Pedagogiska perspektiv på cybersäkerhetsövningar

En motivering samt litteraturöversikt

FREDRIK SÖDERSTRÖM

FOI-R--5575--SE
ISSN 1650-1942 December 2024

Fredrik Söderström

Pedagogiska perspektiv på cybersäkerhetsövningar

En motivering samt litteraturöversikt

Titel	Pedagogiska perspektiv på cybersäkerhetsövningar – En motivering samt litteraturöversikt
Title	Pedagogical perspectives on cyber security exercises - A rationale and literature overview
Rapportnr/Report no	FOI-R--5575--SE
Månad/Month	December/December
Utgivningsår/Year	2024
Antal sidor/Pages	45
ISSN	1650-1942
Uppdragsgivare/Client	Försvarsdepartementet
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	A311022
Godkänd av/Approved by	Emil Hjalmarson
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Sammanfattning

Cybersäkerhetsövningar är ett väl etablerat sätt att öva färdighet och förmåga att hantera hot inom cyberdomänen. Denna typ av övningar genomförs i en kontrollerad, simulerad och realistisk miljö, där deltagarna förväntas utveckla förmåga att hantera olika typer av hot och attacker. Inom forskning och praktik har dock detta område varit mycket tekniskt fokuserat, vilket har resulterat i att deltagarnas kunskapsutveckling och lärande vid övningstillfället tas mer eller mindre för givna. Inom forskning och praktik framförs dock ett tydligt behov av mer gränsöverskridande och holistiska perspektiv på cybersäkerhetsövningar. Framförallt beskrivs ett tydligt behov av att integrera perspektiv på lärande och pedagogik inom området. Utan pedagogiska perspektiv på cybersäkerhetsövningar är det svårt att säkerställa att deltagarna verkligen utvecklar det lärande och den förmåga som eftersträvas. Denna rapport presenterar resultatet av en litteraturöversikt med fokus på pedagogiska perspektiv på cybersäkerhetsövningar. Sammanfattningsvis kan konstateras att detta forskningsområde är tydligt drivet av ökande cybersäkerhetsbehov, är relativt nyetablerat och kräver fortsatt forskning. Nuvarande forskning presenterar flera goda tankar och välmotiverade argument, men tydliga ansatser och metodik där pedagogik är en integrerad del genom övningens livscykel saknas. Pedagogiska perspektiv på cybersäkerhetsövningar är ett delområde i behov av fortsatta studier och kunskapsutveckling. Denna rapport är ett steg mot att motivera och vidareutveckla detta forskningsperspektiv på cybersäkerhetsövningar inom Totalförsvarets forskningsinstitut (FOI).

Nyckelord: cybersäkerhet, cybersäkerhetsövning, lärande, pedagogik

Summary

Cybersecurity exercises are a well-established way of practicing skills and ability to deal with threats in the cyber domain. This type of exercises are carried out in a controlled, simulated and realistic environment, where the participants are expected to develop their ability to deal with different kinds of threats and attacks. However, in practice and research, this area has received primarily a technical focus, resulting in taking the participants' knowledge development and learning, related to the exercise more or less for granted. Within research and practice, there is a clear need for more cross-border and holistic perspectives on cybersecurity exercises. Above all, a clear need to integrate perspectives on learning and pedagogy in the field is described. Without pedagogical perspectives on cybersecurity exercises, ensuring that the participants develop the learning and ability sought is difficult. This report presents the results of a literature overview focusing on pedagogical perspectives on cybersecurity exercises. In summary, this research area is driven by increasing cybersecurity needs, is relatively newly established, and requires further research. Current research presents several good ideas and well-motivated arguments, but approaches and methodologies where pedagogy is a well-integrated part throughout the exercise life cycle is missing. Pedagogical perspectives on cybersecurity exercises is a sub-area needing further studies and knowledge development. This report is a step towards further motivating and developing this research perspective on cybersecurity exercises at the Swedish Defence Research Agency (FOI).

Keywords: cybersecurity, cybersecurity exercise, learning, pedagogy

Innehåll

1 Inledning

Detta kapitel syftar till att presentera en inledande bakgrund och motivering till denna rapport. Kapitlet innehåller även avsnitt kring terminologi, problembild samt syfte och mål. Aktuella avgränsningar och begränsningar presenteras även samt en kortfattad redogörelse av applicerad metod.

1.1 Bakgrund

Föreliggande rapport fokuserar på övningsverksamhet inom cybersäkerhetsdomänen. För närvarande saknas dock en tydlig gemensam och tillräckligt generell definition av begreppet cybersäkerhet (Craigen m.fl., 2014). Följande är ett exempel på en förekommande definition som kan användas som utgångspunkt för denna rapport:

> ”Förebyggande av skada på, skydd av och återställande av datorer, elektroniska kommunikationssystem, elektroniska kommunikationstjänster, trådbunden kommunikation och elektronisk kommunikation, inklusive information som finns däri, för att säkerställa dess tillgänglighet, integritet, autentisering, konfidentialitet och oavvislighet.” (NIST, 2023, egen översättning).

Den skada som åsyftas i detta sammanhang orsakas av olika typer av angrepp och attacker inom cyberdomänen. Skydd mot cyberangrepp är en nationell angelägenhet. Målen för sådana angrepp kan utgöras i form av infrastruktur av samhällskritisk typ (NCSC, 2022a). I takt med att hotbilden ökar och att säkerhetshoten blir alltmer avancerade, ökar även behovet av kompetens inom cybersäkerhetsområdet (Brilingaitė m.fl., 2020). Detta särskilt eftersom cyberattacker kan få konsekvenser långt utanför den digitala domänen. Tänkbara andra typer av skador och negativa konsekvenser till följd av cyberattacker kan till exempel vara fysiska, ekonomiska, psykologiska, sociala samt samhälleliga (Agrafiotis m.fl., 2018). På europanivå beskrivs antalet övningar inom cyberförsvar efter 2012 som ständigt ökande, vilket bekräftar ett växande behov. Detta kan i sin tur sammankopplas med en högre medvetenhet kring cybersäkerhetsaspekter, samt en ökad vikt av övning och träning på nationell och internationell nivå (ENISA, 2015).

Det finns flertalet faktorer som påverkar graden av sårbarhet mot cyberangrepp. Dessa faktorer kan relateras till områden som teknisk infrastruktur, kommunikation, säkerhetsarbete, kravställning samt ökad digitalisering (NCSC, 2022a). Åtgärder för att stärka organisationers säkerhet är ofta av teknisk karaktär, men vikten av människans roll i att etablera, vidmakthålla och utveckla säkerhetsarbete, rutiner och arbetssätt inom en organisation är en kritisk faktor. En nyckelfråga i detta sammanhang blir vilka förberedelser som krävs i organisationer till exempel i fråga om resurser, verktyg, kompetens och system (Dewar, 2018). För att säkerställa den kompetens och förmåga som krävs för om att övervaka, analysera, upptäcka och hantera cyberangrepp krävs aktiv förberedelse och övning i rutiner samt hantering av säkerhetshändelser (NCSC, 2022b). Utbildning, tillsammans med forskning och utveckling ses som viktiga grundläggande medel för att utveckla kunskap och medvetenhet kring säkerhetsaspekter inom samhället (SOU 2015:23). I takt med ökad digitalisering, sammankoppling och automatisering i samhället ökar även antalet sårbarheter som potentiellt kan utnyttjas för att orsaka negativa effekter och skada av olika grad (Nevmerzhitskaya m.fl., 2019). Cybersäkerhet som fenomen kan ses som ett mycket komplext och dynamiskt socioteknisktt system (Rajivan & Gonzalez, 2018). Mot denna bakgrund framgår tydligt att cybersäkerhet som forskningsområde är av en tvärvetenskaplig natur och att alltför begränsade perspektiv riskerar att hindra fortsatt kunskapsutveckling (Craigen m.fl., 2014). Även om den tekniska dimensionen av cybersäkerhet kan tyckas vara central, finns ett tydligt behov av kompletterande forskningsperspektiv för att möta dagens och morgondagens komplexa utmaningar inom området. Beredskap och resiliens kräver att kunskap och kompetens inom cybersäkerhet ständigt utvecklas, vilket i sig skapar behov av realistiska övningar och specifik träning för en vidareutvecklad förmåga att hantera angrepp (Nevmerzhitskaya

m.fl., 2019). För att utveckla denna förmåga behövs relevanta strategier på samtliga nivåer och funktioner i en organisation (Taitto m.fl., 2018). Cybersäkerhet kan sägas handla om organiserandet, resurserna, processerna och strukturerna som krävs för att motverka och hantera cyberangrepp (Craigen m.fl., 2014). Ett enbart tekniskt perspektiv på cybersäkerhet är därmed inte tillräckligt. För att hantera cybersäkerhetshändelser behöver även mänskliga förmågor regelbundet övas och tränas (White m.fl., 2004). Detta kan ses som exempel på behov av mer holistiska ansatser för en utvecklad förståelse för de förmågor och den kompetens som krävs för att tillgodose övningsdeltagarnas behov med hänsyn till relevanta övningsscenarion (Nevmerzhitskaya m.fl., 2019). Inom cybersäkerhet kan övning och träning ses som komplexa lärtillfällen med målet att att utveckla kompetens och expertkunskap huvudsakligen genom olika typer av simuleringar (Karjalainen m.fl., 2019). Totalförsvarets forskningsinstitut (FOI) bedriver sedan tidigare forskning bland annat inom totalförsvarets förmåga att stå emot cyberhot[1]. Föreliggande rapport fokuserar övning inom cybersäkerhet med ett särskilt fokus på hur pedagogiska perspektiv appliceras på sådana övningar.

1.2 Terminologi

Inom cybersäkerhetdomänen saknas en tydligt definierad och konsekvent terminologi (Dewar, 2014). Centrala och vanligt förekommande begrepp inom denna domän är cybersäkerhet och cyberförsvar. Cybersäkerhet kan ses som ett övergripande och inkluderande begrepp som till exempel infattar strategier, ansatser och tekniker inom IT-säkerhet, ICS[2]- och OT[3]-säkerhet samt informationssäkerhet för att minimera sårbarheter, bibehålla systemintegritet och säkerställa korrekt åtkomst (Galinec & Steingartner, 2017). Cyberförsvar syftar å andra sidan på de tekniska mekanismer vars syfte är att skydda, upptäcka och försvara kritisk infrastruktur samt information och tillgångar (Galinec & Steingartner, 2017). Cyberförsvar kan därmed ses som en delmängd av cybersäkerhet. Även om det i denna rapport kommer att finnas beskrivningar av olika typer av övningar som kan ses som tydligt kopplade till cyberförsvar, kommer det övergripande begreppet cybersäkerhet generellt att användas. Detta val kan även ses som ett sätt att öka generaliserbarbeten av detta arbete inom cybersäkerhetsdomänen. Kunskaps- och kompetensutveckling inom cybersäkerhetsdomänen kan på ett övergripande plan delas in i utbildning, träning och övning. I detta sammanhang syftar utbildning till utvecklandet av grundläggande kunskap och förståelse, medan träning relaterar till en vidareutveckling i form av utvecklade färdigheter (Aaltola & Taitto, 2019). Med övningar menas i detta sammanhang planerade evenemang, där en simulerad verklighet presenteras i syfte att utveckla och testa olika specifika förmågor som till exempel att förhindra, upptäcka, mitigera dvs. mildra, besvara och återhämta sig från olika typer av skador och avbrott orsakade av cyberangrepp (Aaltola & Taitto, 2019).

Övning förutsätter grundläggande färdigheter som utvecklas genom träning. Dessa färdigheter är en vidareutveckling, och praktisk tillämpning, av grundläggande kunskap som inhämtats genom utbildning. I likhet med Dewar (2018), kommer denna rapport att primärt använda termen övning, alternativt cybersäkerhetsövning, i betydelsen att relatera till aktiviteter inom cybersäkerhetsdomänen där lärande och självreflektion äger rum. Övning har valts framför begreppet träning eftersom träning som begrepp implicerar en lärandeprocess av mer systematisk och repetitiv karaktär, till exempel kopplat till olika specifika tekniker eller verktyg (Dewar, 2018). En förekommande internationell benämning och förkortning för övningar i cybersäkerhet är Cyber Security Exercises (CSE) (Karjalainen m.fl., 2019, 2020). Det begrepp som fortsättningsvis kommer

[1] FOI - Cybersäkerhet. https://www.foi.se/forskning/informationssakerhet.html (hämtat 2023-09-28)

[2] Industrial Control System (ICS) (Knowles m.fl., 2015)

[3] Operational Technology (OT) (Knowles m.fl., 2015)

användas i denna rapport är cybersäkerhetsövning och i sin förkortade version CS-övning. Detta begrepp kan sägas motsvara CSE i en internationell kontext.

1.3 Problembild

Inom såväl forskning som praktik finns ett tydligt behov av att följa upp och säkerställa resultat och effekter av cybersäkerhetsövningar i form av utvecklad kompetens, kunskap och lärande. Samtidigt beskrivs tydliga utmaningar med att applicera sådana kunskapsbaserade perspektiv inom området. För dessa övningar krävs till exempel en lärandemiljö som är såväl realistisk som tekniskt komplex, för att i sin tur kunna stödja till exempel kollaborativt lärande på expertnivå (Karjalainen m.fl., 2020). Vikten av att dra lärdomar (*lessons learned*) återkommer ofta, det vill säga att aktivt följa upp vad deltagare tar med sig från respektive övningstillfälle. Ett återkommande mönster är emellertid att dessa lärdomar relateras direkt till observation och utvärdering av övningarna i sig (ENISA, 2015) snarare än till deltagarnas kunskapsutveckling under och i anslutning till dessa övningar. Detta bekräftas till exempel av Valassi m.fl. (2021) som konstaterar att utvärderingar av CS-övningars måluppfyllnad verkar sällsynta och att utvärderingsinsatser istället huvudsakligen fokuserar på övningars genomförande. Sådana lärdomar riskerar dock sakna en direkt koppling till, och även relevans för, deltagarnas individuella kunskapsutveckling och lärande. Lärdomarna baseras snarare på deltagarnas upplevda lärande, än på systematiska kontroller av faktiskt lärande i form av utvecklad kunskap och kompetens (Maennel m.fl., 2017). Det konstateras även en avsaknad av tydliga metodologier och rekommenderade arbetssätt för att planera, mäta och genomföra CS-övningar (Vykopal & Barták, 2016).

Utvärdering och uppföljning av resultat och effekter av CS-övningar är av stor vikt. Dels för att bedöma hur deltagarna uppnår definierade lärandemål, samt dels för utveckling av framtida övningar för högre uppfyllelse av lärandemål (Karjalainen m.fl., 2020). Dessa övningar är ofta komplexa sett till sin uppbyggnad, organisation och genomförande (Weiss m.fl., 2016). Denna komplexitet kan främst härledas till att dessa övningar syftar till att åstadkomma den höga grad av realism som krävs för att återskapa de relationer och komplexa beroenden som finns mellan nätverk, system och data i dagens organisationer (Karjalainen m.fl., 2020). Med denna komplexa och flerdimensionella karaktär blir dock CS-övningar mycket utmanande att följa upp med hänsyn till att säkerställa utvecklad kunskap och kompetens (Brilingaitė m.fl., 2020). En konsekvens i detta sammanhang blir att ett tekniskt fokus på dessa typer av övningar oftast blir mer framträdande (Valassi m.fl., 2021) medan aspekter av lärande, kunskap och kompetensutveckling placeras i bakgrunden. I takt med att övningar utvecklas ökar dock även intresset och behovet av att analysera aspekter så som deltagarnas insatser, träningsmetoder, mätning och utvärdering (Henshel m.fl., 2016). Utan att analysera och följa upp dessa aspekter kan resultat och effekter av CS-övningar ur kvalitets- och deltagarperspektiv inte säkerställas. Med ett alltför dominerande fokus på respektive övnings tekniska genomförande finns risken att utföraren applicerar ett alltför ensidigt tekniskt fokuserat övningsperspektiv. Detta till skillnad från mer holistiska perspektiv där övningsverksamheten även skulle kunna relateras till resultat och effekter kopplade till deltagarnas utveckling av kunskap, kompetens och lärande.

Detta ökade behov av utvecklade och nya perspektiv på CS-övningar bekräftas även inom forskningen. Karjalainen m.fl. (2019) beskriver till exempel att övningsdomänen kräver holistiska ansatser för att kunna integrera de olika typer av färdigheter och kompetenser som är relevanta samt för att utveckla en mer grundläggande förståelse för relationer, beroenden och orsakssamband inom cyberdomänen som helhet. Detta innebär även en spegling av cybersäkerhetsområdet som praktisk domän, där forskning pekar på tydliga behov av expanderade perspektiv bortom de traditionella tekniska perspektiven (Da Silva, 2022). Det kan konstateras att det finns ett tydligt formulerat behov av att utveckla kunskap kring hur lärande följs upp och säkerställs inom cybersäkerhetsövningar. Som exempel på behovet av ovan beskrivna holistiska ansatser anges humaniora och

humanvetenskaper som områden med potentiella bidrag. Betydelsen och kunskapen om sådana perspektiv när det kommer till att hantera gränsöverskridande utmaningar inom cybersäkerhetsområdet är dock ännu begränsad inom den aktuella forskningsdomänen (Karjalainen m.fl., 2019). Sammanfattningsvis kan sägas att samhällsrelevansen och vikten av utbildning och kunskapsutveckling inom cyberdomänen generellt, och cybersäkerhet specifikt, ständigt ökar. Detta kan ses som ett resultat av en ständigt ökande samhällsdigitalisering, med mer avancerade cyberhot som konsekvens. Därmed ökar även intresset för, och behovet av, träning och övning inom området. Den ökande tekniska komplexiteten återspeglas även i dessa övningars planering, genomförande och uppföljning. I avsaknad av en tydlig etablerad tradition att systematiskt följa upp kunskapsutveckling och lärandemål, finns ett uttalat behov att identifiera och applicera mer tvärvetenskapliga ansatser för kunskapsutveckling kring hur övningsverksamhetens pedagogiska dimensioner, resultat och effekter kan säkerställas.

1.4 Syfte och mål

Syftet med föreliggande rapport kan sägas vara tvådelat. För det första syftar rapporten till att presentera en bakgrund och motivering till behovet av pedagogiska perspektiv på CS-övningar baserat på ovanstående problembild. För det andra presenteras resultatet av en litteraturöversikt med fokus på cybersäkerhetsövningar generellt, och hur pedagogiska perspektiv appliceras på CS-övningar specifikt. Detta kan ses som ett direkt svar på det ovan beskrivna behovet av fler gränsöverskridande och tvärvetenskapliga ansatser för studier och forskning kring CS-övningar. Rapporten adresserar även ett reellt verksamhetsbehov där ökad kunskap och förståelse för hur dessa övningar kan sammankopplas med olika pedagogiska perspektiv efterfrågas. Denna rapport innebär ett steg i riktningen mot att sammankoppla de två forskningsdomänerna (1) cybersäkerhet och cybersäkerhetsövningar samt (2) forskning inom pedagogik och högre utbildning. Denna rapport är resultatet av en initiering av forskning kring lärande och pedagogiska perspektiv på CS-övningar vid FOI, och bidrar även till efterfrågad forskning inom vetenskap och praktik.

1.5 Avgränsningar och begränsningar

Rapporten utgår ifrån ett utförarperspektiv på CS-övningar och fokuserar säkerställande av måluppfyllnad och kvalitet vid sådana övningar. Aspekter som till exempel berör andra delar av deltagarperspektivet, såsom olika typer av beslutsfattande i taktiska miljöer under pågående övning, berörs inte inom ramarna för detta arbete. Huruvida det fokuserade lärandet i sig bidrar till positiva effekter i form av kunskapsöverföring och förändrade beteenden i deltagarnas ordinarie verksamheter kommer inte att beröras. Rapporten fokuserar på icke-tekniska aspekter av CS-övningar, och därmed redovisas inte heller tekniska lösningar för övningar på detaljnivå. Den litteratur som presenteras i denna rapport är resultatet av en relativt begränsad litteratursökning, och är att beteckna som en översikt. Denna typ av metod skall inte sammanblandas med en strukturerad eller systematisk litteraturstudie. Den litteratur som presenteras skall ses som relevanta exempel på litteratur inom de forskningsområden som presenteras.

1.6 Metod

Den strategi som tillämpades för sökning och identifiering av relevant litteratur kan sägas varit av behovsstyrd och hermeneutisk typ. Hermeneutisk i så mening att en framväxande utvecklad kunskap kring forskningsområdet vidareutvecklade litteratursökningen under arbetets gång. Förståelsen för relevanta forskningsområden och de relevanta utmaningarna vidareutvecklades därmed i iterativ samverkan under processen (Boell & Cecez-Kecmanovic, 2010). En relevant uppsättning sökord i olika kombinationer användes och sökningarna förfinades successivt. De söktjänster som primärt användes för litteratursökningar var en intern söktjänst vid FOI, Scopus samt Google Scholar. Till

skillnad mot en systematisk litteraturstudie (*Systematic Literature Review*) följde litteratursökningen ingen strikt metodik för utsökning, urval och granskning utan genomgången av litteratur var framväxande till sin karaktär. Den genomförda litteraturöversikten gör, som beskrivits ovan, inga anspråk på att vara heltäckande utan har genomförts i syfte att inom rimlig tid sammanställa en hållbar utgångspunkt bestående publicerad forskning inom specificerade områden.

2 Litteraturöversikt

Detta kapitel presenterar resultatet av litteraturöversikten. Kapitlet inleds med en övergripande beskrivning av CS-övningar. Därefter följer exempel på hur olika typer av pedagogiska perspektiv har applicerats i forskning kring CS-övningar och utbildning inom cybersäkerhet. Områden som kommer beskrivas är till exempel pedagogiska principer, mätning och bedömning av lärande, vikten av formulerade lärandemål samt mer specifika pedagogiska perspektiv och ansatser som är relevanta för CS-övningar. Kapitlet avslutas därefter med detaljerade exempel på mätning och bedömning av lärande i en övningskontext.

2.1 Cybersäkerhetsövningar

Att försöka presentera en summerad och övergripande bild över syfte, struktur och process med hänsyn till CS-övningar är en utmanande uppgift. Dels saknas, som tidigare beskrivits, en tydlig konsensus kring förekommande termer och begrepp inom det aktuella området, och dels återfinns en mycket stor variation i perspektiv på denna typ av övningar. Även när det kommer till att beskriva CS-övningars innehåll tycks det saknas gemensamma begrepp och definitioner. Begrepp som simulering, scenario och övning kan till exempel användas med liknande betydelse för att hänvisa till specifika aktiviteter eller delar av aktiviteter under övning (Dewar, 2018). Flera återkommande aspekter framträder dock med hänsyn till hur dessa övningar motiveras och genomförs. Vanligt förekommande övergripande mål och syften för CS-övningar kan delas in i nedanstående kategorier (Dewar, 2018):

1. Identifiering
2. Testning av mekanismer och/eller procedurer
3. Träning
4. Förbättrad kommunikation och samarbete
5. Utveckling av policyer och procedurer

1. Identifiering avser identifierandet av sårbarheter samt bister i procedurer och mekanismer för informationsdelning. *2. Testning* avser utvärdering av etablerade eller nya verktyg, praktiker eller procedurer. *3. Träning* syftar till att erhålla träning med hänsyn till dessa resurser för att säkerställa god beredskap. *4. Förbättrad kommunikation och samarbete* är ett av de viktigaste målen för denna typ av övningar eftersom koordinerad samverkande handling samt fungerande kommunikation är en kritisk förutsättning för fungerande incidenthantering. Behovet av samverkan och kommunikation mellan olika typer av aktörer är tydligt. Den sista kategorin, *5. Utveckling av policyer och procedurer*, beskrivs ofta som åsidosatt, men samtidigt viktig för att motverka luckor eller fördröjningar i existerande policyramverk som annars riskerar att ha negativ påverkan på en organisations incidenthanteringsförmåga (Dewar, 2018). Med hänsyn till typ av övning kan det på ett övergripande plan sägas att det huvudsakligen finns två typer av övningar; simuleringsövningar och diskussionsbaserade övningar (Dewar, 2018). Simuleringsbaserade övningar inom cybersäkerhet betecknas ofta som *Cyber Defense Exercises* (CDX) (Seker & Ozbenli, 2018) medan diskussionsbaserade övningar ofta refereras till som *Table Top Exercises* (TTX) (Brilingaitė m.fl., 2017). Under tekniskt baserade simuleringsbaserade övningar eftersträvas realism, där till exempel olika typer av incidenter och attacker återskapas och övningsdeltagarna har som uppgift att hantera dessa. Medan simuleringar utförs i en teknisk miljö med hjälp av realistiska tekniker och verktyg, har diskussionsbaserade övningar inte samma framträdande tekniska fokus (Dewar, 2018). Simuleringsbaserade övningar kan ses som realistiska men resurskrävande

medan diskussionsbaserade övningar kräver mindre resurser med nackdelen att känslan av realism under övningen kan påverkas negativt (Dewar, 2018).

Sammantaget kan det konstateras att cybersäkerhetsövningar, särskilt av typen CDX, påverkar, och påverkas av, såväl tekniska som mänskliga och organisatoriska perspektiv (Henshel m.fl., 2016). Forskning kring CS-övningars struktur och process, dvs. innefattande delar som planering, design, genomförande och utvärdering, fokuserar ofta övningar av typen simulering. Det förekommer olika typer av sätt att beskriva och kategorisera dessa övningars genomförande, men gemensamt är dock att arbetet på ett övergripande plan innefattar olika steg eller faser med olika inriktning som till exempel *planering*, *genomförande* och *uppföljning*. Andra sätt att beskriva dessa faser är *planering*, *utförande* och *efter träning* (Kick, 2014) eller *planering*, *implementation* och *återkoppling (feedback)* (Karjalainen m.fl., 2019). Som ytterligare ett exempel på hur övningsstrukturen kan beskrivas presenterar Furtună m.fl. (2010) ett mer detaljerat exempel innehållande följande steg:

1. Målformulering
2. Val av ansats
3. Tekniska specifikationer
4. Skapa övningsscenario
5. Etablera regler
6. Välja mätetal
7. Hantera lärdomar

1. Målformulering är ett viktigt första steg som tydligt påverkar det fortsatta arbetet med att utforma övningen. Kortfattat kan mål för denna typ av simuleringsövningar delas in i två kategorier: offensiv säkerhet respektive defensiv säkerhet. Formuleringen av mål påverkar därefter följaktligen nästa steg. *2. Val av ansats* kan utformas med en offensiv respektive defensiv ansats, alternativt med en kombinerad offensiv och defensiv ansats. Vid val av ansats anges även vilka typer av färdigheter och förmågor som deltagna behöver för att genomföra övningen. *3. Tekniska specifikationer* är därefter det steg som syftar till att identifiera och säkerställa de tekniska förutsättningar och resurser som kommer krävas för att genomföra övningen. Detta kan till exempel röra sig om nätverk och infrastruktur samt olika typer av tekniska system. Under steget *4. Skapa övningsscenario,* fylls övningen med kontext och innehåll för att beskriva den realistiska situation som övningsdeltagarna kommer att befinna sig i under övningen. Scenariot utgör en beskrivning av det händelseförlopp eller situation som övningen strävar efter att simulera, samt den logiska följd av händelser som kommer inträffa under övningen. Scenariot bör även innehålla beskrivningen av en bakgrund eller ett narrativ med syfte att fånga övningsdeltagarnas intresse (Furtună m.fl., 2010).

Varje övning behöver även ha tydligt definierade ramar och struktur vilka specificeras under steget *5. Etablera regler*. Dessa regler kan till exempel röra hur det är tänkt att övningen skall genomföras, och hur deltagarna skall organiseras. Reglerna bör även tydliggöra aspekter såsom poängsättning, behörighet för deltagande, juridiska frågor, begränsningar, resurser, tidsåtgång och åtgärder om deltagare bryter mot dessa regler. Notera även att begränsningar kan kopplas till såväl tekniska förutsättningar under simuleringen som vad övningsdeltagarna tillåts göra under övning. *6. Välja mätetal* är en förutsättning för att kunna mäta övningens effektivitet, dvs. hur väl övningens mål har uppfyllts, och valda mått behöver vara tydligt kopplade till formulerade mål. Det sista steget, *7. Hantera lärdomar*, relaterar även till övningars effektivitet. Genom att säkerställa mekanismer för återkoppling och utvärdering skapas möjligheter för utveckling. Det är även viktigt att dessa lärdomar sammanställs och hanteras på ett

transparent sätt så att de kommer både utförare och deltagare tillgodo (Furtună m.fl., 2010).

2.2 Pedagogiska aspekter och principer

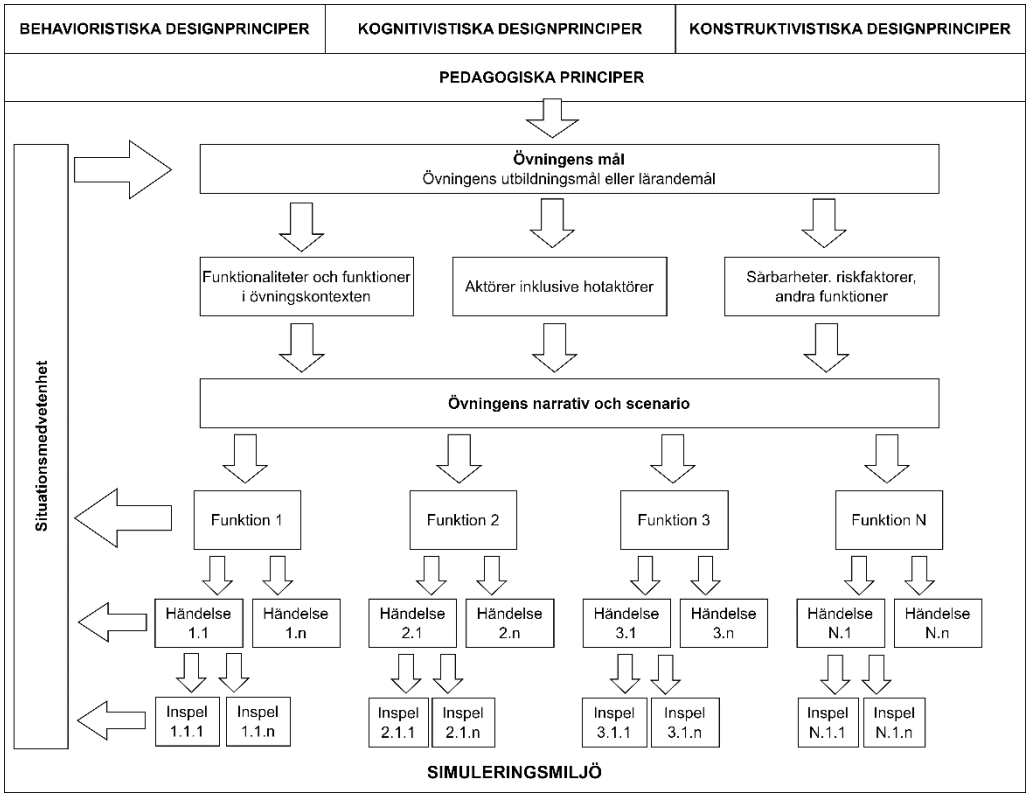
Karjalainen m.fl. (2019) presenterar ett perspektiv baserat på kompetensutveckling under CS-övningens livscykel och argumenterar för ett behov av tydligt identifierade lärandemål (*learning outcomes*). Det finns ett behov av en utvecklad och mer detaljerad förståelse för pedagogiska principer för hur CS-övningar kan användas för att utbilda individer och organisationer inom cyberdomänen. Som en av drivkrafterna bakom detta utbildningsbehov anges behovet av ökad kunskap och förståelse för domänens komplexitet. Som tidigare beskrivits finns inom cyberdomänen behov av mer holistiska ansatser som integrerar såväl specifik kompetens som förståelse för hela landskapet så att relationer och samband som sträcker sig över olika delar av cyberdomänen bättre kan förstås. Det finns behov av forskning med fokus på CS-övningars pedagogiska faktorer för utveckling av kunskap och bättre förståelse kring hur dessa övningar kan nyttjas inom kompetensutveckling inom cybersäkerhet (Karjalainen m.fl., 2019).

Eftersom CS-övningar syftar till att öva, utveckla och bedöma experter behövs kunskap kring hur kompetens och expertis samt expertkunskap fungerar och hur övningar kan användas för att utveckla och förbättra experters förmåga (Karjalainen m.fl., 2019). En koppling görs till forskning inom det medicinska fältet och perspektivet avsiktlig praktik (*deliberate practice*) presenteras som ett sätt att definiera, och på relevanta sätt, öva och utveckla expertkunskap (Ericsson, 2008). Avsiktlig praktik fokuserar på utvecklandet av förmåga kring särskilda uppgifter med centrala inslag som omedelbar återkoppling, tid för problemlösning och utvärdering samt upprepad prestation i syfte att förfina beteende (Ericsson, 2008). Detta perspektiv har sin grund i att expertkunskap eller en överlägsenhet i prestation och utförande ingår i en mer komplex struktur och kan inte enbart kan härledas till ackumulering av erfarenhet och kunskap (Ericsson & Smith, 2011). Karjalainen m.fl. (2019) menar att pedagogiska perspektiv på CS-övningar bör innefatta såväl på *beteendevetenskapliga*, *kognitionsvetenskapliga* samt *konstruktivistiska* principer i sin utformning (se Figur 1 nedan). Med ett ökat fokus på CS-övningars lärandemål motverkas potentiellt traditionen av att se denna typ av övningar som främst tekniska fenomen.

För exempel på olika nivåer av lärandemål anger Karjalainen m.fl. (2019) det Europeiska Kvalifikationsnätverket (European Qualifications Framework, EQF) (European Commission, 2018). Sett till hur de olika faserna i CS-övningars livscykel kopplar till pedagogiska perspektiv utgör planeringsfasen utgör en viktig förutsättning för hur effektiva de senare delarna av en övning kommer att bli. Samtidigt är planeringen av en sådan övning en komplex uppgift där begränsningar i resurser kan påverka. Övningens mål härleds från de pedagogiska principerna och baserat på identifierade lärandemål identifieras relevanta parametrar som integreras i övningskontexten (*övningens narrativ och scenario*). Övningsmålen kommer ligga som grund för definitionen av övningens operativa kontext med hänsyn till funktionalitet, hotaktörer, risker och sårbarheter som kommer att ingå i scenariot och även i den simulering som kommer krävas för övningen. Övningsscenariot kan sedan delas upp i separata händelser och inspel, dvs. simulerade intrång och attacker, som i detalj specificerar de aktiviteter som kommer att simuleras under övningen. Det blir mycket viktigt att kopplingen mellan övningsscenario och de önskade lärandemålen tydliggörs så att varje del och händelse under övningen tydligt kan kopplas till ett specifikt lärandemål (Karjalainen m.fl., 2019). Karjalainen m.fl. (2019) föreslår även att ramverk som National Initiative for Cybersecurity Education (NICE) (NIST, 2020) utnyttjas för att erhålla en standardiserad struktur kring implementationen av lärandemål med hänsyn till övningens interna struktur. NICE-ramverket[4] beskriver

[4] Workforce Framework for Cybersecurity, NICE Framework (NIST, 2020)

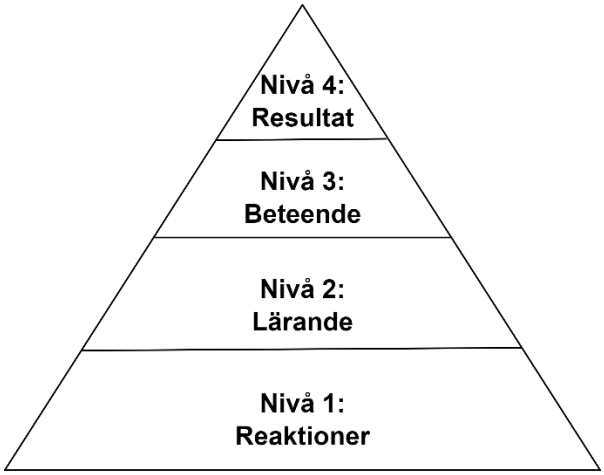
uppgifter, kunskap och färdigheter som behövs för att utföra arbete inom cybersäkerhetsdomänen individuellt samt i team och beskrivs som en referenstaxonomi (NIST, 2020). Under *implementationsfasen* är syftet att genomföra och styra övningen så att samtliga planerade mål för övningen uppnås och för detta krävs ständig medvetenhet om situationen under övningens genomförande. Detta eftersom situationsmedvetenhet (*situational awareness, SA*) är nära sammankopplat med utvecklandet av expertis och expertkunskap (Karjalainen m.fl., 2019). Situationsmedvetenhet kan definieras som uppfattningen av, förståelsen för samt förutsägbarheten kring element i given miljö under given tid (Endsley, 1995). Situationsmedvetenhet blir centralt i flera dimensioner kopplat till en CS-övning och är att beteckna både som mål för övningen, relaterat till expertis och kunskapsutveckling, och som medel för att säkerställa att övningen genomförs på det sätt som planerats (se Figur 1 nedan).



Figur 1. Simuleringsmiljö. Egen figur anpassad efter Karjalainen m.fl. (2019, s. 104, egen översättning)

Situationsmedvetenheten ur ett övningsperspektiv måste inkludera övningsdeltagarnas individuella situationsmedvetenhet som en del av deltagarperspektivet under övning för att säkerställa att övningen genomförs som planerat och att lärandemålen uppfylls (Karjalainen m.fl., 2019). Det är baserat på denna medvetenhet kring deltagarnas egen situationsmedvetenhet som övningsledningen under pågående övning kan göra justeringar för att säkerställa att lärandemålen uppfylls. Ur deltagarnas lärandeperspektiv är återkopplingsfasen mycket viktig (Karjalainen m.fl., 2019). Under denna fas gås övningens samtliga delar och händelser igenom och deltagarna ges möjlighet att ställa frågor. I många fall finns det behov att gå igenom olika händelser och incidenter i detalj samt förklara såväl genomförande som deltagarnas hantering av incidenter. Enligt Karjalainen m.fl. (2019) främjar detta deltagarnas reflektion vilket leder till ökad förståelse och förhoppningsvis uppnådda lärandemål.

Med hänsyn till bedömning av resultat och prestation föreslår Karjalainen m.fl. (2019) att Kirkpatrick-modellens följande fyra nivåer (se Figur 2 nedan) används som utgångspunkt: 1. Reaktioner, 2. Lärande, 3. Beteende samt 4. Resultat (t.ex. Kirkpatrick, 1996). Nivå 1 (Reaktioner) är avsett att mäta hur deltagare känner och upplever olika aspekter av träningen. Viktiga aspekter är här även faktorer som påverkar deltagarens inställning till exempel intresse och motivation. Nivå 2 (Lärande) är avsett att mäta utvecklad kunskap, förbättrade förmågor och förändrade attityder som kan kopplas till träning/övning. Denna nivå är nära sammankopplad med de mål för lärande som formulerats för övningen. Nivå 3 (Beteende) relaterar till i vilken mån deltagarna förändrar sitt beteende i sin normala arbetssituation/yrkesutövning på grund av träningen. Den sista nivån, Nivå 4 (Resultat) är avsedd att mäta de positiva effekterna och resultaten av träning/övning inom deltagarnas organisation/verksamhet (Kirkpatrick, 1996). Denna modell har tillämpats för bedömning av CS-övningar (t.ex. Ahmad m.fl., 2015).



Figur 2. Kirkpatrick-modellen. Egen figur anpassad efter Ahmad m.fl. (2015, s. 4, egen översättning)

Karjalainen m.fl. (2019) beskriver att frågeformulär och enkäter är ett relevant sätt att mäta och bedöma det första steget dvs. deltagarnas reaktioner på övningen. Den andra nivån (lärande) är mer utmanande att bedöma i en CS-övningskontext. Därmed föreslås mer öppna frågeformulär för att om möjligt erhålla mer insikt om deltagarnas lärande som del i bedömningen av om lärandemål uppnåtts. Detta frågeformulär behöver kopplas till de lärandemål som identifierades och formulerades under övningens designfas. Det finns dock utmaningar i att skapa frågeformulär som kan användas som underlag för att bedöma expertinlärning, vilket i sig är ett relevant fokus för fortsatt forskning (Karjalainen m.fl., 2019). Den tredje nivån (beteende) anses som än mer utmanande att hantera. Denna nivå är inte realistisk att försöka mäta och bedöma baserat på en enstaka övning utan deltagaren behöver tid att applicera och tillämpa den nyutvecklade kunskapen i verkliga situationer för att i sin tur över tid resultera i förändrade och utvecklade beteendemönster. Ett sätt att försöka fånga denna nivå av lärande vore att genomföra intervjuer med återkommande deltagare innan nästa övningstillfälle. Den fjärde nivån (resultat) är den svåraste att bedöma vilket kan ses som en effekt av att fokus här flyttas över från övningskontexten till den faktiska verksamhetskontexten där deltagaren är verksam (Karjalainen m.fl., 2019).

Karjalainen och Kokkonen (2020) vidareutvecklar det pedagogiska perspektivet med en kategorisering av pedagogiska principer för CS-övningar. Även om vikten av CS-övningar är brett förankrad, finns tydliga brister i forskning kring pedagogiska aspekter, särskilt relaterat till kompetensutveckling. CS-övningar är ett väl etablerat verktyg för att utveckla förmågan hos professionell cybersäkerhetspersonal samt en operativ miljö för undervisning. Det är viktigt att de behov av utvecklad kompetens och förmåga som finns i praktiken främjas (Karjalainen & Kokkonen, 2020). Praktisk relevans blir ett tydligt krav på CS-övningar. Deltagarna måste möta uppgifter under övning som utvecklar deras förmåga snarare än uppgifter som de kan utföra rutinmässigt. Karjalainen och Kokkonen (2020) hänvisar här till det konstruktivistiska perspektivet på lärande och menar att

deltagarnas utveckling av kompetens möjliggör att ny nivå av kompetens nås genom utvecklade kognitiva förmågor. Kopplat till det konstruktivistiska perspektivet anger de att problembaserat lärande är en relevant pedagogik där deltagarna utvecklar sin kunskap och förmåga genom att lösa problem (Karjalainen & Kokkonen, 2020). En central aspekt av CS-övningar är även att deltagarna oftast arbetar i team vilket i sig även är en återspegling av verkligheten och utvecklar övningsdeltagarnas förmåga och kunskap såväl individuellt som i som team (Karjalainen & Kokkonen, 2020). Som ständigt återkommer i litteraturen ses CS-övning som en komplex entitet bestående av ett antal interagerande och samverkande delar. Denna interaktion äger rum på olika nivåer som med hänsyn till teknisk infrastruktur, aktiviteter, processer samt mänsklig interaktion. Denna interaktion mellan de olika delarna tenderar att vara delvis definierad och delvis odefinierad (Karjalainen & Kokkonen, 2020). I denna senare artikel presenterar Karjalainen och Kokkonen (2020) en mer detaljerad bild bild över hur pedagogiska aspekter skall inkluderas under processens olika delar enligt nedan.

Planering: Under planeringsfasen ska övningens innehåll dvs. scenario, aktörer och händelser stämma överens med målgruppens, dvs. deltagarnas, krav och behov. Baserat på de lärandemål som krävs och den/de organisationer som deltar, härleds övningsparametrar som innefattar scenariots simulerade operativa miljö, teknisk funktionalitet, hotaktörer, risker samt sårbarheter. Scenariot delas därefter in i separata händelser och inspel men ger i sin helhet en översiktsbild över samtliga simulerade aktiviteter. Det är dock mycket viktigt att scenariot i detta steg inte innehåller några oklarheter vilket kan påverka såväl den tekniska miljön som deltagarnas agerande och lärande under övning. De delar som identifierats och formulerats torde stödja att deltagarna når de identifierade lärandemålen. Lärandemål i sig kan formuleras baserat på en önskad utvecklad organisatorisk kompetens eller förmåga likaväl som deltagarnas individuella kompetensutveckling (Karjalainen & Kokkonen, 2020).

Implementation: Under implementationsfasen är situationsmedvetenhet (SA) en central faktor. Denna medvetenhet innefattar såväl övningens operationella dimension som bevakning och utvärdering av övningens pedagogiska mål. Genomförandet av en övning följer scenariot och består av en serie händelser som i sin tur är uppdelade i inspel. Övningsledningen behöver sedan vara medveten om, och bedöma att, övningen genomförs enligt plan och att lärandemålen uppfylls. Vid behov kan övningsledningen behöva guida och leda inriktningen under övningen. Detta kan göras genom inspel eller verbala instruktioner (Karjalainen & Kokkonen, 2020).

Återkoppling: Återkopplingsfasen är viktig när det kommer till att utveckla individers kompetens. Under denna fas sker återkoppling till övningens pedagogiska mål och lärandemål genom relatering till övningens händelser och inspel och hur de hanterats. Deltagaren ges tillfälle att reflektera kring övningsförloppet vilket främjar ett fördjupat lärande. Det är även viktigt att övningens händelser relateras till olika dimensioner av övningsscenariot till exempel med hänsyn till olika hotaktörer och motiv. För denna typ av detaljerad återkoppling är det viktigt att tillräckligt med tid och resurser avsätts. Återkoppling på teamnivå främjar även kollegialt och samverkande lärande (Karjalainen & Kokkonen, 2020).

Bedömning: För bedömning av prestation och resultat föreslås Kirkpatrick's tidigare beskrivna fyrstegsmodell (se Figur 2 ovan) vilket är en användbar modell både med hänsyn till bedömning på såväl organisatorisk nivå som individnivå (Karjalainen & Kokkonen, 2020).

Karjalainen och Kokkonen (2020) beskriver även att övervakning av kommunikation kan användas som ett sätt för att utveckla förståelse för situationsmedvetenhet och deltagarnas beteenden. Baserat på CS-övningars komplexitet rekommenderas formativ bedömning och återkoppling genom övningens samtliga delar. Återkoppling genomförs här i syfte att minska gapet mellan deltagarens existerande kompetensnivå och den kompetensnivå som övningen syftar till att utveckla. Den kompetens som utvecklas gäller såväl övningens ingående delar som relationen mellan dessa delar och miljöns helhet (Karjalainen &

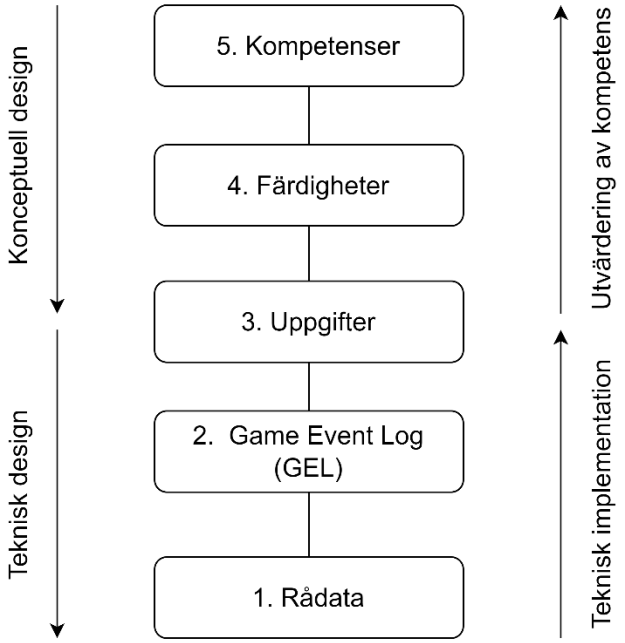
Kokkonen, 2020). Strategier för lärande varierar med hänsyn till deltagarnas förutsättningar. För CS-övningar i professionell kontext relaterar Karjalainen m.fl. (2020) till vuxnas lärande (*adult learning*) och individens egenskaper som självstyrd med förmåga att applicera tidigare kunskap. Utbildning bör introducera en kognitiv dissonans som bryter invanda tankebanor och skapar ett kritiskt-analytiskt förhållningssätt som förutsättning för lärande (Karjalainen m.fl., 2020). Expertkompetens inom cybersäkerhet kräver såväl detaljerad kunskap som förståelse för relationer och konsekvenser inom andra områden, processer och funktioner. Karjalainen m.fl. (2020) relaterar även till erfarenhetsbaserat lärande (*experiential learning*) vilket är ett perspektiv som hävdar att erfarenhet inte är en förutsättning för positivt lärande utan att kognitiva och kommunikativa processer samt reflektion behövs samt kollaborativt lärande (*collaborative learning*) där en grupps samarbete skapar förutsättningar för lärande genom samverkan och samarbete. Det krävs konceptualisering där individen transformerar det omedvetna till konceptualiserad och medveten information. Att kunna beskriva en handling i ord är en förutsättning för att skapa förståelse och utveckla ny kunskap (Karjalainen m.fl., 2020). Kollaborativt lärande är ett pedagogiskt perspektiv och en teori som fokuserar inlärning i grupp. Genom att ansvara för sitt eget lärande delas insikter inom gruppen, samtidigt som gruppen arbetar mot ett gemensamt mål och utvecklar sitt lärande (Laal, 2013). Karjalainen m.fl. (2020) ser tydliga kopplingar mellan CS-övningar och kollaborativt lärande.

2.3 Mäta och bedöma lärande

För kollaborativt och samverkande lärande på expertnivå krävs en tillräckligt realistisk lärandemiljö och som tidigare beskrivits är utvärdering en viktig uppgift både för att bedöma hur deltagare uppnår lärandemål samt hur övningsverksamheten kan förbättras (Karjalainen m.fl., 2020). Karjalainen m.fl. (2020) använder NICE-ramverket (NIST, 2020) som grund för att formulera kunskapskategorier i frågeformulär och enkäter. Ett webbaserat frågeformulär skickades ut till övningsdeltagare för att undersöka kunskaps- och skicklighetsnivå före och efter övning. Baserat på resultatet menar Karjalainen m.fl. (2020) att övning utvecklar kunskapen hos deltagarna inom de kunskapsområden som inkluderas i övningen. Ernits m.fl. (2020) fokuserar mätning av relevant kompetens och hur loggning av tekniska händelser kan relateras till lärandemål och mätning av kompetens genom mellanliggande abstraktionslager. Det ultimata målet är en övningsmiljö som känner av deltagarens nivå av färdighet och skicklighet och automatiskt väljer ut de mest passande uppgifterna för deltagaren. Som ett steg mot att utveckla denna adaptiva förmåga hos en övning behövs sätt att fånga och mäta deltagarens förmåga och Ernits m.fl. (2020) presenterar en metod för automatisk strukturerad återkoppling av deltagarens kompetens och förmåga samt beskriver att forskning adresserar olika aspekter av CS-övningar inklusive kompetensbedömning och utvärdering. Poängsättning ses ofta som ett sätt att ge utvärdering och återkoppling till deltagare, men poängberäkningssystem behöver i sig inte ha någon koppling till lärandemål. Det saknas en praktisk och skalbar modell för att säkerställa att hög kompetensnivå kan erhållas genom analys av de data som insamlas under en övning (Ernits m.fl., 2020).

Under CS-övningar inträffar olika händelser i snabb takt i en semikontrollerad miljö vilket leder till att erfarenheter med hänsyn till lärande varken är förutsägbara eller linjära (Ernits m.fl., 2020). Deltagare kan till exempel hantera och lösa olika typer av händelser på olika sätt som kan anses vara mer eller mindre korrekta, vilket i sig försvårar mätning och bedömning. En övnings design börjar med en konceptuell design där den kompetens som är fokus för övningen definieras. Dessa kompetenser delas därefter in i olika förmågor med relaterade mätbara lärandemål och baserat på dessa lärandemål beslutas om specifika mätbara aktiviteter och uppgifter. Game Event Logs (GEL) designas för att fånga all relevant aktivitet, vilket i sig minskar den datamängd som behövs. Rådata som samlas in under en övning används för att generera GEL och bedöma om uppgifter slutförts. Slutförandet av uppgifter brukar ligga till grund för poängberäkning men insamlad data även kan användas för att indikera kunskapsnivån kopplat till olika förmågor som i sin tur

kan grupperas och kategoriseras som kompetenser (Ernits m.fl., 2020). Denna föreslagna konceptuella övningsmodell visas i Figur 3 nedan. Modellen består av fem olika lager med rådata på lägsta nivån och de kompetenser som fokuseras under övning på den högsta nivån. I denna modell går dataflödet nedifrån och upp men den konceptuella och tekniska designen går uppifrån och ned. Nedan följer en redogörelse för modellens fem lager (kompetenser, färdigheter, uppgifter, Game Event Log samt rådata (Ernits m.fl., 2020).



Figur 3. Föreslagen övningsmodell för CS-övningar. Egen figur anpassad efter Ernits m.fl. (2020, s. 137, egen översättning)

Lager *5. Kompetenser* är den uppsättning av kunskaper, färdigheter och förmågor som i denna kontext främst fokuserar praktiska färdigheter inom fältet cybersäkerhet som kan mätas i praktiska övningar (Ernits m.fl., 2020). Lager *4. Färdigheter* relaterar till underliggande områden inom ett ämne. Det är dock inte oproblematiskt att definiera uppsättningar av färdigheter för olika professioner. Inom cybersäkerhet menar Ernits m.fl. (2020) att färdigheter kan härledas från olika attackvektorer. Färdigheter kan i sin tur definieras på olika nivå där mer detaljerade färdigheter ses som förutsättningar för färdigheter på högre nivå. Att specificera en färdighet på ett sätt som medför mätbarhet är utmanande och det är viktigt att tydlighet eftersträvas i relaterat lärandemål dvs. att den specifika färdigheten kan härledas från lärandemålet på ett tydligt sätt (Ernits m.fl., 2020). Lärandemål är tydligt relaterade till färdigheter eftersom lärandemål för en övning definierar den kunskap och de färdigheter som deltagarna förväntas utveckla under övningen. Kunskap och färdigheter kan analyseras med hjälp av olika modeller som Bloom och Krathwohl (t.ex. Adams, 2015; Anderson & Krathwohl, 2001) samt SOLO (Biggs & Collis, 1982). Lager *3. Uppgifter* avser uppgifter som tydligt kan definieras och mätas. Olika uppgifter bör representera olika kompetensnivåer för relaterade färdigheter (Ernits m.fl., 2020). I lager *2. Game Event Log (GEL)* kvantifieras uppgifter vilket kan göras genom att bevaka systemloggar eller använda poängsättande script. I det nedersta lagret *1. Rådata*, nås bland annat olika enheters status och systemloggar. Genom att använda Game Event Log (GEL) definieras uppgifter som regelbaserade händelser som skall uppnås. Genom GEL kan även nya regler läggas till övningsmodellens högre nivåer vilka definierar kompetenser, färdigheter och uppgifter till existerande händelser under övning. Den föreslagna övningsmodellen bygger på att deltagarnas utförda aktiviteter korreleras med mål baserat på data från händelseloggar (Ernits m.fl., 2020).

Ernits m.fl. (2020) beskriver att övningsmodellen har utvärderats genom att deltagare fått utföra en förhandsbedömning i form av laborationer, ett antal laborationer för att simulera olika incidenter samt efterbedömning i form av laborationer. Baserat på den ovan beskrivna övningsmodellen för bedömning menar Ernits m.fl. (2020) att resultatet av en jämförelse mellan förhands- och efterbedömning visar på tydliga indikationer av förbättring i färdighet och därmed lärande. Den automatiska bedömningen baserad på GEL kompletteras även med en frivillig skriftlig utvärdering efter övning. Vikten av att gå bortom enkel poängsättning under övning framhålls och att den beskrivna metoden för automatiserad återkoppling kring deltagarnas nivå i färdigheter medför att deltagarna själva kan identifiera och bli medveten om sina styrkor och svagheter och få förståelse för eventuella behov av fortsatt lärande (Ernits m.fl., 2020).

2.4 Pedagogik och självreflektion

Karinsalo m.fl. (2022) beskriver användning av en preliminär undersökningsmetodik (*survey*) för att förbättra övningar ur deltagarnas samt utförarnas perspektiv. Genom att inhämta information om deltagarnas färdigheter och intresseområden innan övning kan övningen justeras i enlighet med inkomna svar och övningen som lärtillfälle kan förbättras. Som förankrande bakgrund anger Karinsalo m.fl. (2022) bland annat Bloom's taxonomi, senare reviderade ramverk med hänsyn till pedagogik samt NICE-ramverket kopplat till cybersäkerhet. Därmed beskrivs en enkel modell kring hur frågeformulär kan användas i anslutning till övningar. Trots denna enkelhet presenteras flera intressanta aspekter kopplat till konstruktion och formulering av frågor. De frågor som ställs gäller till exempel utbildningsbakgrund, kunskaps- och färdighetsnivåer, yrkesroll och i vilken sektor deltagaren är verksam inom. Det övergripande syftet med en preliminär undersökning är en datainsamling kring deltagarnas kompetensnivå och inställningar till övning, dvs. preferenser, innan övningstillfället. För frågor där deltagaren ombeds att skatta sin kunskaps-/färdighetsnivå relateras till Blooms taxonomi med hänsyn till följande nivåer av kunskap: (1) Minnas/förstå, (2) Använda/analysera samt (3) Utvärdera/skapa. Dessa skalor används både för att skatta kunskapsnivå som upplevd nivå inom specifik färdighet och förmåga (Karinsalo m.fl., 2022).

Sammantaget beskriver Karinsalo m.fl. (2022) att denna enkätundersökning kan användas för att skapa en bättre förståelse för deltagarna innan övning och ge möjlighet att justera och anpassa övningen baserat på dessa förutsättningar. Med hänsyn till utbildningsbakgrund används nivåer och kategorier angivna i European Qualifications Framework (EQF). För att ange vilken sektor deltagaren är verksam i används den kategorisering som anges i den föreslagna European Cybersecurity Taxonomy (European Commission, 2019). Vidare ger frågor kring nivå i kunskap och färdighet möjlighet att innan övning undersöka hur grupper och team sätts samman. Både att variera nivåerna och att försöka nå en likvärdig nivå inom samma grupp/team kan ha fördelar. Om samtliga deltagare i ett team har låg kunskaps- och färdighetsnivå blir till exempel behovet av stöd tydligt. Om, å andra sidan, nivåerna varierar inom teamet/gruppen kan detta stöd skötas inom teamet/gruppen. Vidare ingår även en fråga där deltagaren skall kategorisera sin yrkesroll baserat på de sektorer som anges i NICE-ramverket (NIST, 2020). I enkäten anger deltagaren även ett till tre kunskapsområden inom vilka hen är mest intresserad av utveckling och förbättring. Svarsalternativen anger olika typer av perspektiv på säkerhet och är hämtade från ramverket Design of Education and Professional Framework (CyberSec4Europe, 2021).

Frågan om vilka kunskapsområden deltagaren är mest intresserad av utgör ett viktigt underlag eftersom det möjliggör justering av övningen för att passa deltagarnas specifika intressen. Eftersom övningen redan kan ha tydligt formulerade mål kan dock denna information till exempel bidra till att vissa delar av övningen får särskilt fokus. Därefter följer ytterligare en fråga som bygger på kategorisering från NICE-ramverket (NIST, 2020). I denna fråga ombeds deltagaren ange inom vilket område/sektor som denne helst önskar utveckla sig inom. Svar på denna fråga kan användas som underlag för att tilldela

deltagare relevanta roller och eventuellt relevanta uppgifter under övningen för att främja lärande inom det område deltagaren är intresserad av. Detta följs av en fråga som innehåller olika alternativ för antalet deltagare per team/grupp och syftet kan ses som att försöka matcha teamens storlek med deltagarnas preferenser angående detta. Gruppens storlek är även en faktor som tydligt påverkar samarbete, kunskapsutbyte och lärande inom gruppen. Enkätens sista frågor rör vilken längd i tid per session som deltagaren anser vara mest lämplig och berör även vilken takt och tempo under övningens olika sessioner som föredras samt vilka (ett till tre) kunskapsområden baserade på NICE-ramverket deltagaren är minst intresserad av. Detta ger därmed ytterligare underlag för för anpassning och justering av övningen. Enkätens allra sista fråga är en fritextfråga som ger deltagaren möjlighet att uttrycka förväntningar och farhågor innan övningen. Detta kan ses som en del i att stärka interaktionen innan övningen med deltagarna. Avslutningsvis framhålls vikten av att enkäten inte får ha en för krävande struktur vilket i sig skulle kunna ha en negativ påverkan på deltagarnas benägenhet att svara på undersökningen innan övning. Enkäten kan även ses som ett sätt att designa frågor för att försöka öka engagemang och motivation hos övningsdeltagarna (Karinsalo m.fl., 2022).

2.5 Lärandemål och bedömning

Forskning kring deltagarnas prestation och resultat inom cybersäkerhet tycks vara begränsad. Ett exempel på sådan forskning är dock Alluhaidan och Abu-Taieh (2020) som presenterar ett förslag att använda lärandemål (*Student Learning Outcomes, SLOs*) som underlag för bedömning av deltagarnas resultat. Forskning kring vilka ansatser som kan anses som effektiva med hänsyn till identifiering av lärandemål och metoder för bedömning verkar dock saknas i nuläget. Denna forskningslucka skulle behöva fyllas för att bistå med effektiva strategier för lärande samt utveckling av kursplaner, träning och övning (Alluhaidan & Abu-Taieh, 2020). Mätning av måluppfyllnad handlar om förmåga att demonstrera en viss typ av lärande och relateras till prestation. Eftersom behovet av utvecklad kunskap och förmåga inom cybersäkerhet ökar, ökar även behovet av väldefinierade och mätbara lärandemål. Standardiserade mått på lärande till exempel i form av lärandemål används i syfte att nå enhetlighet och jämförbarhet med hänsyn till lärande. Andra fördelar och utmaningar kring att formulera liknande mål för lärande varierar mellan ämnesområden. Dessa mål hjälper utvärderare att bedöma deltagares resultat och medverkar till att förbättra den praktik där undervisning och lärande bedrivs. För effektivitet behöver lärandemål vara anpassningsbara och kunna baseras på olika datakällor samt tydligt presentera deltagarens läranderesultat (Alluhaidan & Abu-Taieh, 2020). För att ytterligare motivera lärandemålens betydelser hänvisas till Lachlan-Haché m.fl. (2012) som menar att dessa lärandemål medverkar till att instruktörer och utbildare tydligt fokuserar på mål som är relevanta för den aktuella populationen av deltagare. Genom tydligt definierade lärandemål förbättras även utbildarens kunskap och färdighet genom utvecklad kunskap kring kursplaner, bedömning, undervisningskontext, samt deltagarnas resultat. Utvärderingssystem som bygger på tydligt formulerade mål ger instruktörer och lärare bättre kontroll och ägarskap över prestation samt ökar potentiellt graden av samverkan och erfarenhetsdelning mellan undervisande personal (Alluhaidan & Abu-Taieh, 2020).

De främsta utmaningarna kring att formulera lärandemål är: (1) identifiera bedömningar av hög kvalitet för betygsnivåer och ämnesområden, (2) skapa utvecklingsmål för deltagare som befinner sig på olika prestationsnivå, (3) sätta ambitiösa men samtidigt uppnåeliga mål samt avgöra storleken av varje mål med hänsyn till bredd kontra djup i kunskap och färdighet, (4) hantera konsekvenser av införandet av lärandemål i aktuell undervisningskontext samt (5) en ständig förbättring av processen kring lärandemål (Alluhaidan & Abu-Taieh, 2020; Lachlan-Haché m.fl., 2012). Bedömning kan genomföras genom förhör, examination, presentation, projekt och laborationsuppgifter samt med indirekta metoder som intervjuer eller undersökningar. Varje metod för utvärdering skall vara designad för att kunna mäta och bedöma ett eller flera lärandemål. Avseende CS-övningar är de vanligaste metoderna laborationsbaserade övningar, baserat på

erfarenhetsbaserat lärande, tester samt problembaserade uppgifter, medan undervisning på högre nivå ofta innefattar organiserade scenarion. För att behålla och förbättra relevansen av utbildning och övning inom cybersäkerhet beskrivs även professionella certifieringar inom industrin som en relevant källa (Alluhaidan & Abu-Taieh, 2020; Bell m.fl., 2015). I sitt resultat presenterar Alluhaidan och Abu-Taieh (2020) att antalet lärandemål för varje delområde inte bör överstiga tre till fyra stycken, och att varje lärandemål behöver mätas med hjälp av flera bedömningsmetoder. En utmaning finns även kring hur målen skall mätas på ett heltäckande sätt med hänsyn till olika faktorer som till exempel antal deltagare, deltagarnas nivå och resurser. Ytterligare en utmaning utgör det faktum att vissa deltagare kan vara mer bekväma än andra med vissa sätt att genomföra bedömningar. Vidare framhålls individuell bedömning och individuella uppgifter som mest relevanta för att mäta uppnådd nivå i färdighet (Alluhaidan & Abu-Taieh, 2020). Med tydligare och mer omfattande lärandemål torde det därmed finnas potential för bättre kvalificerade övningar, utbildning och deltagare som kan ses som en del av utvecklingsarbetet inom området CS-övningar (Alluhaidan & Abu-Taieh, 2020).

2.6 Erfarenhetsbaserat lärande

Aaltola och Taitto (2019) fokuserar till viss del beslutsfattande kopplat till CS-övningar men presenterar även flera relevanta aspekter kopplat till pedagogiska perspektiv och lärande. Syftet med utbildning och övning inom cyberdomänen är att höja nivån med hänsyn till expertis, färdigheter och kompetenser för att säkerställa bättre prestation i komplexa cybersituationer. Vidare beskriver Aaltola och Taitto (2019) att forskningen har adresserat begrepp, modeller, antaganden samt kognitiva aspekter av mänsklig prestation inom cyberdomänen men att teorier och ansatser fokuserade på mänskligt lärande i träning och övning bara delvis berörts. Det finns behov av nya tekniker för att förbättra organisatorisk resiliens mot cyberattacker och dessa saknar fortfarande tydligt vetenskaplig grund (Aaltola & Taitto, 2019). Utveckling av diskussioner kring olika relevanta perspektiv på träning och övning inom cyber med särskilt fokus på kompetens och färdigheter förordas och Aaltola och Taitto (2019) önskar bidra till utvecklad förståelse kring beslutsfattande, teoretiska perspektiv på lärande samt utformningen av cyberövningar. Behovet av diskussion kring mänskligt lärande i en cyberövningskontext poängteras och det finns ett ökat behov av tvärvetenskapliga studier för förbättrad medvetenhet inom cyberdomänen. Istället för att enbart fokusera människan i cyberkontexten, har överväganden med syftet att förbättra kapacitet och mänskliga kompetenser medfört en ökande relevans av lärande, utbildning och träning samt övning på en samhällelig nivå (Aaltola & Taitto, 2019).

Som exempel på mer proaktiva ansatser beskriver Aaltola och Taitto (2019) ett ökande intresse bland forskare och praktiker att analysera mänskliga prestationer under övning och träning. En rådande tendens är dock att man inom cyberdomänen huvudsakligen ser utbildning och övning som mekanismer för informationsdelning och därmed avgränsar sig från potentialen hos pedagogiska modeller och lärandeteorier. Ansatser som erfarenhetsbaserat lärande (*experiential learning*) och organisatoriskt lärande, dvs. från konkret erfarenhet och reflektion mot transformerade handlingar och beteenden (t.ex. Kolb & Kolb, 2009), kan därmed potentiellt bidra positivt till förbättrad förmåga och prestation inom cyberområdet. Det behövs andra ställningstaganden kring mänskliga prestationer inom cyberövning och träning. Under cyberövningar tränas personal från olika organisatoriska nivåer i en simulerad lärandemiljö. Denna lärandemiljö är fokuserad på cyberincidenter och är ofta av eskalerande karaktär. Övningar ger möjligheter att analysera, träna och öva avancerade tekniska cybersäkerhetsincidenter, men syftar även till att hantera komplexa situationer med hänsyn till kontinuitet och krishantering inom organisationer. Inom cyberdomänen hanterar människor katastrofer och kriser med många dimensioner och simuleringsövningar har visat sig vara relevanta för att bygga förmåga och förbereda människor på plötsliga risker (Aaltola & Taitto, 2019).

Cyberövningar innefattar ofta lagbaserade tävlingsmoment vilka inkluderar problemlösning, beslutsfattande och analytiska förmågor. Situationsmedvetenhet är även en viktig aspekt av övning som även ses som relevant vid beskrivning, bedömning och förutsägelse av mänsklig prestation i detta sammanhang. För att överväga lärande på ett övergripande sätt, vilket inkluderar kunskapsutveckling, färdighet, kompetens och expertis, kan erfarenhetsbaserat lärande och betydelsen av tyst kunskap bidra i diskussionen kring övning och utbildning inom cybersäkerhet (Aaltola & Taitto, 2019). Erfarenhetsbaserat lärande kan på ett övergripande plan beskrivas som lärande baserat på erfarenhet eller lärande genom att utföra. Detta är en form av aktivt lärande för att främja och utveckla förståelse för denna erfarenhet genom direkt involvering av deltagarna under erfarenhetsbyggande i en relevant kontext (Aaltola & Taitto, 2019). Aaltola och Taitto (2019) hänvisar även till Lewis och Williams (1994) när de beskriver att erfarenhetsbaserat lärande först ger deltagaren erfarenhet för att därefter främja reflektion kring dessa erfarenheter i syfte att utveckla färdigheter, förhållningssätt eller nya tankesätt och kompetenser.

Erfarenhetsbaserat lärande bygger på ett tvärvetenskapligt och konstruktivistiskt perspektiv på lärande. Kognitiva ansatser har blivit ett vanligt sätt inom cyberdomänen att betona utvecklandet av förståelse genom aktivitet och handling. Sociala interaktioner mellan professionella kan utveckla kunskap och främja en utvecklande miljö men det finns även ett bakomliggande antagande att professionella inom cyberdomänen innehar en stor mängd tyst kunskap (Aaltola & Taitto, 2019). Tyst kunskap är enkelt beskrivet kunskap som utvecklas via informella vägar och dimensioner (Howells, 1996). Tyst kunskap är högst personlig och svår att formalisera och därmed utmanande att kommunicera till andra. Denna typ av kunskap är informell och svår att peka ut och fångas ofta inom begreppet kunnande (*know-how*) (Nonaka, 1991). Denna typ av kunskap är att beteckna som personlig kunskap (Ambrosini & Bowman, 2001). Aaltola och Taitto (2019) gör antagandet att professionella och experter inom cyberdomänen innehar en ansenlig mängd tyst kunskap vilken i sig är svår att kommunicera eller förklara. Utmaningarna kring kommunikation riskerar att öka inom cyberdomänen eftersom komplexiteten inom detta fält ökar och ökar även komplexiteten i beroenden, applikationer och tekniker. Detta innebär utmaningar eftersom kommunikation krävs mellan människor på olika nivåer; såväl organisatoriskt som kunskapsmässigt (Aaltola & Taitto, 2019).

För att kunna säkerställa erfarenhetsbaserat lärande måste utbildning, träning och övning kunna simulera verkligheten och det optimala är att förmåga övas både på individuell nivå och på gruppnivå. För att säkerställa lärande i undervisning och övning måste utmaningar kring planering och genomförande hanteras. Lärandemål behöver även formuleras som i sin tur anger inriktning för lärande och bedömning. Lärandemål avsedda att fånga övningsbehoven behöver analyseras och kopplas till olika mått för att bedöma lärande (Aaltola & Taitto, 2019). Målformulering kan ske baserat på akronymen SMART dvs. specifikt (*specific*), mätbart (*measurable*), accepterat (*achievable*), realistiskt (*realistic*) samt tidsbundet (*time-based*). Målen definieras genom en konstruktivt anpassad process där lärandemål definieras genom att använda sig av en mätbar terminologi. Utformning och design av övning och träning behöver även återspegla och återskapa cyberdomänens ständigt utvecklande karaktär som i sig skapar nya förutsättningar och krav. Aaltola och Taitto (2019) beskriver att identifiering och formulering av lärandemål kan ses som själva kärnan i varje design av övning och träning. Övningar som baseras på simulering skall ses som medel för att överföra formulerade lärandemål från övningsverksamhet till praktiken. Designen av mer intelligenta tränings- och övningssystem som till exempel cyber ranges[5] kräver i sig att mänskliga kognitiva processer simuleras för träning inom till exempel beslutsfattande. Cyber ranges ses även som kostnadseffektiva tekniska lösningar för att demonstrera styrkan av erfarenhetsbaserat lärande av färdigheter och kompetens med hjälp

[5] Cyber range är en specialiserad teknisk miljö för forskning och övning inom cybersäkerhet (Gustafsson & Almroth, 2020)

av simulerade scenarion, rollspel, problemlösning och visuella observationer (Aaltola & Taitto, 2019).

Det krävs tvärvetenskapliga ansatser för att bygga förmåga inom krishantering och resiliens men samtidigt skiljer sig cyberdomänen från andra domäner. Cyberdomänen skär i stället rakt igenom samhällets samtliga organisationer och funktioner. Utvecklingen av färdigheter och kompetens inom cyberdomänen skall ses som en konstruktiv process där deltagarens befintliga kunskaper och kompetenser utnyttjas och utvecklas. Enligt Aaltola och Taitto (2019) kan erfarenhetsbaserat lärande utgöra utgångspunkten för ett holistiskt perspektiv på träning och övning. Den kunskap, kompetens och expertis som behövs i en komplex mångfacetterad krismiljö, skapas tillsammans av aktörer över organisatoriska gränser. Därmed betonas vikten av att forskningen arbetar i nära samverkan med praktiken för att studera mänsklig prestation och mänskliga aspekter under cyberövningar baserat på ett lärandeperspektiv (Aaltola & Taitto, 2019).

2.7 Utbildning inom cybersäkerhet

Švábenský m.fl. (2020) beskriver att vikten av utbildning ökar i takt med cyberdomänens utveckling. Domänens mångfald och komplexitet resulterar dock i en stor uppsättning aspekter och koncept som kan läras ut i olika sammanhang och kontexter för lärande. Švábenský m.fl. (2020) presenterar resultatet av en systematisk litteraturstudie av bidrag till två konferenser inom området ACM SIGCSE[6] samt ACM ITiCSE[7] mellan 2010 och 2019. Motivet för att granska bidragen till dessa konferenser var att de sågs som ledande sammanhang inom cybersäkerhetsutbildning. Švábenský m.fl. (2020) genomförde litteraturstudien i syfte att undersöka vad konferensbidrag inom cybersäkerhetsutbildning fokuserar på, samt hur forskningen inom detta fält ser ut. Av totalt 1748 konferensbidrag fokuserade 71 bidrag på utbildning och undervisning inom cybersäkerhet. Švábenský m.fl. (2020) konstaterar att en stor del av dessa bidrag fokuserade på utbildning i USA och att utvärderingar huvudsakligen bestod i insamling av deltagarnas subjektiva uppfattningar via frågeformulär. Mindre än en tredjedel av de bidrag som ingick i litteraturstudien gav bidrag till andra kontexter av utbildning inom cybersäkerhet. Trots att Švábenský m.fl. (2020) kartlägger forskning, publicering och bidrag huvudsakligen inom undervisningsområdet, framkommer samtidigt aspekter som kan vara relevanta i kontexten av CS-övningar. Kopplat till utbildning inom cybersäkerhet ger denna genomgång av konferensbidrag bland annat en överblick över de utvärderingsmetoder som används, implikationer för fortsatt forskning samt praktiska rekommendationer.

Huvuddelen av de konferensbidrag som fanns med i litteraturstudien tillämpade någon form av praktisk tillämpning och övning (51 av 64 bidrag) och hälften av dessa 64 bidrag innefattade arbete i par eller i grupp. För utvärdering användes bland annat subjektiv deltagarbaserat utvärdering samt mätning av deltagarnas prestation genom summativa test. I 40 konferensbidrag samlades data in via frågeformulär vilka oftast fokuserade deltagarnas subjektiva upplevelser. Av dessa tillämpade 26 bidrag enbart frågeformulär efter utbildningstillfället medan 14 använde sig av frågeformulär både inför och efter utbildningstillfället. Testdata, till exempel i form av tilldelade betyg eller antal klarade uppgifter, användes oftast för objektiv mätning av lärande. Av 22 identifierade konferensbidrag använde 10 stycken enbart eftertest och de kvarvarande 12 bidragen en kombination av för- och eftertest[8]. Intervjuer och fokusgrupper användes oftast för att undersöka deltagarnas subjektiva uppfattningar. Följande tre typer av analys av insamlade data kunde identifieras: deskriptiv statistik, inferentiell statistik samt kvalitativ analys. Deskriptiv statistik var vanligt förekommande men detaljgraden varierade tydligt.

[6] Special Interest Group Computer Science Education

[7] Innovation and Technology in Computer Science Education

[8] Förtest (*pretest, pre-test*) används för att kartlägga studentens/deltagarens förkunskaper och eftertest (*posttest, post-test*) genomförs i syfte att säkerställa att studenten/deltagaren har utvecklad önskad kunskap.

Inferentiell statistik bygger på att en hypotes formuleras för att sedan testas med lämpligt statistiskt test där resultaten redovisas som statistiskt säkerställda eller inte. Kvalitativ analys bestod av olika typer av expertintervjuer. Švábenský m.fl. (2020) uppmärksammar även att 15 publikationer inte innehöll någon analysmetod alls. En typisk utvärdering inom området undersöker subjektiva upplevelser och uppfattningar hos deltagare främst genom att använda frågeformulär och i studier som fokuserar att säkerställa lärande används företrädesvis för- och eftertest. För bättre förståelse för deltagarnas lärandeprocesser föreslås *educational data mining*[9] eller *learning analytics*[10] (Švábenský m.fl., 2020).

2.8 Interventionskartläggning

Existerande ramverk som till exempel NIST[11] och ENISA[12] definierar krav på utbildning och övning inom cybersäkerhet men ger inga rekommendationer för hur dessa skall utvecklas. Enligt Pirta-Dreimane m.fl. (2022) behöver utbildning bygga på en teoretisk bas och stödjas av bevis och de föreslår interventionskartläggning (*intervention mapping*) som en relevant metodologi. Denna ansats innefattar intressentperspektiv, identifierade kompetensbehov samt hur lärandemål skall utformas och utvärderas (Pirta-Dreimane m.fl., 2022). Kompetens är därmed centralt och detta begrepp kan beskrivas ur såväl ett internt som externt perspektiv. Ur ett internt perspektiv kan kompetens ses som förutsättningar för till exempel kunskap, färdigheter samt kognitiva faktorer som övertygelse, attityder och beslutsfattande. Som exempel på kompetens som externa förutsättningar anges utbildning, roller samt relationer. De färdigheter som CS-övningar behöver fokusera på innefattar såväl specifika tekniska färdigheter som förståelse för mänskligt beteende och situationsbaserade faktorer. Pirta-Dreimane m.fl. (2022) föreslår ett ramverk för utbildning inom cybersäkerhet som innefattar roller, uppgifter, kompetenser samt önskade beteenden inom det aktuella området. Detta ramverk beskrivs som informerat av NICE-ramverket (NIST, 2017) och rekommendationer kring kompetensbaserat lärande i syfte att integrera tekniska och mänskliga färdigheter ur ett holistiskt perspektiv. Pirta-Dreimane m.fl. (2022) betonar även gränserna i ansvar mellan de olika roller som är relevanta inom cybersäkerhetsdomänen eftersom varje roll har olika krav och olika lärandemål.

Pirta-Dreimane m.fl. (2022) beskriver interventionskartläggning som ett teoretiskt perspektiv som karaktäriseras av följande tre aspekter: (1) en ekologisk ansats, (2) intressenters deltagande samt (3) tillämpning av teorier och bevis. Detta perspektiv har sitt ursprung inom hälsofrämjande initiativ och program men ansatsen har även tillämpats inom andra områden där beteendeförändring studeras som till exempel för att främja energisparande beteenden (Kok m.fl., 2011) och för att främja säkerhetsmedvetenhet (Renaud & Warkentin, 2017). Följande steg för interventionskartläggning med hänsyn till planering av utveckling beskrivs: (1) Bedömning av behov/behovsanalys baserat på *Precede – Proceed* modellen[13], (2) identifiering och definition av resultat och förändringsmål baserat på vetenskaplig grundad problemanalys, (3) användning av teoribaserade metoder för intervention och praktiska tillämpningar för att förändra beteenden, (4) utveckling av komponenter och design, (5) förväntningar kring införande, implementation och hållbarhet samt (6) förväntningar på processen och utvärdering av effekt. Även om stegen presenteras sekventiellt är processen som helhet tydligt iterativ och kumulativ. Den beskrivna processen säkerställer att planeringen vägleds genom att (1) identifiera påverkansfaktorer/determinanter som är relaterade till ett målproblem samt (2)

[9] Educational data mining är datautvinning ur stora datamängder för att identifiera mönster i en utbildningskontext.

[10] Learning analytics innefattar mätning, insamling, analys och rapportering av data baserat på studenter/deltagare i en utbildningskontext.

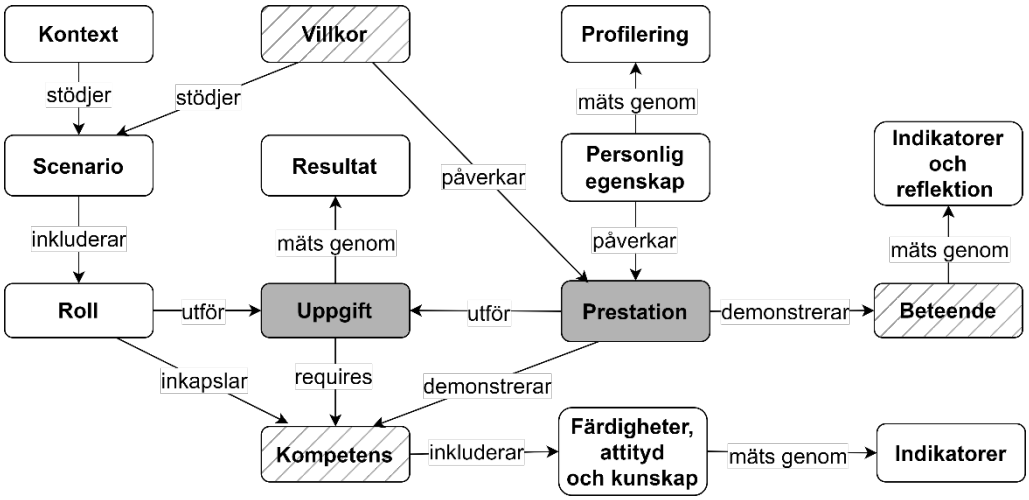
[11] National Institute of Standards and Technology (NIST)

[12] The European Union Agency for Cybersecurity (ENISA)

[13] Ett ramverk med olika faser för att identifiera, utveckla, implementera och utvärdera hälsofrämjande program inklusive systematisk tillämpning av relevanta teorier (Porter, 2016).

val av lämpliga teoretiska metoder och tillämpningar för att adressera identifierade determinanter/faktorer. NICE-ramverket (NIST, 2017) ses som ett sätt att koppla samman utbildning och övningar med industrins förväntningar. Ramverket identifierar relevanta faktorer kopplat till kunskap, färdigheter och förmågor (*Knowledge, Skills, Abilities, KSAs*) som krävs inom olika typer av cybersäkerhetsarbete. I ramverket beskrivs även uppgifter som kan kopplas till en specifik roll eller arbetsområde och denna typ av ramverk kan användas som grund för att formulera lärandemål för utbildning (Pirta-Dreimane m.fl., 2022).

Pirta-Dreimane m.fl. (2022) beskriver att ENISA har identifierat att samhällsvetenskap bör integreras i utbildning inom cybersäkerhet vilket bygger på forskning som visar att mänskliga faktorer kopplat till beteenden så som attityder, motivation och kommunikation måste hanteras under träning och utbildning (ENISA, 2018). Pirta-Dreimane m.fl. (2022) noterar dock att ramverk såsom NICE-ramverket, huvudsakligen fokuserar på tekniska färdigheter och förmågor och konstaterar att detta ramverk saknar de mänskliga och beteendemässiga aspekter som har identifierats som viktiga. Genom att enbart fokusera på specifika färdigheter, som till exempel tekniska eller administrativa, tas ingen hänsyn till mer generella mänskliga färdigheter, som till exempel utvecklar förståelse för hur den sociala miljön relaterar till och påverkar inom cybersäkerhetsområdet. Ansatser som syftar till att förändra beteenden, som till exempel interventionskartläggning, måste även ha en teoretisk grund som inkluderar olika typer av lärande, kognitiva förmågor samt utveckling på meta-kognitiv nivå (Pirta-Dreimane m.fl., 2022). I Figur 4 nedan visas ett exempel på en kompetensmodell för deltagare för kurser inom cybersäkerhet. Denna modell utgör ett ekosystem för utbildningen och tar hänsyn till de krav som finns på kompetens och beteende för att en individ skall kunna fylla en roll och utföra uppgifter på ett specifikt sätt i varje given situation (Pirta-Dreimane m.fl., 2022).



Figur 4. Kompetensmodell för deltagare. Egen figur anpassad efter Pirta-Dreimane m.fl. (2022, s. 6, egen översättning)

Deltagaren genomför uppgifter och demonstrerar ett specifikt beteende och uppgiften bedöms genom resultatets kvalitet. Samtidigt agerar deltagaren i en specifik roll inom scenariot där uppgiften ingår. Därmed krävs olika indikatorer för att bedöma den kompetens som demonstreras och som kopplar till den aktuella rollen. Simuleringens fördefinierade villkor och kontext påverkar och stödjer specifika förutsättningar och omständigheter för deltagaren. Holistiska ansatser behöver innefatta såväl interna som externa determinanter och faktorer där interna faktorer kan kopplas till kunskap, färdigheter och kognitiva faktorer medan externa determinanter består av specifika scenarion, roller och relationer (Pirta-Dreimane m.fl., 2022). Baserat på Fernandez m.fl. (2019) menar Pirta-Dreimane m.fl. (2022) att en applicering av interventionskartläggning

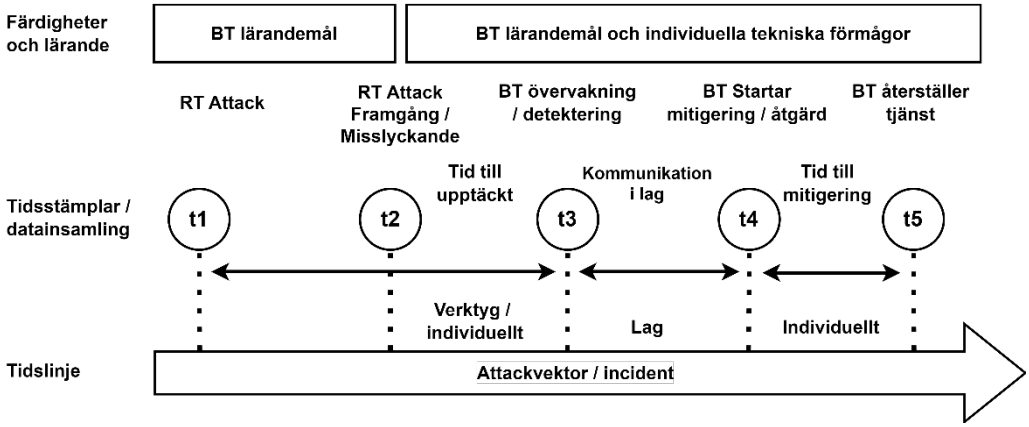
för att utveckla utbildning inom cybersäkerhetsområdet bidrar med praktisk vägledning för effektiv planering och implementation av insatser för utveckling av relevant kompetens, identifiera aktuella behov och nödvändiga beteenden samt bidra till effektiv utvärdering (Pirta-Dreimane m.fl., 2022). Interventionskartläggning är en effektiv ansats för att planera, utveckla, implementera och utvärdera utbildningars mål. De olika föreslagna stegen tillåter deltagande av olika relevanta intressenter och blir evidensbaserade om såväl utförare som deltagare är representerade. Intressenterna blir delaktiga i utvecklingen som i sin tur även tar relevanta ramverk i beaktande för att möjliggöra struktur och utvärdering. Den ansats som presenteras har därmed tre dimensioner där den första dimensionen är det identifierade kompetensområdet vilket inkluderar arbetsroller kopplade till aktuell profession. Den andra dimensionen är implementationen av struktur för kompetensutveckling av respektive roll medan den tredje dimensionen avser lärandemiljön som innehåller verktyg och metoder för deltagarnas kompetensutveckling. Dessa tre dimensioner integreras i undervisning genom interventionskartläggningens olika steg (Pirta-Dreimane m.fl., 2022).

2.9 Exempel på mätning och bedömning

Som tidigare beskrivits råder tydliga utmaningar kring hur man kan säkerställa att övningsdeltagarna uppnår de lärandemål som identifieras och formuleras för övning. Även om utvärdering är ett etablerat steg i processen kring cybersäkerhetsövningar i syfte att förbättra övningar framförs kritik och frågor kring hur lärandemålen kan valideras (Maennel m.fl., 2017). Det finns tydliga exempel på att mål- och resultatformulering huvudsakligen fokuseras under övningens planeringsstadier (t.ex. Kick, 2014) varvid man riskerar att ta mål- och resultatuppfyllelse för givna så länge övningen är utformad i enlighet med dessa mål och resultat. Forskning kring cybersäkerhetsövningars effekter är väl etablerad men fokuserar huvudsakligen på själva utförandet av övningen eller deltagares och deltagande teams prestation i enlighet med övningens målsättning och upplägg (Granåsen & Andersson, 2016; Henshel m.fl., 2016). God effekt definieras som att övningsdeltagarna löser uppgifterna under övningen på det sätt som avses, dvs. att deltagarna följer målen och intentionen med själva övningen. Dessa effekter i form av övningens mer formella och explicit kommunicerade mål är viktiga men samtidigt framförs inom forskningen ett behov av att om möjligt anlägga perspektiv på lärande på dessa övningar. Detta skulle utveckla bättre förståelse och kunskap kring hur dessa övningstillfällen påverkar deltagarnas lärande och kunskapsutveckling. Detta framväxande behov kan ses som en konsekvens av de begränsningar som upplevs kring de mer traditionella sätten att utforma, genomföra och utvärdera resultat av genomförda övningar.

Trots det tydligt identifierade forskningsbehovet finns i nuläget flera relevanta och intressanta exempel på studier som fokuserar på mer strukturerade ansatser i syfte att applicera olika perspektiv på lärande och undersöka effekter av cybersäkerhetsövningar. Ett exempel på sådan studie är Maennel m.fl. (2017) som fokuserar på övningar av typen CDX organiserade med röda lag (*Red Teams, RT*) samt blå lag (*Blue Teams, BT*) och presenterar en metod för att mäta inlärningseffektivitet från den organiserande partens perspektiv. Maennel m.fl. (2017) motiverar sin studie med att denna typ av övningar normalt tenderar att sakna en design och upplägg som möjliggör mätning av lärande och att existerande mätmetoder, till exempel poängsättning, vanligtvis inte kopplas till mätetal som kan relateras till lärande. Även om poängsättning kan ge viss indikation kring deltagarnas progression under övning saknas en tydlig förankring i deltagarnas lärande. Den metod som Maennel m.fl. (2017) istället föreslår är av kvantitativ typ men samtidigt poängteras vikten av att kombinera kvantitativa och kvalitativa metoder för att mäta och följa upp lärande kopplat till övningar. Som exempel på kvantitativ mätning av lärande presenteras en metod kallad *5-Timestamp Methodology* som fokuserar på insamling av data under övning som i sin tur kan relateras till lärandemål (Maennel m.fl., 2017).

Maennel m.fl. (2017) menar att trots att lärande under övningar av typen CDX påverkas av flertalet variabler så kan faktorer som tidtagning samt mätning av noggrannhet och precision ses som nyckelfaktorer för att jämföra lärprocessen hos deltagande team. Detta argument styrks av forskning som visar på relationen mellan tid och korrekt lösning av utmaningar och problem under övning, till exempel att längre tid till upptäckt (*Time-to-Detect, TTD*) tycks ha en positiv korrelation med ökad korrekthet med hänsyn till hantering av incidenter under övning, vilket i sin tur kan sammankopplas med faktorer som ökad noggrannhet (Henshel m.fl., 2016). Maennel m.fl. (2017) föreslår en icke-inkräktande metod, vilken bygger på insamling och analys av tidsstämplar (*timestamps*) baserat på de digitala spår som aktiviteter utförda av röda lag (RT) och blå lag (BT) efterlämnar (se Figur 5 nedan).



Figur 5. 5-timestamp methodology. Egen figur anpassad efter Maennel m.fl. (2017, s. 125, egen översättning)

Analys av tidsintervall mellan definierade tidsstämplar möjliggör mätning av teknisk förmåga och skicklighet samt av mjukare sociala förmågor som relaterade till ledarskap, kommunikation och beslutsfattande. Den föreslagna metoden används för att analysera data på maskinnivå, men bistår potentiellt med mätvärden för att följa upp olika typer av lärandemål (Maennel m.fl., 2017). Vid analys bryts varje incident ned i olika faser för att tydliggöra styrkor och eventuella utmaningar kopplat till individens och lagets förmågor, vilket i sin tur möjliggör en mer detaljerad och effektiv återkoppling (Maennel m.fl., 2017). Metoden följer tidslinjen för varje incident och data samlas in på ett icke-inkräktande sätt från relevanta nätverk (t.ex. *game-net, management-net*). Denna idé bygger på att all datatrafik kan samlas in från relevanta nätverk och att digitala spår i denna trafik kan användas för att detektera aktiviteter från såväl röda lag (RT) som blå lag (BT). Genom att (1) specificera tydliga tidsstämplar (t1-t5) och (2) samla in datatrafik för att spåra aktivitet som kan kopplas till respektive tidsstämpel ger (3) tidsintervallen mellan dessa tidsstämplar grundläggande mätvärden för det aktuella lärandet (Maennel m.fl., 2017).

I detta sammanhang kan även tilläggas att själva loggningen med hänsyn till varje incidents olika faser och tidsstämplar även potentiellt kan anges manuellt. Ett exempel på mätvärden från denna typ av loggning och hur dessa mätvärden kan kopplas till lärandemål visas i Tabell 1 nedan. Maennel m.fl. (2017) beskriver att det finns flera fördelar med den föreslagna metoden (*5-Timestamp Methodology*). Genomgångar efter övningar (*post-exercise debrief*) kan förbättras genom att man har tillgång till övergripande mål för övningen tillsammans med korrekta tidsstämplar. Genom att kunna referera till korrekta tidsintervall ökar meningsfullheten i dessa genomgångar. Vidare kan tidsstämplar användas för att skapa en grund för att mäta prestation eller effektivitet. Detta möjliggör beräkning av medelvärden för olika typer av attacker, jämförelser av upprepade attacker mot samma system samt jämförelse av samma attacker mot olika system

(Maennel m.fl., 2017). Genom att analysera tidsstämplar kan även olika mönster hos deltagande lag analyseras. Det är dock viktigt att notera att det baserat på tidsstämplar enbart går att utläsa hur lång tid det tar för ett lag att lösa utmaningarna dvs. effektiviteteten. Dock kan förändringar i denna effektivitet under själva övningen tyda på förbättringar i prestation vilket Maennel m.fl. (2017) menar skulle kunna tolkas som en indikator på lärande.

Tabell 1. Lärandemål baserade på tidsstämplar och intervall. Egen tabell anpassad efter Maennel m.fl. (2017, s. 127, egen översättning)

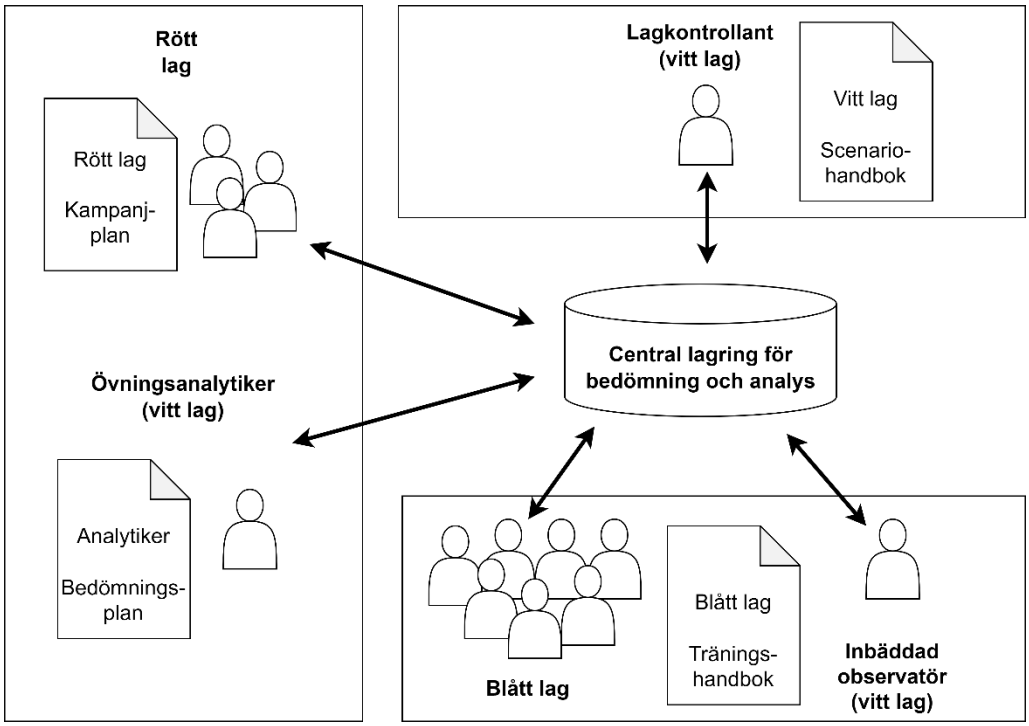
Tidsstämplar intervall	**Beskrivning**	**Lärandemål**	**Lag kontra individuell**
$t_5 - t_2$	Responstid för incident	Övergripande prestation (arrangörens mål=poäng)	Lag
$t_5 - t_4$	Tid till mitigering	Svara på attacker (tekniska förmågor)	Individuell, del av lag
$t_4 - t_3$	Tid mellan mitigering och upptäckt	Tidshantering och prioritering Lagarbete: delegering, dela arbete och tilldela roller, ledarskap Hantera cyberincident	Lag
$t_3 - t_2$	Tid mellan attack/kompromettering och upptäckt	Nätverksövervakning, detektera attacker	Individuell, del av lag
$t_2 - t_1$	Tid till attack/kompromettering	Lära känna nätverket; Systemadministration och förhindra attacker.	Individuell, del av lag

Maennel m.fl. (2017) beskriver samtidigt flera utmaningar och begränsningar med den föreslagna metoden. De mätningar som skall genomföras under övning kräver planering och acceptans hos berörda intressenter och måste även bli en integrerad del av organisering och utvärdering av en övning (Maennel m.fl., 2017). Urvalet av vad som skall mätas ses även som en potentiell utmaning, dvs. vilka mätvärden som har relevans ur ett lärandeperspektiv. Det kan även uppstå problem att mäta tidsåtgång relaterat till lagens aktivitet med hög tillförlitlighet, samt det kan finnas utmaningar med att kombinera och integrera kvantitativa och kvalitativa indata. Vissa mål kan även vara svåra att mäta beroende på hur de hanteras av lagen. De olika lagens agerande kan till exempel styras av olika standarder, procedurer och rutiner vilket leder till att incidenter hanteras på olika sätt av olika lag (Maennel m.fl., 2017).

I nästa exempel på mätning och bedömning presenterar Henshel m.fl. (2016) en strategi för att bedöma de deltagande lagens prestation under övning. På ett övergripande plan beskrivs vikten av att etablera system, procedurer och processer för övervakning och kvantifiering av lagens beteende i syfte att kunna genomföra relevanta analyser (Henshel m.fl., 2016). En övnings design utgår från en övergripande lista av händelser som ingår i övningens scenarier (*Master Scenario Event List, MSEL*) vars syfte är att simulera realistiska scenarier och händelser under en övning. Övningen som exemplifieras organiserades som en traditionell typ av övning där blått lag ställs mot rött lag (*Blue Team – Red Team exercise*) dvs. det röda laget attackerar och det blå laget försvarar. Övningens övergripande målsättning är att utveckla deltagarnas förmåga att identifiera och mitigera, dvs. mildra eller minska konsekvenserna av, cyberhot mot kritisk nationell infrastruktur. I övningen ingår även vitt lag (*White Cell*) som ansvarar för övningsledning och en övningskontrollgrupp (*Exercise Control Group*). Det finns även ett ytterligare utsett lag som ansvarar för övervakning av lagens prestation samt andra bedömningsmått (Henshel

m.fl., 2016). I varje blått lag finns en lagledare (*Team Lead*) och en stridskapten (*Battle Captain)* vilka utses innan övningen startar. Det är lagledarens ansvar att tilldela roller till medlemmarna inom laget och dessa roller kan variera mellan lagen (Henshel m.fl., 2016).

Varje lagledare arbetar även tillsammans med en observatör från det vita laget (*Embedded Observer*) för att bestämma takten för lagets arbete. Stridskapten är den roll som ansvarar för informationsflödet mellan varje blått lag och andra informationskanaler under övningen. Röda lag är inte organiserade enligt någon formell struktur. Det vita laget (*White Cell*) finns representerat i blå lag genom inbäddade observatörer (*Embedded Observer, EO*), i röda lag genom övningsanalytiker (*Training Analyst, TA*) samt i det centrala kontrollrummet genom lagkontrollanten (*Team Controller, TC*). Varje blått lags inbäddade observatör (*EO*) övervakar hur laget interagerar under övning och bidrar även vid genomgång efter övning (*After Action Review, AAR*). Den inbäddade observatören kartlägger även blått lags insatser, tid för att genomföra insatser samt rapporterar kring lagets dynamik efter varje övningspass. På detta sätt skapas underlag för att bedöma lagens process och effektivitet samt utvecklingen inom scenariot dokumenteras. Lagkontrollanten (TC) ingår i övningskontrollen där övningsmiljön övervakas och koordinerar även direkt med röda lags övningsanalytiker (TA) och blå lags inbäddade observatörer (EO). Övningsanalytiker (TA) följer röda lag under övningen och övervakar de händelser som exekveras samt ger daglig återkoppling till röda lag, vilken även inkluderas i genomgång efter övning (AAR) tillsammans med de blå lagens prestation. Bedömningslaget (*Assessment Team*) aggregerar data från övningen till en central lagring för bedömning och analys (*Assessment Data Repository*) (Henshel m.fl., 2016). Denna strategi för bedömning under övning bygger på grundlig insamling och aggregering av data och denna övningsstruktur presenteras översiktligt i Figur 6 nedan.



Figur 6. Övningsstruktur. Egen figur anpassad efter Henshel m.fl. (2016, s. 2, egen översättning)

Som resultat av tillämpningen av ovan presenterad övningsstruktur beskriver Henshel m.fl. (2016) att bedömningen av lagens färdighet och prestation under övningen (*team proficiency data*) innefattade incidentrapporter, efterfrågad information och handlingar, styrkort för incidentspårning (*incident tracking scorecard*) samt observatörers subjektiva expertbedömningar. Fem lag bevakades ytterligare genom loggning av nätverkstrafik och intrångsdetektering (*intrusion detection logs*). Övningens bedömningsplan bestod av en bedömning av expertis och kompetens innan övning (enkät), insamling av data för bedömning under övning samt en enkät som besvarades efter övningen (Henshel m.fl., 2016). Enkäten som genomfördes innan övningen var frivillig och syftade till att kartlägga deltagarnas kompetens och expertis, tidigare träning samt erhållna certifieringar. Datainsamlingen av bevakningen av blå, röda samt det vita laget innefattade lagens agerande samt bedömningar och skedde via följande fyra kanaler:

Bedömningsenkäter (*assessment surveys, scorecards*): Enkäter som fylldes i av inbäddade observatörer (EO), vilka inkluderade starttid för varje inspel, initial tid för detektering, om assistans behövdes (*hints needed*), verktyg som användes, identifierade indikatorer och varningar, tid för incidentrapportering (*incident report submission time*) samt tid för att hantera mitigering (*mitigation action times*).

Chatt-loggar: Loggar från chatt-forum och kanaler som användes av både de blå och vita lagen för snabb kommunikation mellan deltagare. I dessa chattar noterade deltagarna misstänkt aktivitet, diskuterade möjliga sätt för mitigering samt generell strategi. Bedömningslaget (*Assessment team*) utvecklade specifika nyckelord och hashtaggar som användes för att fånga tidssignaler.

Aktivitetsloggar: Röda och blå lags aktivitetsloggar.

Loggar från gemensamt informationsdelningssystem: Tanken var här att använda organisationens etablerade system för registrering, informationsdelning samt begäran om assistans. Detta system bedömdes dock inte passande för rapportering på lagnivå. Datainsamlingen var inte automatiserad utan sammanställdes manuellt (Henshel m.fl., 2016). De utvalda mätetalen för mätning av färdighet och prestation under övning presenteras i Tabell 2 nedan.

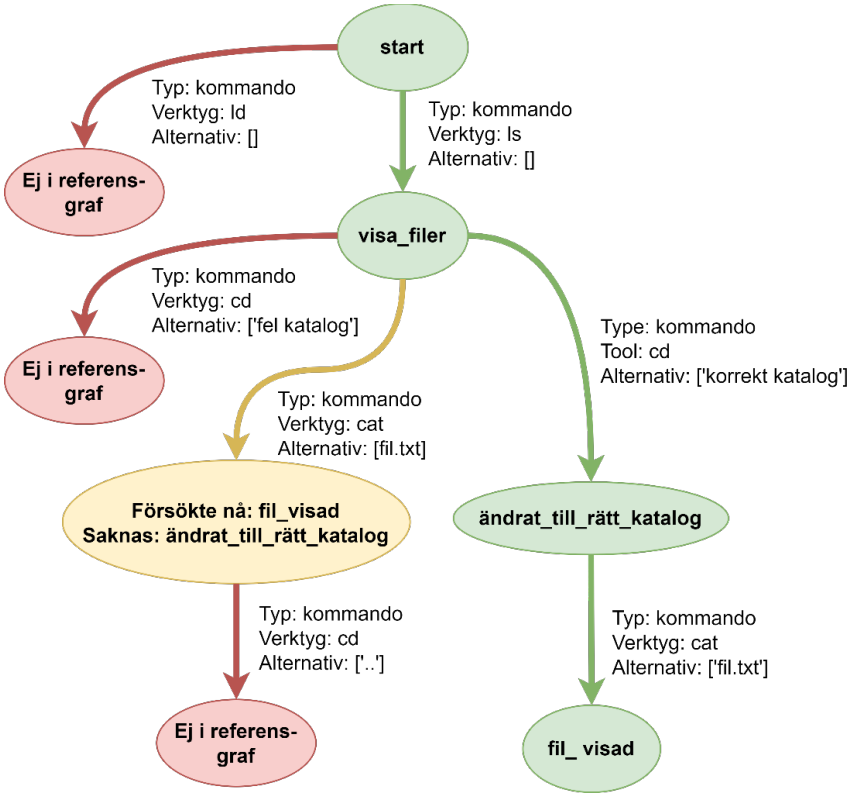
Tabell 2. Mätetal för färdighet och prestation under övning. Egen tabell anpassad efter Henshel m.fl. (2016)

Mätetal/mätsystem (metrics)	**Beskrivning**
Tid till upptäckt (Time-to-Detect, TTD)	Tidsskillnad mellan start av inspel och första validerade rapporterade upptäckt.
Tid till godkännande (Time-to-apProval, TTP)	Tidsskillnad mellan start av inspel och erhållet godkännande av lagets controller.
Tid till avslut (Time-to-End, TTE)	Tidsskillnad mellan start av inspel tills Blått lag lämnar in slutrapport (Close Out Report)
Korrekt kategorisering (Category Correct, CatCorrect)	Graden av korrekt identifiering av Blå lag enligt standardiserad kategorisering (NIST).

Lagens beteende utvärderades vid slutet av varje övningsdag av inbäddad observatör (EO) och dokumenterades i en lagdynamikundersökning (*Team Dynamics Survey*). Denna utvärdering bestod av ett antal frågor inom områdena distribuering av uppgifter, samarbete, kommunikation, diskussion, person-till-person lärande (*peer-to-peer*) samt ledarskap. För att fastställa relationen mellan data insamlad innan, samt under övningen, extraherades och analyserades data som indikerande skicklighet och förmåga ur den centrala lagringen. Datas reliabilitet påverkades dock av hur de olika rapportinstrumenten ifylldes av deltagarna. Trots detta kunde intressanta fynd identifieras; till exempel den positiva korrelationen mellan tid till upptäckt (TTD) och korrekt upptäckt av inspel enligt

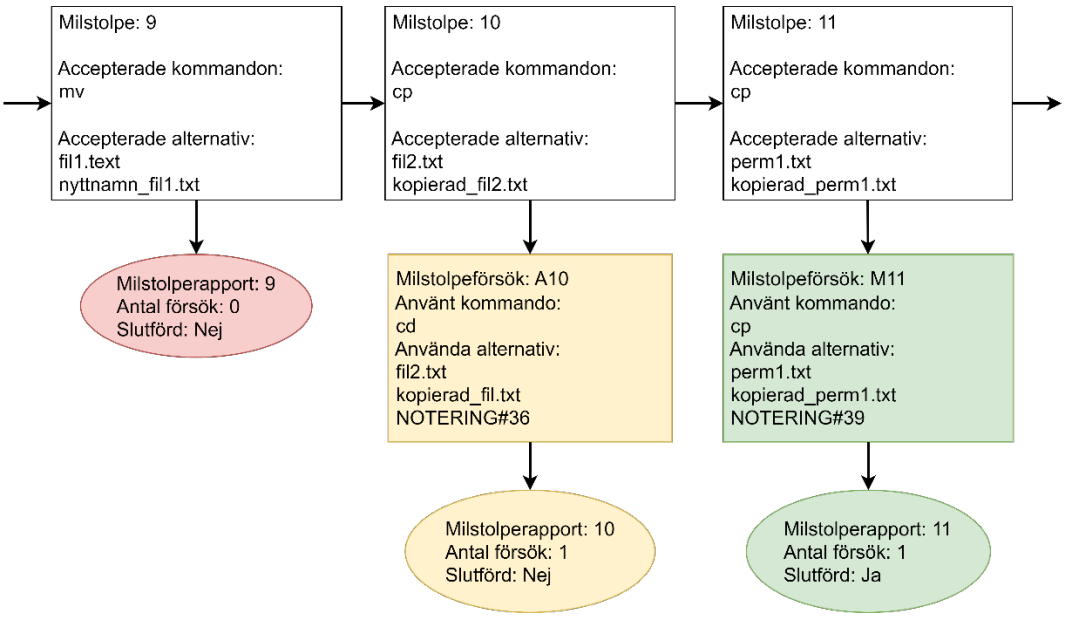
angiven kategorisering, dvs. ju mer noggrant laget arbetade under detektering och identifiering desto högre var sannolikheten att kategoriseringen blev korrekt (Henshel m.fl., 2016). Avslutningsvis konstaterar Henshel m.fl. (2016) att datainsamling under övning måste systematiseras och effektiviseras. Det är även viktigt att försöka eftersträva så hög svarsfrekvens som möjligt på inledande enkäter. Det rekommenderas även att bedömningslaget (*assessment team*) utför så mycket som möjligt av sin analys i realtid under övningen, även om detta kan vara en utmaning sett till planering och resurser. Det finns annars en stor risk att stora datamängder samlas in utan att analyseras. Utmaningen under denna typ av övningar är inte datainsamlingen i sig, utan förmågan att på ett meningsfullt sätt analysera insamlade data. Som lösning föreslås olika typer av automatiserad eller semiautomatiserad datainsamling med mänsklig validering och verktyg för att aggregera data för bedömningsgruppen under pågående övning (Henshel m.fl., 2016).

I det tredje exemplet på mätning och bedömning beskriver Švábenský m.fl. (2022) att löpande bedömning av övningsdeltagares lärande är viktigt men samtidigt utmanande på grund av att denna bedömning ofta görs manuellt och att kvantiteten och komplexiteten är hög i insamlad data, som i sin tur baseras på deltagarnas interaktion under övningen (Švábenský m.fl., 2022). Bedömning på djupet är även att föredra framför en mer ytlig ansats där bedömningen endast anger om ett korrekt resultat har uppnåtts eller inte (Weiss m.fl., 2016). Švábenský m.fl. (2022) presenterar två semiautomatiserade metoder för att modellera och visualisera deltagares framsteg, vilka bygger på de kommandon som används av deltagarna för att lösa uppgifter under övningstillfället. Dessa kommandon presenteras i grafiska modeller som kan användas för att ge ökad förståelse för deltagarnas lärande under övningar, och som underlag för såväl formativ som summativ återkoppling (Švábenský m.fl., 2022). I den första typen av visualiserad graf kallad deltagargraf (*Trainee graph)* skapas först en referensgraf, vilken visar det korrekta sättet att lösa uppgiftens olika delar uppdelat i olika steg och baserat på de kommandon och verktyg som används (grön del av graf i Figur 7 nedan).



Figur 7. Deltagargraf. Egen figur anpassad efter Švábenský m.fl. (2022, s. 789, egen översättning)

Röda delar av deltagargrafen (Figur 7) visar felaktiga eller onödiga kommandon i operativsystemet Linux, medan gula delar visar kommandon som sannolika, men potentiellt saknar korrekta förutsättningar. Syftet med de korrekta (gröna) delarna av grafen är att visa innehåll i en katalog, byta till korrekt katalog samt visa innehåll i korrekt fil. I den andra typen av graf kallad milstolpegraf (*Milestone graph*) bryts varje uppgift ned i delar där varje del representeras av en milstolpe. Uppgiften visualiseras som en kedja av delar, där röd markering anger att försök att lösa aktuell del saknas, gul markering anger att försöket att lösa delen misslyckades samt grön markering anger korrekt genomförd del av uppgiften (se Figur 8 nedan). Vidare anges antal försök per del i milstolpegrafen och delarna är strukturerade efter det förväntade sättet att lösa uppgiftens olika delar (Švábenský m.fl., 2022). Milstolpegrafen syftar till att med hjälp av Linux-kommandon byta namn på en fil (Milstolpe 9) och kopiera filer (Milstolpe 10-11).



Figur 8. Milstolpegraf, egen figur anpassad efter Švábenský m.fl. (2022, s. 789, egen översättning)

När bedömare utvärderade dessa två typer av visualiseringar av deltagares utveckling under övning framkommer att deltagargrafen ger en något annan bild än milstolpegrafen eftersom samtliga försök är synliga i deltagargrafen medan milstolpegrafen endast visar försök som stämmer överens med en milstolpe. Enligt Švábenský m.fl. (2022) kunde graferna användas som underlag vid direkt återkoppling till deltagare. Eftersom deltagargrafen var mer detaljerad så upplevdes den som ett bättre underlag för att utveckla och förbättra prestationen medan milstolpegrafen sågs som det bättre underlaget för att få en överblick över deltagares förmåga och utveckling. Dessa två sätt att visualisera deltagares utveckling och framsteg har potential att identifiera respektive deltagares förmåga, framgångar och utmaningar. De kan även fungera som underlag för formativ och summativ återkoppling samt ge deltagare möjlighet till att själva reflektera kring valda ansatser för att lösa uppgifter under övning och även reflektera kring sin egen lärprocess (Švábenský m.fl., 2022). Utmaningen för denna typ av visualisering är dock övningar och uppgifter som innefattar sekvenser av ett mycket stort antal kommandon. Det finns därmed en risk att deltagare skulle kunna lösa uppgifter utan att dessa klassas som korrekta, eftersom lösningen inte genomfördes på förväntat sätt. Ytterligare en begränsning är att denna metod baseras på kommandoradsbaserade verktyg och gränssnitt (Švábenský m.fl., 2022).

Granåsen och Andersson (2016) redovisar en studie där de valde att fokusera på lagens prestation och effektivitet baserat på en tvärvetenskaplig ansats där tekniker för bedömning av lagens beteenden kombineras med en mer traditionell uppgiftsbaserad bedömning. Därmed utvärderades olika metoder för bedömning av lagens prestation under övning, som till exempel automatisk tillgänglighetskontroll, explorativ sekventiell dataanalys samt intrångsdetektering. Som kompletterande datakällor användes observatörsrapporter och enkäter för att utveckla förståelse kring lagens strukturer och processer kan påverka skillnad i effektivitet hos lagen. Övningen som studerades var organiserad genom fyra olika lag där blått lag försvarade, rött lag attackerade, vitt lag kontrollerade och poängsatte medan grönt lag ansvarade för den tekniska miljön. Den sammanställda datamängden för analys innehöll dataloggar, observationer samt subjektiva självskattningar av till exempel lagets prestation, aspekter kopplat till lagets kognition, interaktion inom laget, lagets sammansättning och organisering samt strategier. Granåsen och Andersson (2016) beskriver i sin övergripande slutsats av studien att bedömning av lags effektivitet under övning kräver såväl teknisk effektmätning som tekniker för bedömning av lagens beteende. Situationsmedvetenhet beskrivs som centralt under övning, och är av mycket stor vikt för såväl deltagande lag, observatörer samt övningsledning. Eftersom denna typ av övning äger rum i såväl den fysiska som den virtuella samt digitala domänen, måste observatörerna vara medvetna om lagens aktiviteter i samtliga av dessa domäner samt ha kompetens inom både cybersäkerhet och lagkognition. Det är viktigt att observatörer under övning får stöd av både metod, teknik och verktyg för att utveckla den medvetenhet som krävs för att utföra sina uppgifter (Granåsen & Andersson, 2016).

3 Diskussion

Nedan följer en diskussion kring relevanta utvalda aspekter och teman som identifierats i litteraturen. Baserat på presenterad litteraturöversikt har diskussionen indelats i följande tre teman: (1) Kontextuella och situationella faktorer, (2) Behovet av mätning och bedömning samt (3) Pedagogiska perspektivens potential.

3.1 Kontextuella och situationella faktorer

Som beskrivits är simuleringsövningar (CDX) en vanligt förekommande typ av CS-övning. Ofta strävar denna typ av övning efter att simulera incidenthantering i en realistisk miljö. Tekniken får därmed en framträdande roll både vad gäller övningens kontext samt vad gäller de tekniska färdigheter som krävs för att lösa uppgifter (Dewar, 2018). Ett övningsscenario beskriver den situation eller händelseförlopp inom vilken övningen utspelar sig (Furtună m.fl., 2010) och scenariot bidrar med en tydlig kontext och ett sammanhang för övningen, som i sig innehar en hög grad av komplexitet. Inte desto mindre syftar även scenariot till att skapa intresse och verka motiverande för deltagarna genom sitt upplägg och narrativ. CS-övningar har därmed ett tydligt värde, både för en professionell och för en akademisk kontext. Inom utbildning ger denna typ av övning studenterna möjlighet att verka i en verklighetstrogen operativ miljö för utveckling av praktisk tillämpad kunskap och färdighet. Det akademiska perspektivet, dvs. forskning kring CS-övningar inom utbildning, är ett område som tydligt influerar det pedagogiska perspektivet på CS-övningar generellt och har inkluderats i litteraturöversikten.

Eftersom förutsättningar och sammanhang tydligt skiljer sig mellan den professionella och akademiska kontexten är det dock viktigt att vara medveten om likheter, men framförallt skillnader mellan dessa övningskontexter. Ett tydligt sådant exempel är deltagarnas förutsättningar och förkunskaper, där man inom akademin potentiellt har en avsevärt bättre vetskap om studenternas kunskapsmässiga förutsättningar jämfört med om deltagarna är yrkesverksamma. Därmed påverkas överförbarhet och generaliserbarhet av forskningsresultat, dvs. resultat av forskning på CS-övningar i en akademisk utbildningskontext kan inte med automatik sägas vara direkt tillämpbara i en professionell kontext. Skillnader i kontextuella förutsättningar för CS-övningar, skapar även skillnader i situationella faktorer under själva övningen. Detta poängteras även, men det tycks finnas tendenser att forskningen rör sig relativt sömlöst mellan professionell och akademisk övningskontext. Denna skillnad i kontexter bekräftas och tydliggörs till exempel av Karjalainen m.fl. (2019) som beskriver det professionella perspektivet på CS-övningars syfte som att öva, utveckla och bedöma expertkunskap, vilket i sin tur ställer krav på forskningskompetens inom relevanta områden kopplat till expertis och kompetensutveckling.

Komplexiteten återkommer i flera dimensioner och kontexter kopplat till CS-övningar. Till exempel beskrivs att dessa övningars syfte är att utveckla deltagarnas kunskap och förståelse kring cybersäkerhetsområdets komplexitet (Karjalainen m.fl., 2019). Medvetenhet om den rådande situationen fångas i begreppet situationsmedvetenhet (*Situational Awareness, SA*) som återkommer i flera sammanhang kring CS-övningar. Som tidigare beskrivits kopplar situationsmedvetenhet till uppfattning, förståelse samt förutsägbarhet i en given miljö (Endsley, 1995). I en CS-övning relateras situationsmedvetenhet därmed till aktuella intressenters uppfattning och förståelse för övningens aktuella scenario och dessa aktiviteter, och blir en viktig förutsättning för att kunna agera i enlighet med övningens mål och intention. Situationsmedvetenheten om deltagarnas individuella situationsmedvetenhet, till exempel övningsledningens och observatörernas förståelse för deltagarnas medvetenhet, blir därmed en viktig faktor att bevaka och eventuellt agera utifrån, ur ett utförarperspektiv under pågående övning. Situationsmedvetenheten blir för deltagare både ett mål och ett medel för övningen och för utförare ett medel för att säkerställa övningens syfte och mål (Karjalainen m.fl., 2019). Situationsmedvetenhet som en viktig aspekt att bevaka under pågående övning återspeglas

även i presenterad forskning kring mätning och bedömning. Till exempel beskriver Henshel m.fl. (2016) en relativt komplex struktur där flera typer av observatörer i olika positioner bevakar olika delar av övningen. Sett till de olika aspekter som dessa observatörer bevakar torde olika slags situationsmedvetenhet vara en viktig faktor i sammanhanget. Det kan konstateras att även om situationsmedvetenhet i flera dimensioner är en viktig aspekt av CS-övningar krävs det resurser och kompetens för att skapa, bibehålla och som utförare av övning, agera baserat på en god förståelse för deltagarnas egen situationsmedvetenhet under pågående övning.

Något som även tydligt kopplar till deltagarnas situationsmedvetenhet under övning är återkoppling till deltagare. För att på ett positivt och bidragande sätt kunna handleda och återkoppla till deltagare krävs förståelse för hur dessa deltagare valde att agera i en given situation under övningen, och detta agerande relaterar i sin tur till deltagarnas situationsmedvetenhet, dvs. uppfattning och förståelse för den givna situationen. Återkoppling som ett sätt att återföra deltagares prestation och resultat under en övning är en viktig del av CS-övningar (Karjalainen m.fl., 2019). Denna återföring främjar deltagares reflektion och förståelse, vilket därmed har en positiv påverkan uppfyllandet av lärandemål. Vid vid återkoppling kan till exempel övningens händelser och deltagarnas agerande i detalj diskuteras vilket i sin tur tydliggör och ökar förståelsen för såväl deltagarnas agerande som deras situationsmedvetenhet. Något som inte tydligt lyfts fram i den forskning som presenterats men som samtidigt är av stor vikt är relationen mellan deltagarnas situationsmedvetenhet under övning och utförarens bedömning av deras prestation. Situationsmedvetenheten, både på individ- och gruppnivå, inom de olika lagen, torde vara en faktor som har en tydlig påverkan på vad och hur deltagare och lag agerar, dvs. hur de olika incidenter som ingår i övningsscenariot uppfattas, prioriteras och hanteras. Därmed, eftersom situationsmedvetenhet är en subjektiv upplevelse hos varje deltagare torde det vara svårt att kvantifiera och instrumentellt mäta denna aspekt. Detta talar i sig för strategier för bedömning, där såväl objektiv som subjektiv bedömning och mätning ingår, vilket även bekräftas av t.ex. Henshel m.fl. (2016). Det är även viktigt att CS-övningar fyller de behov av förmåge- och kompetensutveckling som finns i den praktiska kontexten (Karjalainen & Kokkonen, 2020). För detta krävs såväl praktisk relevans som upplägg och uppgifter som verkligen utvecklar deltagarnas förmåga.

3.2 Behovet av mätning och bedömning

Traditionellt används ofta enkel poängsättning som ett sätt att mäta prestation och effektivitet under CS-övningar. Poängsättning i sig behöver dock inte ha någon koppling till lärande och lärandemål (Ernits m.fl., 2020). Även om tilldelning av poäng baserat på prestation är tydligt och kommunicerbart, riskerar tävlingsmomentet att förstärkas och perspektiv på lärande att hamna i bakgrund. Som beskrivits finns olika presenterade modeller och strategier för mätning som grund för bedömning av deltagare under CS-övningar. Det beskrivs till exempel som att korrekt identifierade mätmetoder och mått är förutsättningar för att kunna mäta en övnings effektivitet och måluppfyllnad (Furtună m.fl., 2010). Samtidigt ligger utmaningen i vad som är att beteckna som ett korrekt mått i detta sammanhang. Begreppen mått och mätetal implicerar även en mätbarhet, och det framgår tydligt från de exempel kring mätning och bedömning, att i kontexten av CS-övningar föreslås ofta mätning som är kvantitativ och möjlig att använda som underlag för objektiv bedömning. Ett tydligt exempel är den tidigare presenterade ”5-Timestamp Methodology” som bygger på mätning baserat på en given tidslinje (Maennel m.fl., 2017). Även om en teknisk lösning för insamling av mätetal som underlag för kvantitativ mätning är såväl relevant som realistisk, kvarstår tydliga utmaningar kring till exempel hur dessa mätetal relateras till bedömningen av deltagarens lärande.

I de exempel som presenteras av till exempel Maennel m.fl. (2017) och Švábenský m.fl. (2022) framgår tydligt att mätning och bedömning utgår ifrån en tydligt definierad korrekt lösning av varje uppgift. För att denna bedömningsmodell skall fungera krävs att deltagare löser uppgifter som förväntat, dvs. det finns en tydligt definierad lösning som anses vara korrekt. Inom cyberdomänen torde dock inte detta vara en självklarhet. Det kan finnas flera olika strategier och sätt att hantera och lösa en uppgift på, till exempel för att hantera en incident, särskilt i en professionell övningskontext. Detta innebär en utmaning för bedömningsmodeller som utgår ifrån tydligt korrekta svar och definierade sätt att lösa uppgifter. Detta bekräftas även av Ernits m.fl. (2020) som beskriver lärandet under CS-övningar som icke-linjärt och svårt att förutsäga. Vilken typ av aktiviteter som förekommit under respektive tidsperiod, kan dock till exempel användas för att identifiera återkommande mönster med hänsyn till hur uppgifter och incidenter hanteras av deltagare och lag, samt möjliggöra jämförelser vid upprepade attacker av samma typ (Maennel m.fl., 2017). Tidsstämpelbaserade mätningar kan även bidra med värdefulla tidsbaserade faktorer i en modell där andra typer av bedömningar ingår.

Om utgångspunkten är en lösning för teknisk mätning av deltagarnas aktivitet under övning, uppstår även utmaningar när denna tekniska nivå för mätning skall relateras till bedömningsnivåer för kompetens och lärande. Ernits m.fl. (2020) beskriver denna utmaning som formulerandet av färdigheter, som möjliggör mätbarhet såväl som härledning till lärandemål. Denna utmaning är i sig inte konstig, eftersom det är i detta skede som gränsen mellan de tekniska och pedagogiska dimensionerna överbryggas. Eftersom CS-övningar oftast fokuserar på praktiskt tekniska färdigheter (Ernits m.fl., 2020) torde detta innebära att varje mätbar färdighet, på ett tydligt sätt behöver kopplas till ett lärandemål via relevant kunskap och förmåga. Dessa kopplingar blir därmed en del av övningens pedagogiska struktur där tydliga relationer skapas mellan respektive praktisk färdighet och relaterad förmåga och kunskap. Det torde därmed först vara när det finns en sådan etablerad och integrerad pedagogisk struktur, där varje uppgift deltagarna ställs inför under en CS-övning, tydligt kan kopplas till såväl specifik färdighet som kunskap, som det finns ett underlag för att börja diskutera i termer av att fokusera på lärande i CS-övningar.

Därmed beskrivs även vikten av att tydliggöra relationen mellan färdighet och lärandemål eftersom detta definierar den kunskap som övningen förväntas utveckla (Ernits m.fl., 2020). Denna intressanta och samtidigt kritiska aspekt av CS-övningars struktur, dvs. analys och sammankoppling av färdighet och kunskap/förmåga, vidareutvecklas dock inte i den forskning som identifierats inom ramen för denna litteraturöversikt och torde vara ett område i behov av fortsatt forskning. Dock presenteras rekommendationer kring etablerade ramverk och modeller kring lärande och kunskap som till exempel Blooms reviderade taxonomi (Krathwohl, 2002). De tidigare beskrivna exemplen på mätning och bedömning av CS-övningar kopplar tydligt till detaljerad färdighet att hantera det tekniska perspektivet på övningar (se Avsnitt 2.9), men som tidigare beskrivits ingår dock fler dimensioner och kunskapsområden i CS-övningar (t.ex. Karjalainen m.fl., 2019; White m.fl., 2004).

När det kommer till mätning och bedömning av lärande och kunskap är det dock en fråga om vilken kunskap som skall bedömas. Vilken kunskap och kompetens hos deltagarna en övning syftar till att utveckla kopplar även tydligt till identifierandet av lärandemål för övningen. Inom forskningen finns flera exempel där en gemensam nämnare består i att använda sig av olika standarder och ramverk för standardiserade definitioner av kunskap och kompetens inom det aktuella området, som till exempel NICE-ramverket (NIST, 2017). För att fånga upplevelser och reaktioner på en övning föreslår Karjalainen m.fl. (2019) frågeformulär eller enkäter som datainsamlingsmetod. För att i enkäter och frågeformulär samla in data kring lärande krävs mer öppna formulär eftersom man eftersöker deltagarens subjektiva uppfattning kring om lärandemål uppnåtts (Karjalainen m.fl., 2019). Detta innebär i sig en utmaning eftersom det kräver att deltagaren har förståelse för sitt eget lärande. Är det förväntade lärandet kopplad till en specifik övning inte tydliggjort ökar därmed risken för att i sådana enkäter erhålla svar som inte återspeglar deltagarnas faktiska lärande.

Trots att enkäter och formulär är en välbeprövad insamlingsmetod för att på detta sätt samla in underlag för bedömning av expertinlärning finns därmed tydliga utmaningar (Karjalainen m.fl., 2019). Som Karinsalo m.fl. (2022) föreslår, kan enkäter vara mer lämpliga för att skapa förståelse och utveckla kunskap kring deltagarnas förutsättningar och färdigheter innan en övning. När det kommer till de högre nivåerna i Kirkpatrick-modellen (t.ex. Kirkpatrick, 1996), dvs. beteende och resultat, är dessa, enligt Karjalainen m.fl. (2019) inte lämpliga att försöka mäta i anslutning till en enstaka övning. Detta på grund av att deltagarens förändrade beteenden potentiellt utvecklas över längre tid, och att effekter i deltagarens ordinarie verksamhet är mycket utmanande att försöka fånga ur ett övningsperspektiv. Beteendeförändringar skulle dock potentiellt kunna mätas genom att deltagare som återkommer till övningar intervjuas inför varje nytt övningstillfälle (Karjalainen m.fl., 2019). Tendensen som blir tydlig är att ju högre upp i Kirkpatrick-modellen man önskar undersöka effekter av en CS-övning, desto rikare och mer kvalitativ data måste samlas in, för att utgöra ett underlag för hur en övning påverkar och potentiellt utvecklar deltagare på ett djupare plan.

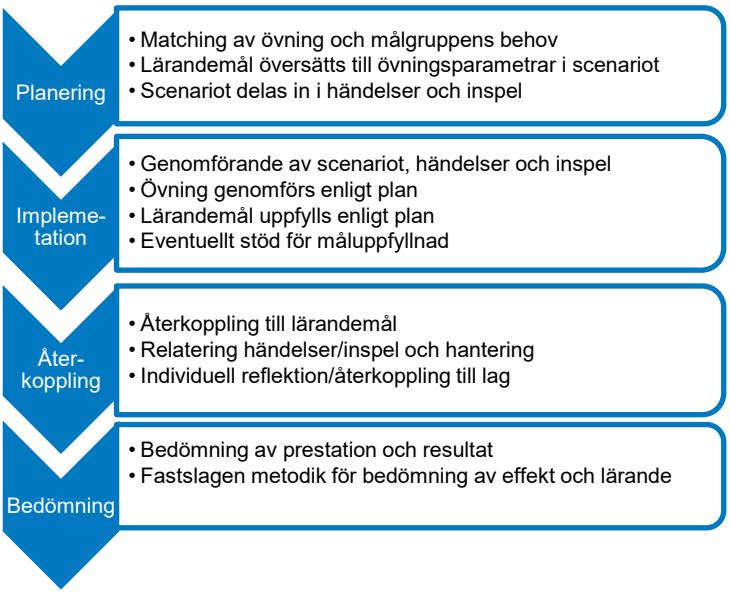
3.3 Pedagogiska perspektivens potential

På ett övergripande plan kan det beskrivna behovet av utvecklade pedagogiska perspektiv på CS-övningar kopplas till att det finns tydligt definierade kunskapsbehov som går bortom traditionellt tekniska perspektiv. Det finns ett behov av perspektiv och förklaringsmodeller från andra relevanta forskningsområden, för att hantera föreliggande utmaningar med att utveckla kunskap och förståelse kring pedagogik och lärande i CS-övningar. Genom att applicera icke-tekniska perspektiv från andra forskningsdiscipliner, kan tekniskt fokus på detta fenomen potentiellt balanseras. Eftersom CS-övningar har tydliga kopplingar till den tekniska forskningsdomänen kring cybersäkerhet, blir det symptomatiskt att de exempel på pedagogiska perspektiv på CS-övningar som beskrivits, bygger på ämnesområdesmässigt gränsöverskridande ansatser. Som exempel beskrivs att pedagogiska ansatser bör innehålla såväl beteendevetenskapliga som kognitionsvetenskapliga samt konstruktivistiska principer (Karjalainen m.fl., 2019). Ju fler perspektiv, med olika forskningsmässig hemvist som integreras inom samma pedagogiska modell blir det viktigt att (1) tydligt motivera och klargöra vad varje forskningsmässigt perspektiv tillför det pedagogiska perspektivet på CS-övning sett till sin helhet samt (2) vara medveten om att varje forskningsområde vilar på olika grundläggande antaganden, föreställningar och förutsättningar.

Ett tydligt sådant exempel är när Karjalainen m.fl. (2019) gör kopplingar mellan CS-övningar och den medicinska domänen via det pedagogiska perspektivet avsiktlig praktik (Ericsson, 2008) som en relevant modell för att beskriva utveckling av förmåga ur ett expertbaserat perspektiv. Även om det är viktigt att inom forskning nyttja och vidareutveckla redan existerande kunskap, är det lika viktigt att vara medveten om, och tydliggöra, sådana tvärvetenskapliga ansatsers fördelar, och eventuella konsekvenser och utmaningar. Pedagogiska perspektiv på CS-övningar ställer även krav på att det finns ett väl etablerat och integrerat pedagogiskt perspektiv under övningens hela livscykel, dvs. under utformning, planering, genomförande och uppföljning. Utformning och plan blir viktiga förutsättningar för övningens fortsatta steg och mål kopplat till de pedagogiska perspektiv som identifieras och som sedan följs upp och säkerställs i anslutning till övningen. Därmed adderas ytterligare en dimension, den pedagogiska, till övningens struktur och genomförande. Detta kan i sig innebära en utmaning eftersom planeringen och genomförandet av sådana övningar redan idag är resurskrävande (Karjalainen m.fl., 2019). Vidare krävs även att utvalda pedagogiska principer kopplas samman med såväl övningsmål som lärandemål som grund för identifierandet och integrerande av relevanta parametrar i övningskontexten (Karjalainen m.fl., 2019).

Detta ställer frågan om hur man skall förhålla sig till och hantera mål för övningen, kontra mål för deltagarnas lärande under övningen. Är det endast en uppsättning mål som skall identifieras och formuleras för övningen, och att det i denna uppsättning skall integreras mål som syftar till att säkerställa lärande, eller rör det sig om två separata uppsättningar av mål, dvs. för övning och för deltagarnas lärande, som dock är tydligt relaterade till varandra? Karjalainen m.fl. (2019) förespråkar här att man skiljer skiljer på övnings- respektive lärandemål. Övningsmålen lägger grunden för övningens operativa kontext och scenario och utgör förutsättningarna för de aktiviteter som kommer ingå i övningen, som i sin tur är kopplade till definierade lärandemål. Det är dock viktigt att kopplingen mellan, till exempel scenario och lärandemål, tydliggörs så att varje del av övningen är tydligt förankrat ur det pedagogiska perspektivet (Karjalainen m.fl., 2019).

Karjalainen och Kokkonen (2020) presenterar relevanta rekommendationer med hänsyn till hur pedagogiska perspektiv kan integreras i CS-övningar (se Figur 9 nedan). Bland annat framhålls vikten av att under planeringsfasen tillse att övningens innehåll överensstämmer med övningens behov och krav, och att lärandemål tas i beaktande när dessa integreras som övningsparametrar i scenariot. Karjalainen och Kokkonen (2020) framhåller även vikten av att vara medveten om att såväl övningens operationella, som pedagogiska dimensioner, följs under implementationen, samt återkoppling som ett av de viktigaste stegen med hänsyn till deltagarnas utveckling. Denna återkoppling sker lämpligtvis genom en relatering till de händelser och inspel som ingått i scenariot samt hur dessa har hanterats. Givet att lärandemål integrerats i övningens scenario, enligt tidigare steg i övningens livscykel, dvs. planering och implementation, sker här även en återkoppling tillbaka till övningens lärandemål. Med hänsyn till steget bedömning finns behov av bedömning av prestation och resultat, på individnivå som på andra nivåer, och här kan till exempel Kirkpatrick-modellen användas som utgångspunkt (Karjalainen & Kokkonen, 2020).



Figur 9. Övningens faser. Egen figur baserad på Karjalainen och Kokkonen (2020)

Karjalainen och Kokkonen (2020) ger en detaljerad bild över hur en CS-övning kan struktureras ur den operationella dimensionen men ur ett pedagogiskt perspektiv ger de endast relativt övergripande rekommendationer och råd. Det är även viktigt att ta hänsyn till hur deltagarnas lärande påverkas av deltagarnas förutsättningar. Som exempel på detta relaterar Karjalainen m.fl. (2020) till pedagogiska perspektiv som vuxnas lärande, erfarenhetsbaserat lärande samt kollaborativt lärande. Detta visar tydligt på kontextens

betydelse ur ett professionellt perspektiv på CS-övningar där syftet är att vidareutveckla deltagarnas expertkunskap snarare än att utveckla kunskap på mer grundläggande kunskapsnivåer. Sett till typ av kunskap handlar det för denna målgrupp inte om sakkunskap utan om olika typer av konceptuell och procedurell kunskap (t.ex. Krathwohl, 2002), och påverkar i sig vilka typer av lärandemål som definieras för övningen. Karjalainen m.fl. (2020) beskriver detta som utvecklad förståelse och kunskap kring konsekvenser och relationer, kopplat till andra områden, processer och funktioner. Vidare poängteras även här deltagarnas ansvar för sitt eget lärande samt delning av insikter och erfarenheter för positivt lärande i grupp. Det är dock viktigt att i detta sammanhang även ha i åtanke att deltagarna behöver ha en inställning till övning som är i linje med detta perspektiv på lärande som en självdriven och samskapande process där varje deltagare har tydliga incitament och motiv till att vidareutveckla sin egen kunskap och kompetens och samtidigt bidra till andra deltagares utveckling.

Behovet av fortsatt forskning inom området beskrivs till exempel i termer av att det behövs utvecklas effektiva strategier för lärande med hänsyn till identifiering av lärandemål och bedömningsmetoder (Alluhaidan & Abu-Taieh, 2020). Det är även viktigt att se tydligt formulerade lärandemål som ett hjälpmedel ur utförarperspektivet eftersom dessa tillsammans skapar en kontext och inriktning för övningen för såväl deltagare som utförare. Det finns dock en risk med, att som Alluhaidan och Abu-Taieh (2020), se effektivitet som en drivande faktor bakom formulerandet av lärandemål. En anledning till detta kan dock vara att Alluhaidan och Abu-Taieh (2020) fokuserar på CS-övningar ur ett akademiskt perspektiv, där volymen av examination och bedömning är en tydligt påverkande faktor. De beskriver även att för att uppfylla lärandemål, behöver utföraren ta ett tydligt större ansvar för deltagarnas måluppfyllelse, och eventuella behov av stöd (Alluhaidan & Abu-Taieh, 2020). Detta borde dock skilja sig från en professionell CS-övningskontext, där deltagarna kan förväntas ta ett större eget ansvar för sitt eget lärande.

4 Slutsatser

Syftet med denna rapport har varit att beskriva, motivera och diskutera pedagogiska perspektiv på CS-övningar, samt att presentera exempel på relevant forskning kopplat till detta område. Baserat på föreliggande rapport torde det tydligt framgå, att det finns tydlig potential och möjlighet för en ökad integrering av övningsperspektiv och pedagogiska perspektiv. Behovet av att gå från traditionella tekniska perspektiv till tvärvetenskapliga och holistiska ansatser på CS-övningar stöds av såväl forskning som praktik. Som tydligt har framgått, utvecklas och genomförs oftast denna typ av övningar med ett huvudsakligt fokus på genomförandet. Genom att genomföra övningen i enlighet med identifierade övningsmål förutsätts övningens mål vara uppfyllda. Därmed säkerställs inte att dessa övningar får avsedd effekt med hänsyn till deltagarnas utvecklade kunskap och lärande. Som beskrivits i denna rapport finns det dock tydliga behov inom forskning och praktik att adressera denna problematik genom att integrera pedagogiska perspektiv i CS-övningar. Perspektivet på CS-övningar står därmed inför ett potentiellt skifte, där även deltagarnas lärande behöver inkluderas och integreras i dessa övningars utformning, genomförande och målbild.

Med fokus på pedagogiska perspektiv och lärande, beskriver forskningen att det finns tydliga kopplingar till det akademiska området via utbildningar och kurser inom cybersäkerhet. Denna koppling kan te sig naturlig, eftersom pedagogiska perspektiv, kunskapsutveckling och lärande är centrala delar inom högre utbildning. Det finns dock tydliga skillnader mellan en akademisk övningskontext, och en professionell övningskontext, som måste tydliggöras och tas hänsyn till. Flera exempel av forskning har presenterats där perspektiv på pedagogik och lärande snarare blir ytterligare en dimension som läggs till på en befintlig, och redan komplex, övningsstruktur, vilket i sig ger upphov till nya utmaningar att hantera. I rapporten har även olika exempel på tekniska lösningar för kvantitativa mätningar och bedömningar av deltagarnas prestationer under CS-övningar presenterats. Även om det säkerligen finns möjligheter med sådana ansatser, är det samtidigt viktigt att vara medveten om riskerna med att lägga till perspektiv på pedagogik och lärande på en redan mycket komplex övningsdesign och struktur. Det finns en risk för att det pedagogiska perspektivet inte uppfattas som en integrerad dimension för att utveckla förståelse för, och skapa möjligheter för, bedömning av deltagarnas lärande.

Den komplexitet som beskrivs med hänsyn till traditionella perspektiv på CS-övningar relaterar ofta till en i huvudsak teknisk komplexitet. CS-övningar är komplexa företeelser med många samverkande faktorer och dimensioner, men denna komplexitet kan vara av såväl teknisk, som social, kognitiv, organisatorisk eller pedagogisk natur. Som presenteras i flera exempel finns det inom forskning ett återkommande mönster att perspektivet på lärande handlar om att säkerställa deltagarnas framsteg och kunskapsutveckling i enlighet med en fastslagen övningsdesign. Även om detta kan vara en möjlig strategi, finns det risk för att perspektivet på lärande blir något av en pålaga, som appliceras på en övningsdesign där lärande inte ingått som en grundläggande förutsättning. En mer passande lösning torde vara att låta perspektiv på pedagogik och lärande finnas med som en förutsättning under övningens hela livscykel. Denna integrerande syn på pedagogik i detta sammanhang är även något som stöds av t.ex. Karjalainen m.fl. (2019). Detta skulle innebära att man går från lärande som effekt och resultat av övning, till lärande som del av övningens grundläggande förutsättningar med hänsyn till design, planering, genomförande och uppföljning.

Det kan även konstateras att de möjligheter att applicera och integrera perspektiv på lärande och pedagogik, som presenteras baserat på forskning i denna rapport inte skall ses om att domänen kring cybersäkerhetsövningar har brister. Tvärtom, anledningen att dessa perspektiv nu förs fram som möjliga möjliggörare, har snarare att göra med att området har nått en mognad och en grad av reflexivitet, som i sig är en förutsättning för fortsatt utveckling i positiv riktning. Det faktum att forskningen tydligt framhåller behov av mer holistiska ansatser, tyder på ett behov att applicera sådana perspektiv på CS-övningar,

snarare än att betrakta övningars olika delar som separata tekniska delsystem. Det är därmed av vikt att försöka kartlägga och analysera hur de olika delsystem som samverkar i en CS-övnings struktur relaterar till och samverkar med varandra.

Avslutningsvis, ett specifikt område i behov av fortsatt forskning som identifierats rör sammankopplingen av färdighet, förmåga, kompetens samt lärande i CS-övningar. Det är dessa relationer som utgör grunden för sammankoppling och integrering mellan CS-övning som ett tekniskt och pedagogiskt fenomen och är av särskilt intresse.

5 Referenser

Aaltola, K., & Taitto, P. (2019). Utilising experiential and organizational learning theories to improve human performance in cyber training. *Information & Security: An International Journal*, *43*(2), 123–133.

Adams, N. E. (2015). Bloom's taxonomy of cognitive learning objectives. *Journal of the Medical Library Association: JMLA*, *103*(3), 152–153.

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), 1–15.

Ahmad, A., Johnson, C., & Storer, T. (2015). A cyber exercise post assessment: Adoption of the Kirkpatrick model. *Advances in Information Sciences and Service Sciences*, *7*(2), 1–8.

Alluhaidan, A., & Abu-Taieh, E. M. (2020). Student Learning Outcomes (SLOs) and Assessment of Cybersecurity Body of Knowledge (BOK): Evaluation & Challenges. *International Education Studies*, *13*(5), 13–23.

Ambrosini, V., & Bowman, C. (2001). Tacit knowledge: Some suggestions for operationalization. *Journal of Management studies*, *38*(6), 811–829.

Anderson, L. W., & Krathwohl, D. R. (Red.). (2001). *A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives*. New York : Longman.

Bell, R. S., Vasserman, E., & Sayre, E. C. (2015). Developing and piloting a quantitative assessment tool for cybersecurity courses. *2015 ASEE Annual Conference & Exposition*, 26.496.1-26.496.13.

Biggs, J. B., & Collis, K. F. (1982). *Evaluating the quality of learning: The SOLO taxonomy (Structure of the Observed Learning Outcome)*. Academic Press.

Boell, S. K., & Cecez-Kecmanovic, D. (2010). Literature reviews and the hermeneutic circle. *Australian Academic & Research Libraries*, *41*(2), 129–144.

Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security*, *88*, 1–13. https://doi.org/10.1016/j.cose.2019.101607

Brilingaitė, A., Bukauskas, L., Krinickij, V., & Kutka, E. (2017). Environment for cybersecurity tabletop exercises. *ECGBL 2017 11th European Conference on Game-Based Learning*, 47–55.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21.

CyberSec4Europe. (2021). *D6.3 Design of Education and Professional Framework* (Proposal No. 830929). The CyberSec4Europe Consortium.

Da Silva, J. (2022). Cyber security and the Leviathan. *Computers & security TC 11 Briefing Papers*, *116 Article number 102674*, 1–17.

Dewar, R. S. (2014). The "triptych of cyber security": A classifi cation of active cyber defence. *2014 6th International Conference On Cyber Conflict (CyCon 2014)*, 7–21.

Dewar, R. S. (2018). *Cybersecurity and cyberdefense exercises*. Center for Security Studies (CSS) ETH Zurich.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human factors*, *37*(1), 32–64.

ENISA. (2015). *The 2015 report on national and international cyber security exercises: Survey, analysis and recommendations*. European Union Agency For Network And Information Security.

ENISA. (2018). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. European Union Agency For Network and Information Security.

Ericsson, K. A. (2008). Deliberate practice and acquisition of expert performance: A general overview. *Academic emergency medicine*, *15*(11), 988–994.

Ericsson, K. A., & Smith, J. (2011). Prospects and limits of the empirical study of expertise: An introduction. *Foundations of cognitive psychology*, 393–424.

Ernits, M., Maennel, K., Mäses, S., Lepik, T., & Maennel, O. (2020). From Simple Scoring Towards a Meaningful Interpretation of Learning in Cybersecurity Exercises. *ICCWS 2020 15th International Conference on Cyber Warfare and Security*, 135–143.

European Commission. (2018). *The European Qualifications Framework: Supporting learning, work and cross-border mobility*. European Commission.

European Commission. (2019). *A proposal for a European cybersecurity taxonomy*. European Commission.

Fernandez, M. E., Ten Hoor, G. A., Van Lieshout, S., Rodriguez, S. A., Beidas, R. S., Parcel, G., Ruiter, R. A., Markham, C. M., & Kok, G. (2019). Implementation mapping: Using intervention mapping to develop implementation strategies. *Frontiers in public health*, *7*, Article 158.

Furtună, A., Patriciu, V.-V., & Bica, I. (2010). A structured approach for implementing cyber security exercises. *2010 8th International Conference on Communications*, 415–418.

Galinec, D., & Steingartner, W. (2017). Combining cybersecurity and cyber defense to achieve cyber resilience. *2017 IEEE 14th International Scientific Conference on Informatics*, 87–93.

Granåsen, M., & Andersson, D. (2016). Measuring team effectiveness in cyber-defense exercises: A cross-disciplinary case study. *Cognition, Technology & Work*, *18*(1), 121–143.

Gustafsson, T., & Almroth, J. (2020). Cyber range automation overview with a case study of CRATE. *Nordic Conference on Secure IT Systems*, 192–209.

Henshel, D. S., Deckard, G. M., Lufkin, B., Buchler, N., Hoffman, B., Rajivan, P., & Collman, S. (2016). Predicting proficiency in cyber defense team exercises. *MILCOM 2016-2016 IEEE Military Communications Conference*, 776–781.

Howells, J. (1996). Tacit knowledge. *Technology analysis & strategic management*, *8*(2), 91–106.

Karinsalo, A., Saharinen, K., Päijänen, J., & Salonen, J. (2022). Pedagogical and self-reflecting approach to improving the learning within a cyber exercise. *ECCWS 2022 21st European Conference on Cyber Warfare and Security*, 105–114.

Karjalainen, M., & Kokkonen, T. (2020). Review of Pedagogical Principles of Cyber Security Exercises. *Advances in Science, Technology and Engineering Systems Journal*, *5*(5), 592–600. https://doi.org/10.25046/aj050572

Karjalainen, M., Kokkonen, T., & Puuska, S. (2019). Pedagogical Aspects of Cyber Security Exercises. *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 103–108. https://doi.org/10.1109/EuroSPW.2019.00018

Karjalainen, M., Puuska, S., & Kokkonen, T. (2020). Measuring Learning in a Cyber Security Exercise. *2020 12th International Conference on Education Technology and Computers*, 205–209. https://doi.org/10.1145/3436756.3437046

Kick, J. (2014). *Cyber exercise playbook.* The MITRE Corporation.

Kirkpatrick, D. L. (1996). Great Ideas Revisited. Techniques for Evaluating Training Programs. Revisiting Kirkpatrick's Four-Level Model. *Training & Development*, *50*, 54–59.

Knowles, W., Such, J. M., Gouglidis, A., Misra, G., & Rashid, A. (2015). Assurance techniques for industrial control systems (ics). *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, 101–112.

Kok, G., Lo, S. H., Peters, G.-J. Y., & Ruiter, R. A. (2011). Changing energy-related behavior: An Intervention Mapping approach. *Energy Policy*, *39*(9), 5280–5286.

Kolb, A. Y., & Kolb, D. A. (2009). Experiential learning theory: A dynamic, holistic approach to management learning, education and development. I *The SAGE handbook of management learning, education and development* (Vol. 7, s. 42–68).

Krathwohl, D. R. (2002). A Revision of Bloom's Taxonomy: An Overview. *Theory Into Practice*, *41*(4), 212–218. https://doi.org/10.1207/s15430421tip4104_2

Laal, M. (2013). Collaborative learning; elements. *Procedia-Social and Behavioral Sciences*, *83*, 814–818.

Lachlan-Haché, L., Cushing, E., & Bivona, L. (2012). *Student Learning Objectives: Benefits, Challenges, and Solutions.* American Institutes for Research.

Lewis, L. H., & Williams, C. J. (1994). Experiential learning: Past and present. *New directions for adult and continuing education*, *1994*(62), 5–16.

Maennel, K., Ottis, R., & Maennel, O. (2017). Improving and measuring learning effectiveness at cyber defense exercises. *Secure IT Systems: 22nd Nordic Conference, NordSec 2017, Tartu, Estonia, November 8–10, 2017, Proceedings 22*, 123–138.

NCSC. (2022a). *Cybersäkerhet i Sverige 2022—Del 1: Hot, metoder, brister och beroenden*. Nationellt cybersäkerhetscenter.

NCSC. (2022b). *Cybersäkerhet i Sverige 2022—Del 2: Rekommenderade säkerhetsåtgärder*. Nationellt cybersäkerhetscenter.

Nevmerzhitskaya, J., Norvanto, E., & Virag, C. (2019). High Impact Cybersecurity Capacity Building. *eLearning & Software for Education*, *2*.

NIST. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (NIST Special Publication 800-181).

NIST. (2020). *Workforce Framework for Cybersecurity (NICE Framework)* (800-181 Revision 1; NIST Special Publication).

NIST. (2023). *Glossary—Cybersecurity*. https://csrc.nist.gov/glossary/term/cybersecurity

Nonaka, I. (1991). The knowledge-creating company. *Harvard Business Review*, *69*(6), 96–104.

Pirta-Dreimane, R., Brilingaitė, A., Majore, G., Knox, B. J., Lapin, K., Parish, K., Sütterlin, S., & Lugo, R. G. (2022). Application of intervention mapping in cybersecurity education design. *Frontiers in Education*, *7*, 1–12.

Porter, C. M. (2016). Revisiting Precede–Proceed: A leading model for ecological and ethical health promotion. *Health Education Journal*, *75*(6), 753–764.

Rajivan, P., & Gonzalez, C. (2018). Human factors in cyber security defense. *Human Factors and Ergonomics for the Gulf Cooperation Council. Edited by Shatha Saman. CRC Press, Boca Raton, Florida*, 85–104.

Renaud, K., & Warkentin, M. (2017). Using intervention mapping to breach the cyber-defense deficit. *12th Annual Symposium on Information Security*.

Seker, E., & Ozbenli, H. H. (2018). The concept of cyber defence exercises (cdx): Planning, execution, evaluation. *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–9.

SOU 2015:23. (2015). *Informations- och cybersäkerhet i Sverige* (Statens Offentliga Utredningar SOU 2015:23).

Švábenský, V., Vykopal, J., & Čeleda, P. (2020). What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 2–8. https://doi.org/10.1145/3328778.3366816

Švábenský, V., Weiss, R., Cook, J., Vykopal, J., Čeleda, P., Mache, J., Chudovský, R., & Chattopadhyay, A. (2022). Evaluating Two Approaches to Assessing Student Progress in Cybersecurity Exercises. *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education*, 787–793. https://doi.org/10.1145/3478431.3499414

Taitto, P., Nevmerzhitskaya, J., & Virag, C. (2018). Using holistic approach to developing cybersecurity simulation environments. *The 14th International Scientific Conference eLearning and Software for Education*, *4*, 77–84. https://doi.org/10.12753/2066-026X-18-226

Valassi, C., Westerdahl, L., & Borg, A. (2021). *Inventering av cyberövningar* (FOI-D--1068--SE). Totalförsvarets forskningsinstitut.

Vykopal, J., & Barták, M. (2016). On the design of security games: From frustrating to engaging learning. *2016 USENIX workshop on advances in security education (ASE 16)*.

Weiss, R., Locasto, M. E., & Mache, J. (2016). A Reflective Approach to Assessing Student Performance in Cybersecurity Exercises. *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, 597–602. https://doi.org/10.1145/2839509.2844646

White, G. B., Dietrich, G., & Goles, T. (2004). Cyber security exercises: Testing an organization's ability to prevent, detect, and respond to cyber security events. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004.*, *37*, 2635–2644.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

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

www.foi.se