & Owen, S. V. (1989). Development and validation of the computer self-efficacy scale. *Educational and Psychological measurement, 49*(4), 893-899.

Nationalencyklopedin. (1995) (Vol. 16, pp. 359).

NATO. (2014). *C2 Agility* (STO Technical report). North Atlantic Treaty Organization.

NICE. (2015). National Cybersecurity Workforce Framework. from http://csrc.nist.gov/nice/framework/

Noel, S., & Jajodia, S. (2008). Optimal IDS sensor placement and alert prioritization using attack graphs. *J. Netw. Syst. Manag, 16*(3), 259-275.

Norman, D. (1988). *The design of everyday things*. New York: Basic Books.

O'Connor, P., Campbell, J., Newon, J., Melton, J., Salas, E., & Wilson, K. (2008). Crew resource management training effectiveness: A meta-analysis and some critical needs. *International Journal of Aviation Psychology, 18*(4), 353-368.

Olson, W. A., & Sarter, N. B. (1998). *"As long as I'm in control...": pilot preferences for and experiences with different approaches to automation management*. Paper presented at the Proceedings Fourth Annual Symposium on Human Interaction with Complex Systems, Dayton, OH.

Orasanu, J., & Connolly, T. (1995). The reinvention of decision making. In G. Klein, J. Orasanu, R. Calderwood, & C. Zsambok (Eds.), *Decision making in action: models and methods*. Norwood, NJ: Ablex.

Oser, R. L., Gualtieri, J. W., Cannon-Bowers, J. A., & Salas, E. (1999). Training team problem solving skills: and event-based approach. *Computers in Human Behavior, 15*, 441-462.

Poposki, E. M., & Oswald, F. L. (2010). The Multitasking Preference Inventory: Toward an Improved Measure of Individual Differences in Polychronicity. *Human Performance, 23*(3), 247-264. doi: 10.1080/08959285.2010.487843

Rankin, W. J., Gentner, F. C., & Crissey, M. J. (1995). After action review and debriefing methods: Technique and technology *In Proceedings of the 17th Interservice / Industry Training Systems and Education Conference* (pp. 252-261). Albuquerque, New Mexico, USA.

Reid, G. B., & Nygren, T. E. (1988). The Subjective workload assessment technique: A scaling procedure for measuring mental workload. In P. Hancock & N. Mehtaki (Eds.), *Human mental workload* (pp. 185-218). Amsterdam: North Holland Press.

Salas, E., Dickinson, T. L., Converse, S. A., & Tannenbaum, S. I. (1992). Toward an understandning of team performance and training. In R. W. Swezey & E. Salas (Eds.), *Teams: Their training and performance*. Norwood, NJ.: Ablex.

Salas, E., Prince, C., Baker, D., & Shrestha, L. (1995). Situation Awareness in Team Performance: Implications for measurment and Training. *Human Factors, 37*(1), 123-136.

Salvucci, D. D., & Taatgen, N. A. (2011). *The Multitasking mind*. New York, U.S.: Oxford University Press.

Sawyer, B. D., Finomore, V. S., Funke, G. J., Mancuso, V. F., Funke, M. E., Matthews, G., & Warm, J. S. (2014). Cyber Vigilance: Effects of Signal Probability and Event Rate. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58*(1), 1771-1775. doi: 10.1177/1541931214581369

Schwartz, D. (1990). *Training for situation awareness*. Houston, TX.: Flight Safety International.

Sheridan, T. B., & Verplank, W. (1978). *Human and Computer Control of Undersea Teleoperators*. Cambridge, MA: Man-Machine Systems Laboratory, Department of Mechanical Engineering, MIT. .

Sommestad, T., & Holm, H. (2015). *Variabler av vikt för förmågan att analysera cybersäkerhetsloggar* (FOI-R--4126—SE). Linköping, Sverige.

Sommestad, T., & Hunstad, A. (2013). Intrusion detection and the role of the system administrator. *Information Management & Computer Security, 21*(1), 30-40. doi: doi:10.1108/09685221311314400

Stanton, N., Salmon, P., Rafferty, L., Walker, G., Baber, C., & Jenkins, D. (2013). *Human Factors Methods*. Surrey, England: Ashgate Publishing Limited.

Su, R., Rantanen, E. M., & Yurcik, W. (2006). *Network intrusion detection cognitive task analysis: textual and visual tool usage and recommendations*. Paper presented at the PROCEEDINGS of the Human Factors and Ergonomics Society 50th Annual meeting, San Fransisco.

Tannenbaum, S. I., & Cerasoli, C. P. (2013). Do Team and Individual Debriefs Enhance Performance? A Meta-Analysis. *Human Factors, 55*(1).

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set, *IEEE Symposium on Computational Intelligence for Security and Defense Applications* (pp. 1-6).

Thompson, R. S., Rantanen, E. M., & Yurcik, W. (2006). Network Intrusion Detection Cognitive Task Analysis: Textual and Visual Tool Usage and Recommendations. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 50*(5), 669-673. doi: 10.1177/154193120605000511

Thompson, R. S., Rantanen, E. M., Yurcik, W., & Bailey, B. P. (2007). Command line or pretty lines?: comparing textual and visual interfaces for intrusion detection *in Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 1205).

Thorstensson, M. (2008). *Using Observers for Model Based Data Collection in Distributed Tactical Operations.* Linköpings universitet, Linköping, Sweden. (No. 1386)

Tosto, M. G., Hanscombe, K. B., Haworth, C. M. A., Davis, O. S. P., Petrill, S. A., Dale, P. S., . . . Kovas, Y. (2014). Why do spatial abilities predict mathematical performance? *Developmental Science, 17*(3), 462-470. doi: 10.1111/desc.12138

Tsang, P., & Wilson, G. F. (1997). Mental workload. In G. Salvendy (Ed.), *Handbook of Human Factors and Ergonomics* (Second edition ed.). New York, U.S.: John Wiley & Sons, Inc.

Weltman, G., Smith, J. E., & Engstrom, G. H. (1971). Perceptual narrowing during simulated pressure-chambre exposure. *Human Factors, 13*, 99-107.

Wickens, C., Hollands, J., Banburry, S., & Parasuraman, R. (2013). *Engineering Psychology and Human Performance*. New York: Pearson Education Inc.

Wickens, C. D., Hutchins, S., Carolan, T., & Cumming, J. (2013). Effectiveness of Part-Task Training and Increasing-Difficulty Training Strategies: A Meta-Analysis Approach. *Human Factors, 55*(2), 461-470.

Wierwille, W. W., & Casali, J. G. (1983). *A validated rating scale for global mental workload measurement applications*. Paper presented at the Proceedings, 27th Annual Meeting of the Human Factors Society, Norfolk, Virginia.

Wikberg, P., Albinsson, P.-A., Andersson, D., Danielsson, T., Holmström, H., Johansson, M., . . . Wulff, M.-E. (2005). *Methodological tools and procedures for experimentation in C2 system development—Concept development and experimentation in theory and practice* (FOI-R--1773--SE). Linköping, Sweden.: Swedish Defence Research Agency.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Spec. Publ., 800*(50).

Winfred, A., Winston, B., Edens, P. S., & Bell, S. T. (2003). Effectiveness of Training in Organizations: A Meta-Analysis of Design and Evaluation Features. *Journal of Applied Psychology, 88*(2), 234-245.

Winther-Jörgensen, M., & Phillips, L. (2000). *Diskursanalys som teori och metod*: Studentlitteratur.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*(0). doi: http://dx.doi.org/10.1016/j.ress.2015.03.018

Zimmerman, C. (2014). *Ten Strategies of a World-Class Cynersecurity Operations Center*. Bedford, MA, U.S.: The Mitre Corporation.

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