Ragnarök – från kaos till lärande och stärkt cyberförmåga

Övningskoncept för stärkt incidenthanterings-förmåga i samhällsviktig verksamhet

Malin Granath, Fredrik Söderström

FOI-R--5748--SE

Juni 2025

Malin Granath, Fredrik Söderström

Ragnarök – från kaos till lärande och stärkt cyberförmåga

Övningskoncept för stärkt incidenthanteringsförmåga i samhällsviktig verksamhet

Titel	Ragnarök – från kaos till lärande och stärkt cyberförmåga – Övningskoncept för stärkt incidenthanteringsförmåga i samhällsviktig verksamhet
Title	Ragnarök – from chaos to learning and strengthened cyber capability – Exercise concept for strengthened incident response capabilities in critical operations
Rapportnr/Report no	FOI-R--5748--SE
Månad/Month	Juni / June
Utgivningsår/Year	2025
Antal sidor/Pages	61
ISSN	1650-1942
Uppdragsgivare/Client	Nationellt cybersäkerhetscenter
Forskningsområde	Cyberförsvar och cybersäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E38068
Godkänd av/Approved by	Emil Hjalmarson
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Bild/Cover: Shutterstock /JLStock

Sammanfattning

På grund av det osäkra världsläget och ständigt nya hot, är Sverige i stort behov av att stärka sin cyberförmåga. Ett sätt att stärka denna cyberförmåga är att erbjuda övningar i incidenthantering, som syftar till att utveckla deltagarnas förmåga att upptäcka och hantera cyberhot och cyberangrepp. En del av samhällsstrukturen med högt skyddsvärde är samhällsviktig verksamhet inom sektorer som till exempel energi, transport, telekom, finans och hälso- och sjukvård. Denna rapport presenterar resultatet av utvecklingen av ett övningskoncept fokuserat på incidenthantering för deltagare inom samhällsviktig verksamhet. Övningskonceptet är framtaget i nära samarbete med centrala relevanta aktörer på nationell nivå inom cybersäkerhetsområdet. Konceptet består av en bärande idé som i sin tur stöds av ett antal grundläggande principer. Principerna är tydligt kopplade till övningsmål samt mål för att säkerställa avsedd effekt och resultat. Genom sitt tydliga fokus på generaliserbarhet, skalbarhet, modularitet och flexibilitet är övningskonceptet tänkt att ge nya och bättre förutsättningar att erbjuda övningar till avsedd målgrupp. Förutom att svara mot ett tydligt formulerat samhällsbehov adresserar övningskonceptet även flera tydligt formulerade behov inom forskningen som till exempel ett integrerat pedagogiskt perspektiv och en logik för mätning av resultat och effekt.

Nyckelord: övningskoncept, konceptuell design, effektmätning, cybersäkerhet, incident- och krishantering

Summary

Due to the uncertain global situation and constant new threats, Sweden needs to strengthen its cyber capabilities. One way to strengthen this cyber capability is to offer exercises in incident response that aims to develop the participants' abilities to detect and manage cyber threats and cyber-attacks. Critical operations in sectors such as energy, transport, telecom, finance and healthcare, are part of the societal structure with high protection value. This report presents the results of developing an exercise concept focused on incident response for participants in critical operations. The exercise concept has been developed in close collaboration with central relevant actors at the national level in the cybersecurity area. The concept consists of a core idea that is supported by a number of fundamental principles. The principles are clearly linked to exercise objectives and goals to ensure the intended effect and results. Through its clear focus on generalizability, scalability, modularity and flexibility, the exercise concept is intended to provide new and better conditions for offering exercises to the intended target group. In addition to responding to a clearly formulated societal need, the exercise concept also addresses several formulated needs within research, such as an integrated pedagogical perspective and a clear logic for measuring results and impact.

Keywords: exercise concept, conceptual design, measuring effect, cyber security and incident- and crisis response

Vinjett

Ragnarök

– från kaos till lärande och stärkt cyberförmåga

I den nordiska mytologin markerar Ragnarök slutet på den gamla världen – en storm av eld - en strid där asar möter jättar, monster och underjordens skaror. Ur havet stiger dock en ny värld - ur kaoset föds en ny gryning.

I vår digitala tidsålder har hoten skiftat form, men känslan av oundviklig konflikt består. Ett tyst larm ljuder i systemen. På skärmar blinkar varningar, och i det osynliga nätet som bär vårt samhälle sprider sig oron. Skuggor samlas vid horisonten. Någonting är fel.

Ragnarök är inte en domedag – det är en prövning.

Cybersäkerhetsövningen Ragnarök simulerar ett eskalerande angrepp mot samhällskritisk verksamhet. Den blottlägger svagheter, utmanar rutiner och kräver beslutsamhet under tryck.

Deltagarna kastas in i en komplex och föränderlig hotmiljö där inget är statiskt, och där varje val får konsekvenser. I denna moderna myt kämpar inte asar mot jättar – utan analytiker, tekniker, strateger och beslutsfattare mot kod, kaos och angrepp.

Men syftet är inte seger – det är insikt.

I lågan av Ragnarök smids lärdomar. Genom analys, samarbete och strategiskt agerande stärks förmågan att upptäcka, hantera och motverka cyberhot. Det handlar om att bygga motståndskraft – inte bara i system, utan i människor.

Övningen blir en katalysator för utveckling, där varje identifierad brist är en möjlighet till förbättring. Precis som den gamla världen i mytologin gav plats åt en ny, spirar här en starkare incidenthanteringsförmåga ur prövningen.

Ragnarök är inte slutet – det är början på något nytt och bättre.

Innehållsförteckning

1 Inledning

Detta kapitel inleds med att beskriva arbetets bakgrund, syfte och mål samt motivering. Därefter följer en kortfattad redogörelse för applicerad metod samt en tydlig definition av rapportens målgrupp och avgränsningar. Kapitlet avslutas med tydliggöranden kring centrala begrepp.

1.1 Bakgrund

I takt med samhällets ökande digitalisering, ökar även krav och behov att skydda sig mot cyberangrepp. Samhällsviktig infrastruktur ses som ett tydligt mål för en hotaktör som vill orsaka skada på Sveriges såväl fysiska som digitala infrastruktur, och därmed är skydd mot cyberhot och cyberangrepp en nationell angelägenhet (NCSC-SE, 2024). Den ökande hotbilden i cyberdomänen kan till exempel spåras till såväl traditionella angrepp från olika typer av hotaktörer (statliga aktörer, kriminella grupper, ideologiskt drivna aktörer), olika typer av statsfinansierade påverkanskampanjer (Whyte, 2020), traditionell kriminalitet som i ökande takt flyttar till den cyberdomänen (Aslan m.fl., 2023) som direkt cyberkrigföring. En viktig faktor i sammanhanget är även att den ökande digitaliseringen och ökande närvaron i cyberdomänen resulterar i en ständigt ökande teknisk komplexitet, vilket i sin tur resulterar i nya typer av sårbarheter som kan utnyttjas av hotaktörer. Vi ser alltmer avancerade och sofistikerade angrepp, eftersom hotaktörernas tekniska kompetens ökar i takt med den tekniska utvecklingen (Aslan m.fl., 2023).

För att kunna hantera alltmer sofistikerade och avancerade cyberhot ökar även behoven av kompetensutveckling inom cyberdomänen (Brilingaitė m.fl., 2020). Bristen på cyber- och cybersäkerhetskompetens är tydligt identifierad (Försvarsdepartementet, 2023, 2025; NCSC-SE, 2024) och en ökad kunskap och främjandet av kompetensutveckling inom cybersäkerhetsområdet efterlyses (RiR 2023:8, 2023). Utvecklad kunskap och kompetens inom incidenthantering, och att anordna övningar inom cybersäkerhetsområdet, beskrivs som centrala delar för en nationell strategi inom cybersäkerhet (Enisa, 2016). Denna behovsbild bekräftas även av till exempel Dewar (2018), som beskriver att det ökade antalet cyberincidenter och den ökande komplexiteten i dessa angrepp, samt förändringar i hotlandskapet, har lett till ett ökat behov av att vara förberedd på såväl nationell som internationell nivå.

För att stå emot och hantera ökande hot inom cyberdomänen skapas även ökande behov av övning och träning inom cybersäkerhet. Praktiska cybersäkerhetsövningar, inom till exempel incidenthantering, är ett etablerat sätt att öva inom detta område där deltagarna utsätts för, och förväntas hantera, olika typer av hot och angrepp i en realistisk simulerad teknisk miljö. Dessa typer av

övningar har traditionellt haft ett företrädesvis tekniskt perspektiv, men inom forskningen framkommer tydliga behov av att se cybersäkerhetsövningar som mer komplexa och tvärvetenskapliga fenomen (Craigen m.fl., 2014; Rajivan & Gonzalez, 2018; Söderström, 2025).

För att utveckla förståelse för och vidareutveckla denna typ av övningar behöver olika vetenskapliga perspektiv från olika forskningsområden appliceras på cybersäkerhetsövningar. Det räcker inte för verksamheter att inneha den tekniska förmåga och färdighet som krävs för att till exempel hantera incidenter, utan i detta sammanhang blir även organisatoriska och mänskliga förmågor viktiga (White m.fl., 2004). För att kunna hantera hot och angrepp inom cyberdomänen behöver till exempel personer i olika positioner, och med olika kunskaper och kompetenser, kunna kommunicera och samarbeta (Aaltola & Taitto, 2019). Dessutom behöver förståelsen kring kunskapsutveckling och lärande kopplat till cybersäkerhetsövningar vidareutvecklas för bättre kunskap om dessa övningars resultat och effekt (Söderström, 2025).

1.2 Syfte och mål

Syftet med arbetet som presenteras i denna rapport har varit att adressera ett tydligt formulerat behov av att utveckla ett övningskoncept rörande cybersäkerhetsövning för deltagare från samhällsviktig verksamhet i Sverige. Det övergripande syftet kan därmed beskrivas som att bidra till att stärka Sveriges förmåga att stå emot, hantera och lära av cyberhot och cyberangrepp genom att vidareutveckla förmågan inom samhällsviktig verksamhet. Målet kan beskrivas som att tydligt formulera och bidra med en välgrundad beskrivning av ett övningskoncept samt presentera ett exempel på övning baserad på konceptet. Övningskonceptet består i sig av dess bärande idé och grundläggande principer, som i sin tur ligger till grund för övningsdesign, övningens delar samt logik för effektmätning. Samtliga dessa delar skall ses som tätt sammankopplande och interagerande och främjar tillsammans god uppfyllelse av såväl syfte som mål.

1.3 Motivering

Under lång tid har övningar använts i militära sammanhang som ett effektivt sätt att visualisera, praktisera och lära för verkliga situationer. Enligt Dewar (2018) ger cybersäkerhetsövningar möjlighet att till exempel:

- Samla deltagare från olika organisationer och verksamheter för att stärka den nationella cybersäkerheten och stärka kommunikationen mellan berörda parter.
- Validera och testa policyer, planer, rutiner och kommunikationsverktyg, samt identifiera luckor och brister i såväl kompetenser som rutiner.

- Stödja och främja strategisk planering och identifiering av nödvändig utrustning, rutiner, processer, teknik och kompetens kring cybersäkerhetsfrågor samt krishantering.
- Öka medvetandegrad och kunskap samt främja förbättrad lägesbild och situationsmedvetenhet inom cyberdomänen samt stärka incidentberedskapen.
- Vara ett anpassningsbart verktyg för övningar som kan ta hänsyn till den övande verksamhetens egna behov och önskemål.
- Genomföras som storskaliga simuleringsövningar i en kontrollerad virtuell miljö, vilket i sig kan vara utmanade att arrangera för respektive deltagande verksamhet.
- Riktas mot olika delar av verksamheten, det vill säga incidenthantering på operativ nivå respektive skrivbordsövning på strategisk nivå.
- Kombineras med olika forskningsperspektiv, till exempel pedagogiska, för att följa upp och utvärdera deltagarnas lärande och verklig effekt i deltagarnas verksamhet.

1.4 Metod

Arbetet med att utveckla övningskonceptet har genomförts baserat på en tolkande ansats (t.ex. Walsham, 1993). Baserat på en framväxande kunskap kring olika aktörers tolkningar inom det aktuella området genomfördes riktade litteratursökningar i Google Scholar och Scopus. Sett till sitt genomförande har arbetet genomförts baserat på en explorativ och iterativ ansats där övningskonceptet successivt konkretiserats. Arbetet har primärt genomförts i samverkan mellan Totalförsvarets forskningsinstitut (FOI) och Nationellt cybersäkerhetscenter (NCSC-SE) där medverkan från NCSC-SE innefattat representanter från Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB), Försvarets radioanstalt (FRA) samt Säkerhetspolisen. Enskilda sakfrågor och konceptet har diskuterats och förankrats med experter och behovsägare inom området, till exempel vid workshops. Det praktiska arbetet har bedrivits i form av tydligt behovsstyrda aktiviteter såsom:

- En workshopserie som fokuserat på följande relevanta områden: förutsättningar och förmågor, övningsmål och lärandemål, övningsmiljön och tekniken, scenarion och aktiviteter, affärsmodell, övningsdesign, uppföljning och effekt.
- Kontinuerliga avstämningsmöten internt på FOI och med beställaren NCSC-SE för intern och extern förankring, samt för att kontinuerligt säkerställa inriktning, relevans och kvalitet.

1.5 Målgrupp och avgränsningar

Målgruppen för övningskonceptet, och de övningar som baseras på konceptet, är det civila försvaret, som en del av totalförsvaret i Sverige, och personer som arbetar med cyberssäkerhet inom samhällsviktig verksamhet. Eftersom arbetet som presenteras i rapporten har bestått i att utveckla en konceptuell design, kommer rapporten inte ta hänsyn till detaljerade tekniska beskrivningar och exempel.

1.6 Terminologi

För läsarens förståelse behöver några centrala termer och begrepp förtydligas. Detta behov kan i sig relateras till avsaknad av en tydlig konsensus kring grundläggande begrepp och terminologi inom cyberdomänen (Dewar, 2014; Futter, 2018).

Cybersäkerhet relaterar till de förutsättningar som krävs för att hantera och motverka cyberattacker och andra typer av angrepp som utgår från cyberdomänen (Craigen m.fl., 2014).

Koncept är ett centralt begrepp i denna rapport. Med hänsyn till framtagandet av det övningskoncept som presenteras, definierar vi koncept som en generell och sammanhållen representation av vad som krävs för att designa och beskriva en specifik övningsansats. Det handlar om att identifiera lämpliga nivåer i presentationer med hänsyn till abstraktion, kategorisering och representation. I detta sammanhang framhålls även konceptutvecklingens tydliga framväxande natur.

Cyber Security Exercises (CSX) *och Cyber Defence Exercises* (CDX) är två olika sätt att namnge cybersäkerhetsövningar. I rapporten kommer det i förekommande fall att hänvisas till den internationella akronymen. Vi har i dessa fall valt att använda oss av CSX som benämning på övning som syftar till att utveckla deltagarnas färdighet och förmåga kring hantering av hot, angrepp och incidenter i en simulerad realistisk teknisk miljö. Vi motiverar detta givet övningskonceptets syfte och mål, det vill säga att stärka förmåga inom cybersäkerhetsområdet.

Skrivbordsövning (*Table Top Exercise*, TTX) inriktas på förmågeutveckling på strategisk nivå i verksamheter. Denna övning karaktäriseras av att den är inriktad på att öva personer i deras professionella roller och ansvar när det kommer till krishantering (Grance m.fl., 2006; Švábenskỳ m.fl., 2024).

Då övningskonceptet riktas till *samhällsviktig verksamhet*, det vill säga verksamheter, tjänster eller infrastrukturer som är viktiga för att upprätthålla

samhällets grundläggande behov, värden och säkerhet[1], förekommer även kopplingar till sektorer i rapporten. *Sektor* avser verksamheter och tjänster som har gemensamma egenskaper i fråga om funktioner, verksamheter och mål. Exempel på sektorer är telekomsektorn, hälso- och sjukvårdssektorn, finanssektorn samt transportsektorn.

Cyberhot, angrepp och incident. Ett cyberhot är en potentiell fara eller en sårbarhet inom verksamheten, det vill säga en svaghet eller brist, som en hotaktör kan välja att utnyttja. Den aktiva handlingen att exploatera sårbarheten utgör själva angreppet och konsekvenserna av denna aktiva handling kan resultera i en incident, det vill säga en säkerhetshändelse som leder till att ett intrång sker och system, nätverk eller data påverkas på ett otillåtet sätt. Det finns olika typer av incidenter där det kan röra sig om till exempel dataläckor, obehörig åtkomst eller att skadlig kod sprids i verksamheten.

[1] Se SOU 2024:64 för en mer utvecklad tolkning av begreppet samhällsviktig verksamhet.

2 Övningskonceptet

Detta kapitel beskriver övningskonceptet genom att först presentera den bärande idén som konceptet utgår från, och sedan beskriva de grundläggande principer som bidrar till att uppfylla den bärande idén. Därefter presenteras en konceptskiss som beskriver hur de olika delarna i konceptet hänger samman. Övningskonceptet ligger sedan till grund för design och genomförande av övningar.

2.1 Bärande idé

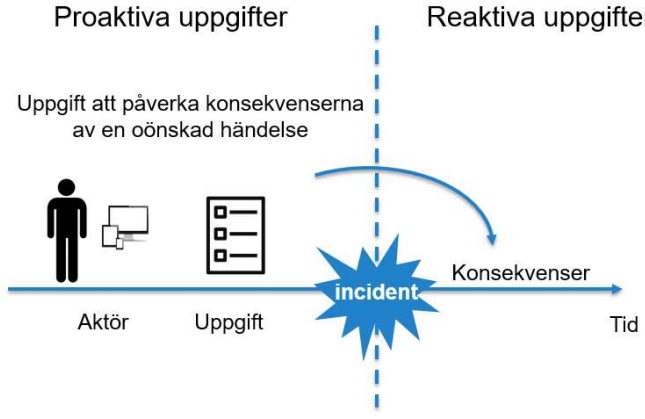
Den bärande idén i övningskonceptet är att *stärka* Sveriges *förmåga* att *förebygga*, *upptäcka* och *hantera* cyberhot och cyberangrepp, samt *lära* av angrepp och incidenter. Övningskonceptets bärande idé är därmed baserad på ett holistiskt perspektiv och syftar till att adressera den tidigare beskrivna behovsbilden. Notera att de centrala delar som kommer att förklaras har markerats med kursiv stil. Dessa delar är av stor vikt var för sig, men utgör också tillsammans grunden i övningskonceptets bärande idé.

2.1.1 Centrala delar

Stärka handlar om att göra Sverige starkare och mer robust när det gäller den samlade förmågan att förebygga, upptäcka, hantera och lära av cyberhot, cyberangrepp och incidenter. Begreppet stärka syftar därmed till en övergripande stärkt förmåga att hantera olika aspekter av hot, angrepp och incidenter, alltifrån att förhindra att hoten inträffar till att minimera skadan när incidenter väl sker. I övningskonceptet har stärka kommit att innefatta ett fokus på att öva på bredden, det vill säga sektors- och verksamhetsövergripande. Konceptet utgår således från att övningsdeltagare omsätter erfarenheter och insikter från övning i sin ordinarie verksamhet och på så vis bidrar till den stärkta nationella förmågan.

Förmåga kan tolkas och beskrivas på olika sätt beroende på sammanhang och användningsområde. I många sammanhang likställs förmåga med de resurser, eller den kunskap och de färdigheter, som behövs för att kunna utföra en given uppgift. När det gäller krishanteringsförmåga menar Lindbom och Tehler (2020) att förmågan kommer till uttryck i effekterna av de handlingar någon genomför i syfte av att uppnå ett visst ändamål. För övningskonceptet handlar förmåga primärt om förmågan att förebygga, upptäcka och hantera incidenter. Denna förmåga syftar till att minska sannolikheten för att en incident inträffar, och om incidenten ändå inträffar, om att minimera och begränsa skadan som uppstår. Ju högre incidenthanteringsförmågan är, desto mindre blir de negativa verksamhetsmässiga konsekvenserna. Incidenthanteringsförmågan illustreras i Figur 1 genom att en aktör (människa eller system) utför både proaktiva uppgifter och reaktiva uppgifter. Proaktiva uppgifter syftar till att minimera

sannolikheten för att en incident inträffar, och reaktiva uppgifter syftar till att begränsa konsekvenser av incidenter samt att förhindra att nya incidenter uppstår.



Figur 1. Aktörer, uppgifter och konsekvenser kopplade till incidenthanteringsförmåga.

Förebygga handlar om att på förhand vidta åtgärder för att hindra att hot realiseras i form av cyberangrepp. Förebyggandet kommer till uttryck i proaktiva uppgifter som bygger på till exempel övervakning, loggning av nätverksaktiviteter, säkerhetsgranskningar, segmentering av nätverk, styrning av behörighetsåtkomst och lösenordsrutiner, säkerhetskopiering av data, upprättande av handlingsplaner, utbildning och övning. Övningskonceptet representerar i sig en förebyggande uppgift genom att personer bereds möjlighet att öva incidenthantering. Samtidigt innebär övningskonceptet fokus på vissa specifika förebyggande uppgifter.

Upptäcka och *hantera* innebär aktivt arbete med att upptäcka hot och sårbarheter innan de kan utnyttjas av en hotaktör, samt att hantera de incidenter som inträffar. Uppgifter som kopplar till att upptäcka och hantera hot kan till exempel handla om att övervaka nätverksaktiviteter och systemloggar för identifiera avvikelser från det normala, eller att bedriva aktiv omvärldsbevakning och hotanalys, samt agera förebyggande på relevant underrättelse. Uppgifter kopplade till att upptäcka och analysera hot kan både vara proaktiva och reaktiva i sin karaktär. Att upptäcka och hantera cyberangrepp innebär också ett aktivt arbete med uppgifter i samband med en incident, såsom att i realtid identifiera och analysera angrepp, isolera och begränsa skadlig aktivitet, utreda, dokumentera och rapportera händelseförlopp samt att åtgärda och återställa verksamheten. Dessa uppgifter är ofta reaktiva till sin karaktär och fokuserar på att minimera negativa konsekvenser av en incident. Sammantaget fokuserar övningskonceptet i sig på reaktiva aktiviteter kopplat till incidenthantering, men bereder även för proaktiva uppgifter i form av framåtsyftande lärdomar.

Lärande handlar om att analysera och dra lärdomar av hot, angrepp och incidenter i syfte att säkerställa att de inte återupprepas, och att stärka förmågan att motstå och minimera de negativa konsekvenserna av framtida angrepp. Uppgifter som kan bidra till lärande kan innefatta att identifiera och analysera grundorsaker till incidenter såsom sårbarheter och attackvektorer, analysera händelseförlopp och tidslinjer, samt analys av konsekvenser för system och verksamhet. I övningskonceptet fokuserar lärandet på att medvetandegöra deltagare om relevanta förmågor, och att genom övning utveckla kunskap och erfarenhet, som sedan kan vidareutvecklas i deltagarens ordinarie verksamhet.

2.2 Grundläggande principer

Baserat på den bärande idén och idéns olika ingående delar har ett antal grundläggande principer formulerats för övningskonceptet. Principerna är resultatet av ett induktivt analysarbete. Syftet med dessa principer är att säkerställa övningskonceptets innehåll, inriktning och måluppfyllelse. Tabell 1 ger en sammanställd bild över konceptets grundläggande principer och hur dessa kan relateras till den bärande idén.

Tabell 1. Grundläggande principer och relationer till bärande idé och idéns centrala delar.

Princip	Relation till bärande idé
Incidenthanteringsförmåga	Relaterar till den bärande idén och den övergripande förmågan att effektivt kunna förebygga, upptäcka och hantera cyberhot och cyberangrepp samt minimera skador genom strukturerad respons.
Storskaliga cyberangrepp	Relaterar till stärkande delar och behovet av att vara beredd på storskaliga antagonistiska angrepp som kan hota nationell säkerhet.
Samhällsviktig verksamhet	Relaterar till behovet av att skydda och stärka funktioner som är centrala för att upprätthålla samhällets grundläggande tjänster vid angrepp.
Roller, funktioner och samspel	Relaterar till uppgifter och ansvar vid hantering och koordinering av agerande vid storskaliga angrepp och incidenter.
Tillit och förtroende	Relaterar till både stärkande och lärande delar i syfte att förebygga och upptäcka cyberhot och cyberangrepp, och utgör förutsättningar för effektiv samverkan och informationsdelning, både förebyggande och under pågående incident.
Relevans och realism	Relaterar till lärande delar och efterfrågad förmåga. Ökar beredskapen genom att träna på, och lära av situationer som ligger nära verkliga scenarier och hotbilder.
Generaliserbarhet och skalbarhet	Relaterar till den övergripande förmågan genom att möjliggöra bred tillämpning och förbättring av förmåga i hela samhället, inte bara hos enskilda aktörer.

Princip	Relation till bärande idé
Lärande och effekt	Relaterar till stärkande delar, samtidigt som lärande och effekt stödjer den bärande idéns del om att lära av incidenter och förbättring genom reflektion, analys och kunskapsdelning.
Holism och tvärvetenskaplighet	Relaterar till den övergripande förmåga som krävs. Cyberhot är komplexa och det krävs bred kompetens, helhetsperspektiv och relevanta forskningsperspektiv för att stärka totalförsvarets samlade förmåga.

2.2.1 Incidenthanteringsförmåga

Principen *incidenthanteringsförmåga* innebär att övningskonceptet fokuserar på incidenthantering och de olika förmågor som krävs för att förebygga, upptäcka, hantera och lära av cyberhot och cyberincidenter. Principen är grunden för utvecklingen av övningskonceptet. Behovet har identifierats baserat på NCSC-SE:s behovsanalys, utlåtanden från experter som arbetar med incidenthantering, till exempel CERT-SE, vetenskaplig litteratur samt relevanta ramverk och guider såsom NICE-ramverket (Newhouse m.fl., 2017) och NIST:s Computer Security Incident Handling Guide (Cichonski m.fl., 2012; Nelson m.fl., 2025).

Principen incidenthanteringsförmåga kopplar till exempel till krisledning och krishantering, teknik, hantering och analys av komplexa problem, problemlösning, ledarskap, kommunikation, samarbete och uthållighet. Forskning lyfter att det finns behov på olika nivåer, såväl organisatorisk nivå, gruppnivå, individnivå samt teknisk nivå, när det kommer till incidenthantering och de förmågor som behöver övas (Van der Kleij m.fl., 2017). På organisationsnivå uttrycks ett behov av att bättre kunna koordinera och dela information med utomstående aktörer och att lära av incidenter. På gruppnivå är behoven kopplade till utmaningar med att dela information och hålla relevanta parter underrättade under långvariga incidenter. Ett kritiskt moment har visat sig vara när incidenthanteringsteam avlöser varandra. På individnivå lyfts utmaningar som kopplar till beslut om eskalering samt etiska och juridiska dilemman fram. På teknisk nivå kan det handla om behov av bättre kommunikationsverktyg (Van der Kleij m.fl., 2017). Identifierade behov och förmågor kring incidenthantering bidrar till att rama in och stärka relevansen av övningskonceptet.

2.2.2 Storskaliga cyberangrepp

Principen *storskaliga cyberangrepp* innebär att övningskonceptet fokuserar på, och tar höjd för, cyberangrepp som både är storskaliga och antagonistiska till sin karaktär. Principen bidrar till att hänsyn till olika aspekter av cyberangrepp tas vid övningsdesign som till exempel scenarion och simulerade angrepp. Dessa aspekter kopplar till hotens och angreppens karaktär och utformning, samt till

hotaktörens tillvägagångssätt och motiv. Följande aspekter av angrepp har varit styrande i sammanhanget:

- Angreppens omfattning, spridning, varaktighet och konsekvenser
- Komplexitet relaterad till avancerad teknik, attackkedjor[2] och faser samt mål och verkansgrad
- Dynamiska variabler som oförutsägbarhet och tidpunkt
- Motiv, metoder och verktyg.

Principen storskaliga cyberangrepp bidrar till att förbereda deltagare på att möta betydande, mångfacetterade och komplexa hot och angrepp. Principen kan i förlängningen förhoppningsvis minimera de negativa konsekvenserna av skador och produktionsbortfall samt minska tiden för att återställa verksamheten till normalläge. Principen bekräftas även av forskning som visar att angripare använder alltmer sofistikerade verktyg och metoder för att nyttja brister och sårbarheter i nätverk och system (Admass m.fl., 2024; Li & Liu, 2021; Uma & Padmavathi, 2013). Det har blivit vanligare med avancerade ihållande hot (Advanced Persistent Threats, APT), det vill säga angrepp som inte bara är sofistikerade utan också målinriktade och organiserade i sin karaktär. Angreppen riktas ofta mot specifika mål såsom kritisk infrastruktur och samhällsviktig verksamhet med ett syfte att antingen stjäla information eller att sabotera (Mallick & Nath, 2024).

2.2.3 Samhällsviktig verksamhet

Principen *samhällsviktig verksamhet* innebär ett tydligt fokus på infrastrukturer, anläggningar, verksamheter och tjänster som är av avgörande betydelse för att upprätthålla viktiga samhällsfunktioner. Viktiga samhällsfunktioner är sådana funktioner som är ”nödvändiga för samhällets grundläggande behov, värden eller säkerhet” (MSB, 2023, s. 8)[3]. Principen bidrar därmed till att fokusera på de specifika egenskaper och faktorer som påverkar samhällsviktig verksamhet.

Forskning konstaterar att det skett ett skifte i fokus vad gäller cyberangrepp, från att tidigare ha riktat sig mot IT-system till att nu i allt högre grad även inkludera operativ teknik (Operational Technology, OT) och industriella styrsystem (Industrial Control System, ICS) inom samhällsviktig verksamhet (Staves m.fl., 2022). OT och ICS karaktäriseras av att dessa typer av system övervakar och styr fysiska eller kemiska processer och utgör en viktig del i våra samhällsviktiga infrastrukturer (MSB, 2021; Wei & Ji, 2010).

Digitala tekniker används bland annat för automatisering, styrning och övervakning av processer, för datainsamling, optimering och underhåll samt för

[2] Från engelskans kill chain. Ett sätt att beskriva ett cyberangrepps olika faser.

[3] Se SOU 2024:64 för vidare tolkning av begreppen samhällsviktig verksamhet (SOU 2024:64, 2024).

fjärrövervakning av system. Integrationen av digitala system med OT och ICS har bidragit till nya typer av sårbarheter och förändrade angreppssätt (Bıçakcı & Evren, 2024). Angrepp mot dessa typer av cyberfysiska system får även konsekvenser utanför cyberdomänen. Principen samhällsviktig verksamhet bidrar således till att rama in sammanhanget i övningskonceptet.

2.2.4 Roller, funktioner och samspel

Principen *roller*, *funktioner och samspel* syftar till att övningskonceptet ska fokusera på relevanta roller och funktioner som har bäring på incidenthantering i samhällsviktig verksamhet. Forskning understryker vikten av att, i ett tidigt skede i planeringen, identifiera målgruppen för övningen (Grance m.fl., 2006). Principen bidrar således till att tydliggöra vilka roller och funktioner som är relevanta för incidenthantering i samhällsviktig verksamhet. Därmed främjas en övningsdesign där organisering och beslutsstrukturer upplevs som realistiska och relevanta.

Rollerna och funktionerna delas upp utifrån verksamhetsområde, kompetenser och ansvar, och utgår från ett strategiskt operativt, samt ett tekniskt operativt perspektiv på incidenthantering. Principen hjälper till att till exempel identifiera organisationsstrukturer, rollbesättningar och aktiviteter som kräver korrekt och tydlig kommunikation mellan roller och funktioner. Forskning visar att övning är ett effektivt sätt att träna beslutsvägar och kommunikation mellan olika roller och funktioner, samtidigt som det ger möjligheter att identifiera svagheter i systemen (Dewar, 2018).

2.2.5 Tillit och förtroende

Principen *tillit och förtroende* syftar till att övningskonceptet ska främja och stärka relationer mellan olika relevanta aktörer och deltagare. Enligt Robbins (2016) är tillit en framväxande känsla av trygghet och säkerhet i interaktionen med andra individer. Robbins kategoriserar den relationella tilliten utifrån tre distinkta dimensioner: hur man litar på, vem man ska lita på och vad man kan lita på att någon annan gör. Vi väljer, i linje med Robbins (2016), att se tillit som något som är relationellt och bygger på erfarenhet och övertygelser.

Tillit och förtroende är viktiga faktorer som påverkar cybersäkerhetsarbete, till exempel när det kommer till att dela information kring incidenter och incidenthantering mellan olika verksamheter. Tillitsfulla relationer karaktäriseras av att parterna kan lita på att motparten agerar på ett förutsägbart och pålitligt sätt. Tillit och förtroende är särskilt viktigt när det kommer till viljan att dela med sig, samt viljan att ta del av information om incidenter. Forskning beskriver informationsdelning som en utmaning, framförallt när det kommer till känslig information (Posso & Altmann, 2024; Van der Kleij m.fl., 2017).

Huruvida verksamheter är villiga att dela denna typ av information eller inte har visat sig bero på om det redan finns förtroliga relationer mellan parterna sedan tidigare. Det finns även andra faktorer som påverkar tilliten och förtroendet mellan parter i sammanhanget såsom till exempel rykten, kundrelationer och konkurrens. Många verksamheter väljer därmed aktivt att inte dela information om incidenter, för att undvika att röja sina brister och sårbarheter. Tillit och förtroende bidrar i övningskonceptet bland annat till att skapa förutsättningar för deltagare att bygga förtroende för varandra och för systemet.

2.2.6 Relevans och realism

Principen *relevans och realism* handlar om att övningskonceptet skall ligga till grund för övningar som efterliknar verkliga händelser som omsätts i realistiska scenarier och aktiviteter i en simulerad teknisk miljö. Principen syftar även till att säkerställa en så hög relevans som möjligt baserat på deltagarnas förutsättningar. Design och genomförande baserat på övningskonceptet strävar efter en tillräckligt hög grad av realism sett till scenarier, aktiviteter och tekniska förutsättningar. Detta krävs för att övningen ska uppfattas som trovärdig och skapa engagemang.

Forskningen menar att realism har stark påverkan på cybersäkerhetsövningar för att kunna utveckla den specifika övning och träning som krävs (Nevmerzhitskaya m.fl., 2019). Vi väljer i detta sammanhang, att i linje med Gross m.fl. (1999), definiera realism som en simulerings förmåga att återskapa en faktisk miljö eller företeelse. Realism i cybersäkerhetsövningar är en faktor som även påverkar hur deltagarna upplever övningens relevans och nytta (Bradshaw, 2011). Realism är dock inte någon statisk mätbar egenskap, utan en framväxande egenskap, det vill säga deltagarens upplevda relation mellan de aktiviteter som genomförs och en professionell praktik (Barab m.fl., 2000). Denna relation består i hur applicerbara och användbara deltagaren upplever att aktiviteterna är baserat på deltagarens egna professionella kontext.

För att skapa relevans och realism behöver även mänskliga och organisatoriska relationer och beroenden simuleras (Henshel m.fl., 2016). Kopplat till realism är det pedagogiska perspektivet *autentiskt lärande* (authentic learning) särskilt relevant med hänsyn till cybersäkerhetsövningar. Enligt detta perspektiv ska lärandet relateras till en framtida användning i professionell praktik (Herrington, 2014). Utmärkande aspekter för autentiskt lärande beskriver Herrington (2014) till exempel som en autentisk kontext och uppgifter, tillgång till expertkunskap, möjlighet att anta olika roller och perspektiv, en samverkande konstruktion av kunskap samt möjlighet till aktiv reflektion kring det egna lärandet.

2.2.7 Generaliserbarhet och skalbarhet

Principen *generaliserbarhet och skalbarhet* syftar till att olika delar av övningskonceptet ska kunna återanvändas och anpassas efter behov. Generaliserbarheten relaterar till att övningskonceptets genomförande, det vill säga en övnings design, verktyg och aktiveter, ska gå att återanvända. Det ska även gå att anpassa genomförandet till olika sammanhang, till exempel med olika scenarier för olika typer av verksamheter. I principen finns således en idé om att övningsdesign och innehåll både är generiska och flexibla. Vad gäller den tekniska miljön innebär det att övningskonceptet fokuserar på att utveckla flexibla digitala system som är relevanta och applicerbara för olika verksamheter. Målet är att grunden i den tekniska miljön ska kunna återanvändas, och att delar kan bytas ut och nya delar integreras. En viktig aspekt i sammanhanget är att den tekniska miljön ska vara enkel att sätta upp och distribuera, oavsett om övningen genomförs på en fysisk plats eller på distans via fjärranslutning. Möjligheten att återanvända övningskonceptet är också en viktig aspekt när det kommer till resultat- och effektmätning, eftersom flera tillfällen för mätning över tid möjliggörs.

Skalbarhet handlar om att övningskonceptet främjar utveckling av övningar som kan anpassas och utökas för att passa olika sektorers och verksamheters behov. Vid planering av övning är det viktigt att få en bred representation av aktörer från aktuell sektor. Det kan handla om att anpassa till exempel inriktning, omfattning eller svårighetsgrad. Skalbarheten möjliggör även ett modulbaserat perspektiv, det vill säga att övningsdesignen kan delas upp i moduler som i sin tur kan kombineras eller användas separat beroende på varje aktuell behovsbild. Principen är tänkt att bidra till effektiv användning av resurser såsom tid, personal, ekonomi och teknisk miljö, samt till möjligheten att följa upp resultat och effekter på ett systematiskt sätt. Denna princip är ett svar på det inom forskningen beskrivna behovet av att en övningsdesign skall vara såväl skalbar (Gurnani m.fl., 2014; Kim m.fl., 2019; Prümmer m.fl., 2023) som flexibel (Mäses m.fl., 2021).

2.2.8 Lärande och effekt

Principen *lärande och effekt* innebär att övningar grundade på övningskonceptet inte bara har fokus på system och processer, utan också syftar till att förbättra deltagarnas framtida färdighet och förmåga att förebygga, upptäcka, hantera och lära av cyberhot och incidenter. Övningskonceptet baseras på olika pedagogiska perspektiv. Detta motiveras av ett tydligt framfört behov inom forskning och praktik kring utvecklad förståelse och kunskap om deltagarnas lärande vid cybersäkerhetsövningar (Karjalainen & Ojala, 2023). Det innebär även att övningskonceptet ligger till grund för övningar som inte är av prövande karaktär, det vill säga att konceptet inte handlar om att pröva och bedöma en enskild verksamhets incidenthanteringsförmåga. Istället utgör den genomförda övningen

en grund för deltagare och deltagande verksamheter att, baserat på sina erfarenheter, värdera insikter samt föreslå och omsätta förbättringar kring incidenthantering i den egna verksamheten. På detta sätt skapas möjlighet till större förankring och spridning samt framförallt större möjligheter att nå avsedd effekt för de verksamheter som övas.

Principen grundas i pedagogisk forskning och relaterar till pedagogiska perspektiv som till exempel *konstruktiv anpassning* (constructive alignment) (Biggs m.fl., 2022) och Blooms taxonomi (Krathwohl, 2002). Detta säkerställer även att innehåll och aktiviteter designas och anpassas enligt formulerade övningsmål med syfte att främja måluppfyllelse, samt att uppföljning av resultat och effekt även sker i enlighet med dessa mål. Ur det pedagogiska perspektivet kan cybersäkerhetsövningar även relateras till perspektiv på situationsbundet lärande (Clancey, 1995), aktivt lärande och erfarenhetsbaserat lärande (Kolb & Kolb, 2009), det vill säga att via reflekterad erfarenhet utveckla förändrade beteenden och handlingar hos deltagare och deltagande verksamheter.

2.2.9 Holism och tvärvetenskaplighet

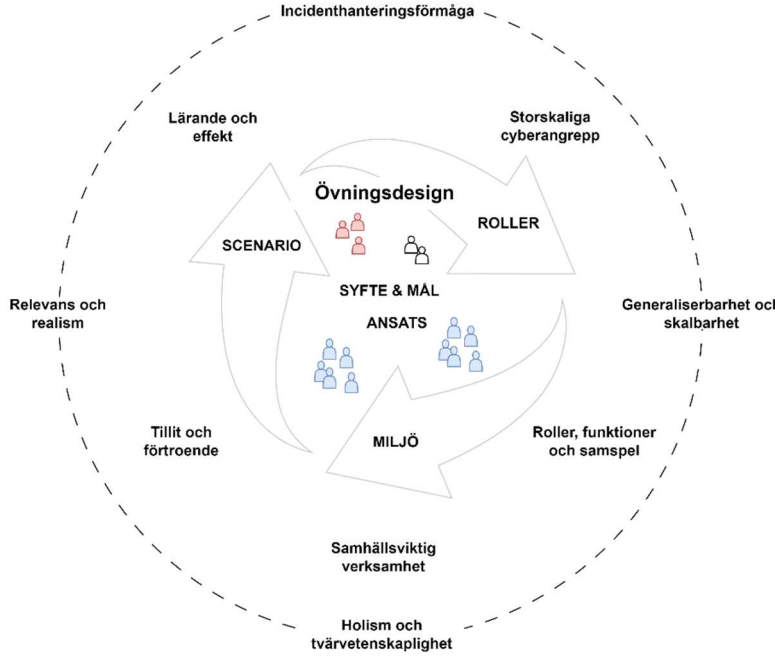
Principen *holism och tvärvetenskaplighet* innebär att övningskonceptet fokuserar på en integrering av kunskap, tekniker och metoder från olika vetenskapliga discipliner för att bättre kunna stärka deltagarnas förmåga att förebygga, upptäcka och hantera cyberhot och cyberangrepp, samt utveckla förmågan att lära av erfarenheter. Behovet av att på detta sätt se cybersäkerhetsdomänen som ett tvärvetenskapligt område är något som bekräftas av forskningen, och för fortsatt kunskapsutveckling behöver perspektiv från olika forskningsområden samverka (Craigen m.fl., 2014). Detta innebär en sammankoppling av forskningsområden inom till exempel pedagogik, teknik, psykologi, organisationsteori, juridik och ekonomi.

Cybersäkerhet är ett komplext fenomen och kan liknas vid ett socioteknisk system (Rajivan & Gonzalez, 2018), det vill säga ett system där både teknik och mänskliga aspekter ses som tätt interagerande och sammanvävda. Detta ställer i sin tur krav på såväl teknik, organisation som mänskliga aspekter. Det efterfrågas även holistiska perspektiv på cybersäkerhetsövningar (Nevmerzhitskaya m.fl., 2019) och i övningskonceptet betonas därmed att helheten av övningen är större än övningsdesignens enskilda delar. Detta säkerställer att samtliga delar och faktorer samspelar och att övningen designas, genomförs och följs upp på ett korrekt sätt.

2.3 Konceptskiss

Övningskonceptet ligger till grund för design och genomförande av övningar. För att ge en inledande förståelse för hur de grundläggande principerna påverkar

den övergripande övningsdesignen och olika designdelar presenteras en konceptskiss i Figur 2.



Figur 2. Konceptskiss övningskoncept

En cybersäkerhetsövning kännetecknas av en genomtänkt struktur och upplägg (Furtună m.fl., 2010; Seker & Ozbenli, 2018). Detta påverkar hur en övning designas och vilka delar som ingår. Vanligt förekommande designdelar är syfte och mål, ansats, scenario, roller och miljö. Designprocessen och dess ingående delar illustreras i flödesschemat i cirkelns mitt i Figur 2. I konceptskissen gestaltas även konceptets nio grundläggande principer som yttre faktorer som påverkar designprocessen. Varje princip i konceptet bidrar på olika sätt till övningsdesignen, där de principer som placerats i mellanrummet mellan cirklarna främst bidrar till specifika delar, medan de principer som placerats på den yttre cirkeln, på ett övergripande plan bidrar till övningsdesignen som helhet.

Principen *incidenthanteringsförmåga* kopplar till en övnings syfte och mål och är grunden för vilken ansats, det vill säga form och upplägg, som väljs för en övnings genomförande. Vad gäller en övnings ansats finns olika former och upplägg att tillgå, till exempel skrivbordsövningar, simuleringsövningar och skarpa övningar. Val av form och typ av övning påverkar andra designdelar såsom roller, scenario och miljö.

Principen *storskaliga cyberangrepp* bidrar likt föregående princip till designdelar som handlar om ansats, och anger ramarna för utveckling av scenario och miljö.

Principen hjälper till att identifiera hur den dimensionerande händelsen ser ut, det vill säga den händelse som deltagare bör förbereda sig på och planera för. Ur ett designperspektiv påverkar denna princip vilka tekniska angrepp som ska simuleras, och hur de ska utformas. Detta ställer i sin tur krav på den tekniska miljön som övningen är tänkt att genomföras i, hur ingående system och nätverk bör se ut, samt vilka verktyg som bör tillhandahållas för övervakning och kommunikation.

Principen *samhällsviktig verksamhet* bidrar främst till designdelar som handlar om scenario och miljö. Principen hjälper till att identifiera aktörer som upprätthåller grundläggande samhällsfunktioner och karaktärisera dessa aktörers verksamhet och behov. Resultaten ligger sedan till grund för framtagning av scenario och ”typverksamhet” utifrån vilket övningens scenario utgår ifrån. Resultaten ligger även till grund för verksamhetsmässiga anpassningar i den tekniska delen av övningsmiljön.

Principen *roller, funktioner och samspel* bidrar dels till designdelar som direkt handlar om roller, och dels till delar som handlar om ansats och scenario. Designdelar som berör roller kopplar till övningens övergripande syfte och mål och handlar om att identifiera vilka roller och funktioner som är relevanta att öva i sammanhanget. Samspel sätter fokus på ansvar och mandat kopplat till identifierade roller, vilket i sin tur påverkar hur man i en övning designar scenariot så att det främjar interaktion och kommunikation mellan dessa roller och funktioner. Det sistnämnda påverkar också val av metoder för kommunikation, vilket är en del av ansatsen. Ytterligare designdelar kopplade till roller sätter fokus på vilka roller som behövs i själva genomförandet av övningen. Större simuleringsövningar bygger ofta på inspel och kräver då roller som blå lag (de som försvarar) och rött lag (de som angriper), samt vitt lag (övningsledning).

Principen *tillit och förtroende* kopplar dels till designdelar som syfte och mål, det vill säga att de utgör ett mål med övningen i sig, och dels till delar som ansats och roller. Ansatsen är den designdel som är mest framträdande då det handlar om att säkerställa att former och upplägg för övningen främjar tillit och förtroende melllan deltagare, verksamheter och system. Det kan till exempel handlar om att lägga upp övningen på ett sådant sätt så att olika aktörer får möjlighet att redovisa hur och varför vissa aktioner genomförs på ett visst sätt.

Principen *lärande och effekt* är uppdelad i Figur 2 vilket har att göra med att det finns en inbördes relation mellan lärande och effekt, det vill säga att kunskap och färdigheter påverkar prestationer och resultat. Principen som helhet kopplar till designdelar som handlar om syfte, mål och ansats. Designdelar som berör syfte och mål handlar om att identifiera, specificera och avgränsa vad som ska övas, och vad övningen ska resultera i, det vill säga mätbara mål. Målen blir sedan styrande för vilka aktiviterer och vilket innehåll övningen bör ha, och hur dessa

realiseras och följs upp på ett ändamålsenligt sätt. Principen bidrar således till att säkerställa övningens övergripande ansats och design.

Till sist illustrerar den streckade cirkeln i Figur 2 de tre återstående principerna, det vill säga *relevans och realism*, *generaliserbarhet och skalbarhet*, samt *holism och tvärvetenskaplighet*. Tillsammans med incidenthanteringsförmågan påverkar och bidrar dessa principer på olika sätt till helheten vad gäller framtagandet av en övning och en specifik övningsdesign.

En sammanställning av designdelarna med dessas ursprung i principer samt tillämpning i form av designfrågor vid design av en ny övning presenteras i Tabell 2. Dessa designfrågor syftar därmed till att stödja och vägleda arbetet med att designa en övning. Detta ska se som ett exempel på hur grundläggande principer kommer att påverka den övergripande designen och praktiska tillämpningen i övningen.

Tabell 2. Principer, designdelar och exempel på designfrågor

Princip	Designdel	Exempel på designfrågor
Incidenthanteringsförmåga	Syfte och mål, ansats	- Vad inom incidenthantering är relevant att öva? Vem ska övas? Hur övas det på lämpligast sätt? - Hur ser målgruppens förutsättningar och behov ut? Hur avspeglas detta på ett ändamålsenligt sätt i övningsdesignen som helhet och i specifika delar?
Storskaliga cyberangrepp	Ansats, scenario och miljö	- Hur ser den dimensionerande händelsen ut som ligger till grund för utformning och planering av övningsupplägg och teknisk miljö? - Vilka metoder, verktyg och angreppssätt är ändamålsenliga för att simulera sofistikerade hotaktörer och avancerade och målinriktade hot och angrepp? - Hur designas narrativet och innehållet i övningen så att det framstår som realistiskt och relevant? Hur ser den tidigare händelseutvecklingen ut som leder fram till händelsen? Start, händelseförlopp, konsekvenser och slut? - Hur designas simulerade angrepp tekniskt? - Hur designas den virtuella miljön så att angrepp kan genomföras?
Samhällsviktig verksamhet	Scenario och miljö	- Vad karaktäriserar den typ av verksamhet som ligger till grund för övningen? Hur är den organiserad? Centrala aktörer, roller och perspektiv?

Princip	Designdel	Exempel på designfrågor
		- Hur designas scenarier som är anpassade efter sektorns typiska verksamhet?
Roller, funktioner och samspel	Roller, ansats och scenario	- Vilka aktörer, roller och funktioner är relevanta att ha med? - Vilka metoder är ändamålsenliga för att främja samspel mellan aktörer? - Hur skapas scenarier på ett ändamålsenligt sätt, som tydliggör ansvar, mandat och samverkanspunkter mellan olika aktörer och identifierade roller och funktioner? - Vilka roller och funktioner behövs vid genomförande av övning?
Tillit och förtroende	Syfte och mål, ansats, roller	- Hur ser en övningsdesign som främjar tillit och förtroende mellan deltagare och till systemet ut? - Vilka aktiviteter, metoder och verktyg behövs för att skapa förtroende mellan aktörer för att främja en vilja att dela information med varandra?
Relevans och realism	Syfte och mål, ansats, scenario, roller och miljö	- Hur säkerställs att innehåll, aktiviteter och verktyg i övningen speglar verkligheten? Behöver alla delar i övningen ha samma grad av realism eller finns det specifika delar som behöver fokuseras? - Hur byggs en teknisk övningsmiljö som upplevs som realistisk och relevant av målgruppen?
Generaliserbarhet och skalbarhet	Syfte och mål, ansats, scenario, roller och miljö	- Hur säkerställs att övningsdesign, tekniska övningsmiljöer och aktiviteter är tillämpbara på olika typer av organisationer? - Hur säkerställs att övningsdesignen är skalbar och anpassningsbar? Hur designas specifika delar, aktiviteter, innehåll eller resultat som skalbara?
Lärande och effekt	Syfte och mål, ansats	- Vilka uppgifter, kunskap och färdigheter är ändamålsenliga och hur kan dessa omsättas i lärandemål och övningsmål? - Hur följs mål upp och säkerställs i aktiviteter, innehåll och resurser på ett ändamålsenligt sätt? - Vilka förkunskaper förväntas deltagarna ha? - Vad behövs i form av förberedelser för att deltagarna ska få ut mesta möjliga av övningen?

Princip	Designdel	Exempel på designfrågor
Lärande och effekt forts.		- Hur utvärderas deltagarnas prestationer på ett ändamålsenligt sätt? - Hur mäts effekterna av övningen på ett ändamålsenligt sätt? Vilka metoder behövs för att följa upp effekter på kort och lång sikt?
Holism och tvärvetenskaplighet	Syfte och mål, ansats, scenario, roller och miljö	- Vilka kompetensområden och perspektiv är relevanta i sammanhanget? Vilken typ av övning är ändamålsenlig för att uppnå syfte och mål? Hur påverkar ansatsen övningens omfattning? - Hur säkerställs en holistisk övningsdesign som integrerar identifierade perspektiv och områden på ett ändamålsenligt sätt?

3 Ragnarök

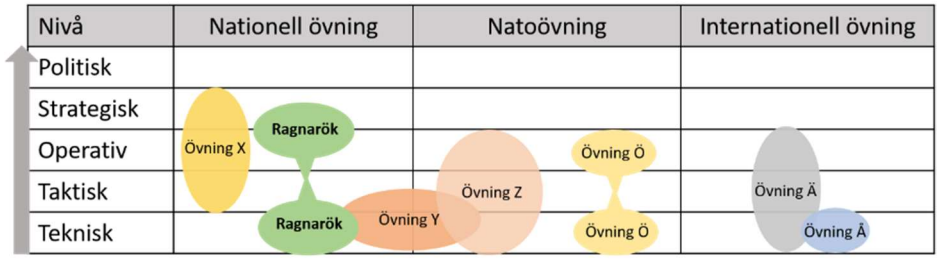
Detta kapitel presenterar hur den bärande idén och principerna i övningskonceptet kan konkretiseras i form av en övning, i detta sammanhang benämnd som Ragnarök[4]. Ragnarök ska ses som en exempelövning, det vill säga ett exempel på hur en övningsdesign baserad på övningskonceptet kan se ut. Övningskonceptet är dock inte begränsat till endast denna typ av design.

3.1 Övningsdesign

Övningsdesign innebär i detta sammanhang en beskrivning av Ragnaröks uppbyggnad, struktur och plan för genomförande. I designen beskrivs grundläggande övningsdelar såsom syfte och mål, ansats och genomförande, scenarier och miljöer på ett övergripande plan. Observera att detta ska ses som en initial övergripande design, som sedan specificeras och preciseras under planering och utveckling.

3.1.1 Övergripande syfte och ansats

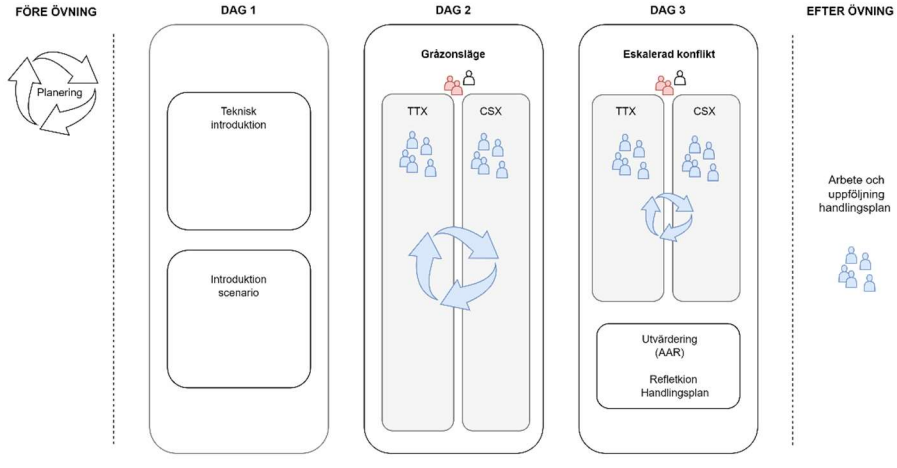
Ragnarök utgår från övningskonceptets bärande idé om en övning i incidenthantering där syftet är att stärka Sveriges förmåga att förebygga, upptäcka och hantera cyberhot och cyberangrepp, samt lära av angrepp och incidenter. För att uppfylla syftet omfattar övningen en del på strategisk operativ nivå, och en del på teknisk operativ (taktisk) nivå när det kommer till incidenthantering. Ragnarök är en nationell övning och riktar sig till samhällsviktig verksamhet, och primärt till ett antal prioriterade sektorer. Övningen ska därmed ses som ett komplement till andra övningar som ges inom cybersäkerhets- och cyberförsvarsområdet, vilket illustreras i Figur 3.



Figur 3. Nivå och övningskontext för övningar inom cybersäkerhets- och cyberförsvarsområdet.

[4] Denna benämning motiveras genom att Ragnarök kan ses som en metafor för att något nytt och bättre kan växa ur det gamla som fallit; i detta fall en stärkt förmåga att förebygga, upptäcka och hantera cyberhot och cyberangrepp.

Ragnarök bygger på ett samspel mellan den strategiskt operativa delen och den tekniskt operativa delen av övningen, och deltagarna är därmed indelade i CSX-lag respektive TTX-lag (se Figur 4). Ansatsen är en simuleringsövning av typen rött lag och blått lag-övning och designen bygger på ett genomförande under tre dagar. Den första dagen är avsatt till att förbereda och sätta in deltagarna i den tekniska miljön (*teknisk introduktion* i Figur 4) och i narrativet som övningen tar utgångspunkt i (*introduktion scenario* i Figur 4). Dessa förberedande aktiviteter är viktiga för att deltagarna ska ha inhämtat de förutsättningar som behövs vid övningens början. Övningsdesignen bygger på att den fiktiva verksamhet som deltagarna övar i, i enlighet med övningskonceptet, tas fram i dialog med berörda parter i samband med planering och utveckling av övningen. Övningen föregås därmed av en planering och utveckling, vilket illustreras av fasen *före övning* till vänster i Figur 4.



Figur 4. Övergripande övningsdesign med strategiskt operativ och tekniskt operativ del.

Under dag två, och merparten av dag tre, genomförs själva övningen (markerat med grått i Figur 4). Ragnarök består av aktiviteter som fokuserar på hanteringen av ett antal inspel, det vill säga simulerade cyberangrepp, som bygger på verkliga händelser och cyberangrepp i ett komprimerat format. Dessa inspel följer en detaljerad plan och utgör grunden för förväntade deltagaraktiviteter. I formatet ligger också att tidshopp, det vill säga en framflyttning i tid enligt en fördefinierad tidslinje, genomförs under övningen, vilket i sin tur förändrar förutsättningar och påverkar deltagare på olika sätt. Syftet är att simulera olika trovärdiga och realistiska scenarier så att deltagarna får erfara så många olika aspekter av incidenthantering under övningen som möjligt. Detta gör deltagarna bättre rustade om något liknande inträffar i verkligheten. Ragnarök avslutas med en utvärdering eller efteranalys (After Action Report, AAR) av genomförda aktiviteter och insatser. Detta genomförs för att identifiera vad som har fungerat

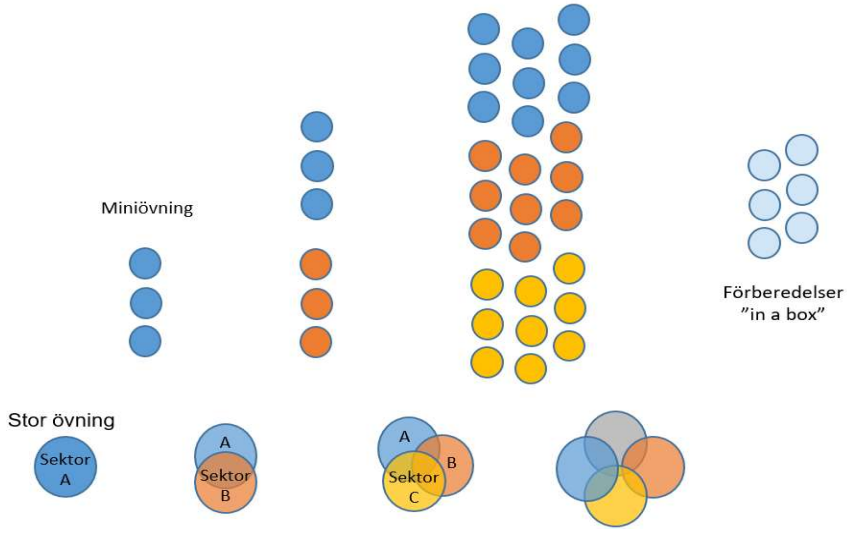
bra och vad som hade kunnat förbättras och är därmed ett viktigt sätt för att erhålla återkoppling från övningen. Denna aktivitet ses även som ett gemensamt tillfälle för lärande där deltagarna tillsammans med utförare av övningen har möjlighet att dela erfarenheter och insikter kopplat till incidenthantering.

Ragnarök förutsätter att deltagarna har kunskap och färdigheter inom incidenthantering baserat på olika perspektiv (mer detaljer framgår under avsnitt 3.2.1.1 och 3.2.2.1). Under övningen tillämpas kunskap och färdigheter för att deltagarna sedan ska kunna reflektera och värdera dessa i relation till sin roll och arbetsuppgifter i ordinarie verksamhet. Målet är att övningen resulterar i ett fortsatt arbete med en handlingsplan. Arbetet med handlingsplanen påbörjas i samband med övningens genomförande, men merparten av arbetet sker i efterhand i deltagarnas ordinarie verksamhet. Detta illustreras genom fasen *efter övning* i Figur 4. Handlingsplanen är en plan som beskriver hur insikter och lärdomar tas vidare, omsätts och förbättrar den egna verksamheten (se vidare avsnitt 3.3.3). I detta ingår även att arbetet handlingsplanen följs upp i syfte att utvärdera och säkerställa övningens effekt.

En viktig aspekt av den övergripande designen är att delar av designen ska kunna brytas ut och tillhandahållas som enskilda moduler. Denna design möjliggör till exempel att inspelen som genomförs dag 2 och 3 kan brytas ut och genomföras som enskilda moduler, så kallade ”miniövningar”, och på så vis nå en potentiellt bredare målgrupp. Den finns även möjlighet att bryta ut den tekniskt operativa delen (CSX) respektive den strategiskt operativa delen (TTX) av Ragnarök och genomföra dessa var för sig. Det finns även idéer om att delar av förberedelsearbetet ska kunna distribueras som förpaketerade ”in-a-box”-övningar, det vill säga som en paketlösning.

Figur 5 illustrerar hur övningsmoduler bidrar till övningens skalbarhet och spridning inom ett antal sektorer. Varje färg representerar en enskild sektor, och att det regelbundet (till exempel en gång per år) designas en ny sektorsanpassad version som läggs till i övningen. I takt med att övningskonceptet och övningar vidmakthålls och vidareutvecklas, finns således även möjlighet att på sikt erbjuda sektorsspecifika miniövningar. I Ragnarök är tanken att övningen till att börja med ska genomföras fysiskt på plats, men i övningskonceptet finns inga

begränsningar för att även genomföra övning eller delar av övning i ett distribuerat format.

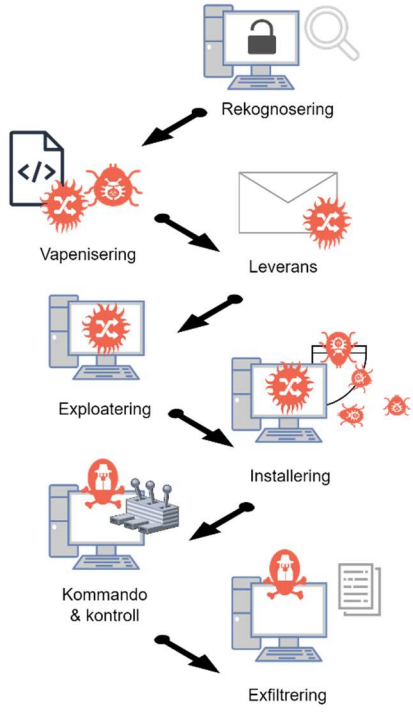


Figur 5. Skalbarhet och modularisering övning.

3.1.2 Scenarier och inspel

Storskaliga antagonistiska cyberhot och cyberangrepp mot samhällsviktig verksamhet utgör dimensionerande händelser för övningen. Ragnaröks scenarier och inspel bygger således på de mest kritiska händelserna som kan drabba samhällskritiska system och är inspirerade av verkliga händelser samt FOI-rapporten *Gråzonslägen i krig och fred* (Jonsson m.fl., 2023). Exempel på händelser kan vara omfattande ransomware-attacker eller cyberangrepp som utnyttjar sårbarheter i system, infekterar nätverk och krypterar kritisk data eller röjer känslig information.

Storskaliga antagonistiska cyberangrepp är följaktligen utgångspunkten för den övergripande berättelsen i Ragnarök och utgör grunden för scenarier och utveckling av inspel. Angreppen är designade att följa en attackkedja, det vill säga att följa en tydlig tidslinje och innefattar olika attackfaser och nyttjandet av olika attackvektorer samt fokuserar på tydliga målsystem för att resultera i tydliga verksamhetsmässiga konsekvenser (se Figur 6). Nyttjade händelsekedjor och attacker redovisas och reflekteras över i samband med utvärderingen i slutet av övningen. Denna utvärdering är en viktig möjlighet till lärande för deltagarna att förstå och lära av cyberhot, cyberangrepp och incidenter. Användningen av dimensionerande händelser vid design av en övning enligt övningskonceptet är således ett effektivt sätt att förbereda deltagarna på olika sannolika situationer.



Figur 6. Exempel på faser i en attackkedja.

3.1.3 Grundscenario och sektorsspecifika scenarier

Givet den dynamiska utvecklingen av cyberhot och cyberangrepp visar forskning att det finns behov av att arbeta flexibelt med scenarioframställning, och det handlar därmed om att ta fram scenarier som är anpassningsbara och öppna för förändring (Yamin & Katt, 2022). Ett scenario beskriver situationen som övningen försöker simulera och logiken i händelseförloppet (Grance m.fl., 2006; Wen m.fl., 2021). Ett scenario innehåller den digitala miljön i vilken övningen utspelar sig och beskrivningar av situationer, händelser och inspel som deltagarna kommer att behöva hantera. I Ragnarök ingår ett grundscenario som sedan kompletteras med olika sektorsspecifika scenarier.

Grundscenariot utgör en bas och beskriver det sammanhang som alla sektorsspecifika scenarier förhåller sig till, och utgör således den sammanhållande länken för olika sektorspecifika inspel. I Ragnarök utgår grundscenariot från en kommunal kontext och i denna kontext finns alla samhällsviktiga verksamheter som är i fokus för övningen representerade. Exempel på sådana är post- och telekommunikation, energiförsörjning, vatten och avlopp, transport och finans. Det finns även andra viktiga verksamheter

representerade som sjukvård, försvarsindustri och militär verksamhet. Grundscenariot beskriver narrativet, eller inramningen till övningen, det vill säga den struktur som organiserar information och händelser till en sammanhängande form. Grundscenariot bygger även på presenterade idéer om dimensionerande händelser, det vill säga det händelseförlopp som har lett fram till det läge och den utgångspunkt som startar själva övningen.

Sektorsspecifika scenarier är till för att skapa ytterligare realism i Ragnarök. Dessa scenarier karaktäriseras av att de utgår från en för sektorn generisk verksamhet till exempel de fiktiva företagen Nordkraft Energi AB, TeleNet Solutions AB eller FinanZen AB. Dessa verksamheter är en sorts genomsnittliga verksamheter som illustrerar det verksamhetsmässiga sammanhanget i vilken händelserna sker. Varje sektorsspecifikt scenario beskriver verksamheten och vad som är skyddsvärt i denna. Sektorsspecifika scenarier tas fram tillsammans med representanter från berörda sektorer och kan handla om att identifiera konsekvenser av skador, aktuella hot och olika typer av incidenter, samt identifiera skyddsvärden. Målet är att skapa ett så realistiskt och trovärdigt scenario som möjligt för deltagarna. Scenariot ligger sedan till grund för anpassningar i den tekniska miljön och de tekniska inspelen.

3.1.4 Generisk teknisk miljö

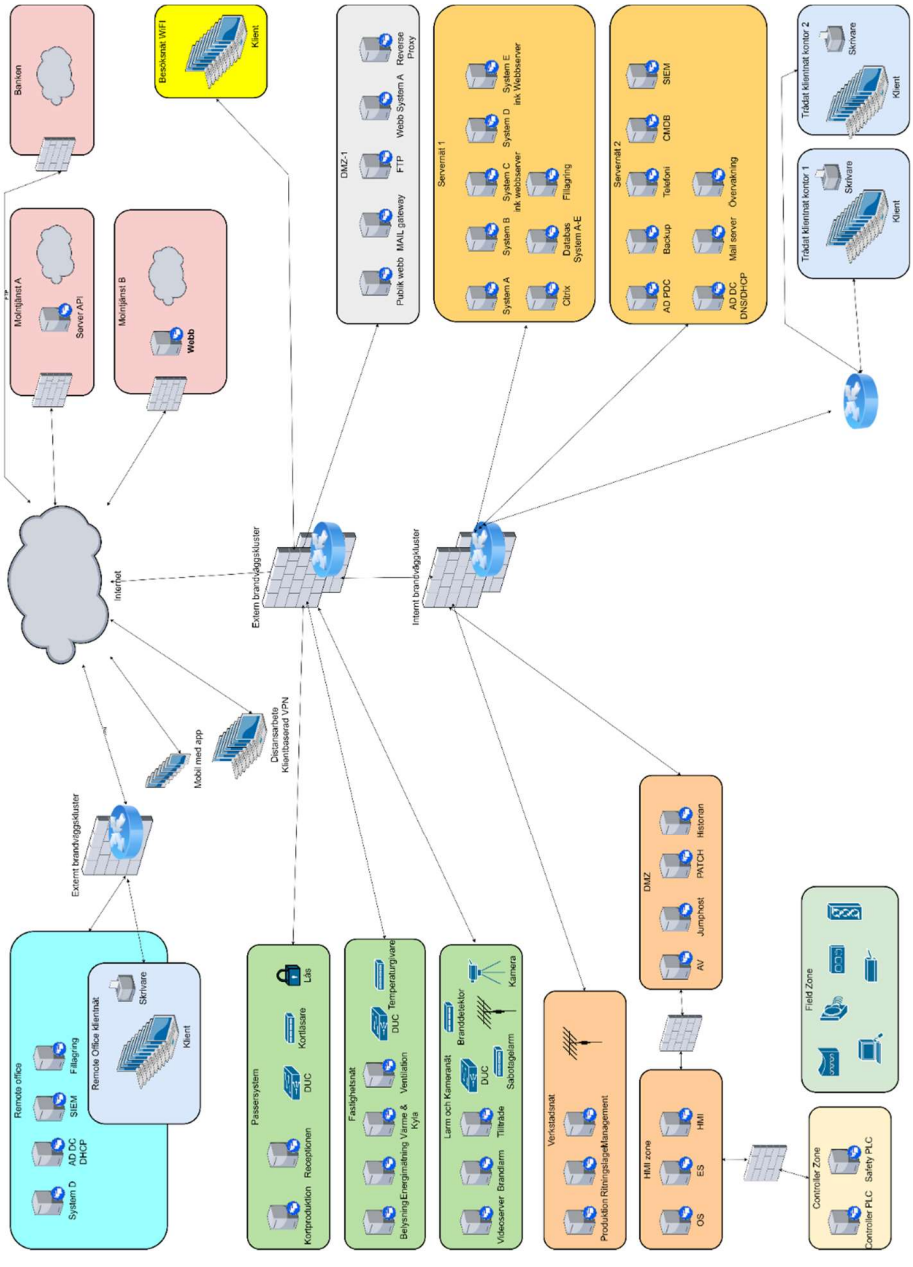
Ragnaröks tekniska miljö tar utgångspunkt i en fiktiv verksamhets IT-miljö och är generisk i sin karaktär. Forskning visar att det är både kostsamt och utmanande att designa och utveckla tekniska miljöer och scenarier som är anpassade efter olika samhällskritiska verksamheters behov (Kim m.fl., 2019). Med anledning av detta bygger övningskonceptet på att en generisk teknisk miljö ligger till grund för övningar (se Figur 7).

IT-miljön bygger på en generisk bild av ett kontorsnät (till höger i Figur 7). OT-miljön innehåller styrsystem som förväntas vara gemensamma för flertalet verksamheter, det vill säga fastighetsnät med värme och kyla, ventilation, energimätning, belysning, passersystem och larm samt övervakning (till vänster i Figur 7). Samhällsviktiga verksamheter har utöver dessa styrsystem olika kritiska styrsystem, system som till exempel reglerar och styr eldistribution och elproduktion, övervakar och hanterar nätverkstransmission. Den generiska tekniska miljön omfattar inte dessa typer av styrsystem, men de utgör en viktig del i de sektorsspecifika scenarierna, det vill säga narrativen kring vad det är som deltagarna förväntas skydda.

Det som karaktäriserar den generiska tekniska miljön är att den är (1) grundsäker, (2) bygger på olika hierarkiska nivåer med standardiserade gränssnitt

och protokoll (jfr Purdue-modellen[5]), (3) innehåller olika kritiska flöden, (4) bygger på öppen och/eller standardiserad programvara samt (5) simulerar normal nätverkstrafik, såväl användargenererad trafik som automatiserade flöden. Att miljön är grundsäker handlar om att det finns säkerhetslösningar på plats, vilket till exempel kan handla om segmentering, brandväggsregler med mera. För att stärka realismen simuleras även ett tekniskt arv, vilket till exempel kan innebära att äldre system behållits i drift på grund av kostnadsskäl. Figur 7 illustrerar den tekniska miljöns arkitektur och hur olika komponenter i verksamhetens IT- och OT-miljö är tänkta att samverka med varandra. Arkitekturen är designad utifrån olika lager, det vill säga från infrastrukturlager till verksamhets- och användarlager samt tjänstelager. Detta gör den generiska tekniska miljön återanvändbar och anpassningsbar.

[5] Ett hierarkiskt ramverk som fokuserar säkerhet och segmentering inom ICS och OT.



Figur 7. Generisk teknisk miljö. Illustration: Ralf Alvarsson och Jonas Wiman, FOI

3.1.5 Generella övningsmål

Ragnaröks övningsmål är framtagna med inspiration från ett pedagogiskt perspektiv på lärandemål. Arbetet med lärandemål har hjälpt till att inrikta övningen med fokus på vad deltagarna förväntas uppnå efter genomgången övning (Seker & Ozbenli, 2018). Genom att formulera lärandemålen som övningsmål har även ett skifte i fokus skett från att mäta och utvärdera individuella prestationer, till att mäta och värdera effekter av övning (se vidare avsnitt 3.3). Det har även funnits behov av att formulera övningsmål på en mer generell nivå, samtidigt som det finns övningsmål som är mer specifikt inriktade på övningens olika delar, det vill säga strategiskt operativa mål och tekniskt operativa mål. De generella övningsmålen motiveras därmed dels genom att undvika överlappande övningsmål, och dels genom att de berör högre kognitiva processer och aspekter som är relevanta för samtliga delar av övningen. Dessa övningsmål syftar till exempel till en utvecklad förmåga att reflektera kring olika aspekter av övningen. De övningsmål som formulerats per del (TTX och CSX) berör procedurell och faktabaserad utveckling av kunskap och förmåga och är specifik för respektive del av övningen (se avsnitt 3.2.1.2 och 3.2.2.2). Denna uppdelning är även förankrad i pedagogisk forskning med hänsyn till olika kognitiva dimensioner av lärande (t.ex. Krathwohl, 2002). Som generella övningsmål förväntas deltagaren ha stärkt sin förmåga att:

- definiera och reflektera kring roller och ansvar
- reflektera kring återställning och kontinuitetshantering
- identifiera och analysera hanteringen av incidenter efter övning
- identifiera och reflektera kring lärdomar från övning
- formulera och dokumentera förslag till förbättringar i egen verksamhet
- reflektera kring eskalering av hotbilder och angrepp

3.2 Övningens delar

I avsnittet presenteras Ragnaröks två ingående delar mer i detalj, det vill säga incidenthantering på strategisk och teknisk nivå. Målgrupp och förkunskapskrav, övningsmål samt innehåll och aktiviteter beskrivs för respektive del.

3.2.1 Incidenthantering strategisk nivå (TTX)

Incidenthantering på strategisk nivå är den strategiska delen av Ragnarök med syftet att bidra till att stärka Sveriges operativa strategiska förmåga att förebygga, upptäcka och hantera cyberhot och cyberangrepp, samt lära av angrepp och incidenter. Målet är att förbättra den strategiska beredskapen för cyberhot och incidenter hos deltagande personer och deltagande verksamheters förmåga att hantera storskaliga cyberangrepp.

3.2.1.1 Målgrupp och förkunskapskrav

Den strategiska delen av Ragnarök vänder sig till personer som arbetar i beslutsfattande positioner och roller och andra funktioner som är viktiga när det kommer till krisledning vid en cyberincident i samhällsviktig verksamhet. Exempel på roller deltagarna kan inneha är insatschefer, personer med operativt ansvar vid krishantering, tekniska ledare, informationssäkerhetschefer, kontinuitetsplanerare, juridiska rådgivare, HR-chefer samt kommunikatörer. Deltagarna i den strategiska delen av övningen förutsätts ha kunskap, färdighet och erfarenhet inom något eller några av följande områden:

- krisledning, krishantering och krisplanering
- cybersäkerhet och cyberhot inklusive verktyg och metoder
- lagar och regler kopplat till cybersäkerhet[6]
- komplexa problem och beslutsfattande under press
- ledarskap, rapportering och kommunikation.

3.2.1.2 Övningsmål TTX

Övningsmålen nedan illustrerar de strategiskt operativa förmågor som Ragnarök har fokus på att utveckla och som är styrande för upplägg och genomförande av övningens strategiska scenarier och inspel. Efter genomgången övning förväntas deltagaren i TTX-delen ha stärkt sin förmåga att:

- leda och koordinera incidenthantering på strategisk nivå i samhällsviktig verksamhet
- inhämta och värdera underrättelse av betydelse för verksamheten
- identifiera och värdera interna och externa sårbarheter
- koordinera och prioritera agerande vid incidenthantering
- sammanställa, kommunicera och rapportera incidenter till berörda instanser
- agera i enlighet med planer, avtal, lagar och förordningar
- värdera och hantera beroenden till externa intressenter och andra påverkande faktorer
- reflektera kring verksamhetens incidenthanteringsplan
- reflektera kring utmaningar vid beslutsfattande vid incidenthantering.

Förutom att vara styrande för utveckling av inspel och scenarier i den strategiska delen av Ragnarök är målen också styrande för utvärdering och mätning av övning och dess effekter. Målen är framtagna för att efterlikna uppgifter som

[6] Exempel på lagar och regler: Säkerhetsskyddslagen (2018:585), Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174), NIS-direktivet (2016/1148), NIS 2-direktivet (2022/2555), Cybersecurity Act (EU-förordning 2019/881), CER-direktivet (2022/2557)

genomförs i verkliga situationer och tydliggör vad som förväntas av deltagarna under övningen.

3.2.1.3 Innehåll och aktiviteter

Den operativt strategiska delen av Ragnarök innehåller således ett antal planerade inspel som simulerar olika verkliga händelser, allt ifrån kontakter med media, leverantörer och andra intressenter till intern kommunikation med den tekniska incidenthanteringsledningen. De angrepp och incidenter som förekommer kan handla om allt ifrån att någon obehörig får tillgång till verksamhetens interna nätverk och stjäl känslig data, till överbelastning och sabotage av system. Deltagarna på strategiska nivån förväntas öva i sina ordinarie roller, och genomföra uppgifter som handlar om att upprätta och upprätthålla lägesbilder, fatta beslut om eskalering av incidenter och åtgärder, samt på ett övergripande plan koordinera och leda hanteringen av incidenterna utifrån den simulerade verksamhetens perspektiv.

3.2.2 Incidenthantering teknisk nivå (CSX)

Incidenthantering på teknisk nivå är den tekniskt operativa delen av Ragnarök och målet med denna del är att förbättra den tekniska beredskapen för cyberhot och incidenter hos deltagande personer och stärka deltagande verksamheters förmåga att tekniskt hantera storskaliga cyberangrepp och incidenter.

3.2.2.1 Målgrupp och förkunskapskrav

Den tekniska delen av Ragnarök vänder sig till personer som arbetar med teknisk incidenthantering och cybersäkerhet framförallt inom IT, ICS och OT i samhällsviktig verksamhet. Exempel på roller deltagarna kan ha är tekniska incidentledare eller samordnare, nätverksexperter och tekniker, systemarkitekter, systemadministratörer, säkerhetsspecialister och analytiker samt tekniska skribenter eller dokumentatörer av incidenter. Deltagare i den tekniska delen av övningen förutsätts ha goda kunskaper inom något eller några av följande områden:

- teknisk ledning och incidenthantering
- säkerhets-, sårbarhets- och hotanalys
- nätverk, nätverksövervakning och nätverkssegmentering
- brandväggar, brandväggskonfiguration och brandväggsregler
- IDS-system och system för att förhindra intrång
- logganalys
- dokumentation, visualisering och rapportering av incidenter och åtgärder.

Det är även en fördel om deltagaren har kännedom om, eller vana av, att hantera olika verktyg kopplat till incidenthantering.

3.2.2.2 Övningsmål CSX

Övningsmålen nedan illustrerar de tekniskt operativa förmågor Ragnarök har fokus på att utveckla när det kommer till hantering av cyberhot och incidenter. Målen ligger till grund för upplägg och genomförande av den tekniska delen av övningen, det vill säga olika tekniska inspel. Efter genomgången övning förväntas deltagaren i CSX-delen ha stärkt sin förmåga att:

- leda och koordinera incidenthantering på teknisk nivå i samhällsviktig verksamhet
- leda och koordinera arbetet i incidenthanteringsteam
- övervaka nätverk, kritiska processer och dataflöden
- identifiera onormal nätverksaktivitet och potentiella hot
- identifiera och värdera incidenter i realtid
- analysera och bedöma incidenters omfattning, angelägenhet och påverkan (triage)
- hantera cyberangrepp och incidenter enligt ett givet arbetssätt (avgränsa, avlägsna, återställ)
- sammanställa och kommunicera aktuella lägesbilder av incidenter
- sammanställa, dokumentera och rapportera incidenter (innefattar tidslinjer, målsystem och systemeffekter)
- värdera och föreslå lämpliga säkerhetsåtgärder
- säkerställa överlämning av information mellan incidenthanteringsteam.

Även dessa mål är styrande för utvärdering och mätning av övningen och dess effekter, och är framtagna för att efterlikna uppgifter som genomförs i verkliga situationer. Målen tydliggör därmed vad som förväntas av de tekniska deltagarna under övningen.

3.2.2.3 Innehåll och aktiviteter

Den operativt tekniska delen av Ragnarök innehåller ett antal utvecklade inspel. Dessa inspel är inspirerade av, och simulerar, olika typer av verkliga attacker och

angrepp till exempel Stuxnet[7], NotPetya[8] och WannaCry[9]. Varje inspel imiterar en eller flera attackkedjor (se Figur 6). Enligt övningsmålen övas deltagarna i att identifiera onormal aktivitet, reagera på olika steg i attackkedjan, få djupare insikt i hur angrepp genomförs samt upptäcka sårbarheter och säkerhetsbrister i den tekniska miljön. Inspel kan handla om allt ifrån att någon utomstående får tillgång till den fiktiva verksamhetens interna nätverk och stjäl känslig data, till överbelastning och sabotage av system. Under övningen förväntas deltagarna utföra aktiviteter som till exempel att:

- övervaka system och nätverk
- analysera händelser och identifiera incidenter
- upprätta loggböcker och dokumentera händelser
- hantera, begränsa och förhindra spridning av skadlig kod
- ta bort skadlig kod och säkra system
- föreslå åtgärder och kommunicera relevant information till relevanta parter
- rapportera incidenter till berörda instanser.

3.2.3 Samspelet CSX och TTX

Forskning pekar på vikten av att öva krisledningsförmågor som är kopplade till hantering av cyberkriser på nationell nivå (Kim m.fl., 2019), det vill säga antagonistiska storskaliga angrepp mot kritisk infrastruktur. På ett övergripande plan handlar det om att öva kriskommunikation som understödjer snabbt och korrekt beslutsfattande när det kommer till angrepp som kan leda till allvarliga konsekvenser i form av omfattande samhällsstörningar som kan påverka Sveriges säkerhet. I Ragnarök möjliggörs interaktion mellan den operativa strategiska delen (TTX) och den operativa tekniska delen (CSX). Genom att låta TTX och CSX samspela förväntas deltagarna få en utvecklad förståelse för både verksamhetsmässiga och tekniska aspekter av incidenthantering. Ett tydligt sätt att möjliggöra och stärka denna samverkan är att tillse att beslutsfattande kräver en integrering av såväl tekniskt operativ som strategiskt operativ nivå.

Det är även viktigt att båda delarna av övningen på ett tydligt sätt har gemensamma mål och att dessa mål formuleras på ett sätt så att den operativa

[7] Stuxnet är ett avancerat datavirus som upptäcktes 2010. Det skapades för att sabotera Irans kärnprogram genom att angripa industriella styrsystem och förstöra centrifuger i kärnanläggningen i Natanz. Viruset tros ha utvecklats av USA och Israel.

[8] NotPetya är samling malware som först upptäcktes 2016 och som utgav sig för att vara ransomware men i själva verket var utformad för att förstöra data. Den riktades främst mot Ukraina men spred sig globalt och orsakade stora ekonomiska skador.

[9] WannaCry är en global ransomware-attack från 2017 som utnyttjade en sårbarhet i Windows för att låsa datorer och kräva lösensumma i Bitcoin. Den drabbade bland annat sjukhus, företag och myndigheter världen över.

och strategiska nivån korsas. Detta innebär till exempel att samma mål för övningen delas av CSX och TTX (se avsnitt 3.1.5), och att CSX därmed med tydlighet ser sin roll i relation till verksamhetsövergripande och strategiska aspekter. Det är även viktigt att tillse att det finns en tydlig parallellitet och ömsesidig påverkan mellan teknisk incidenthantering i CSX-delen, och strategiskt beslutsfattande i TTX-delen av övningen. I Ragnarök har således aktiviteter och inspel designats på ett sätt som tvingar fram samspelet till exempel i form av att CSX löpande ska rapportera till TTX under övningen, och att detta potentiellt resulterar i beslut från TTX som även påverkar CSX arbete. Ytterligare ett sätt som har applicerats i Ragnarök och som är effektivt, är att ha gemensamma utvärderingar, diskussioner och reflektionspass med samtliga deltagare efter övning.

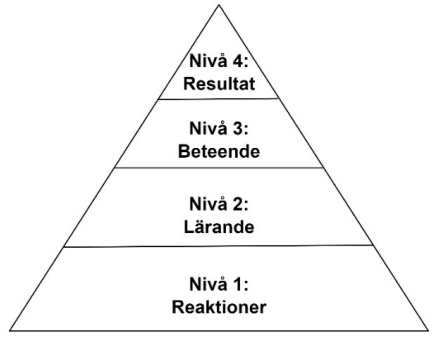
3.3 Effekt och effektmätning övning

Avsnittet om effekt och effektmätning fokuserar på hur Ragnaröks förväntande nytta säkerställs och hur uppföljning av resultat på olika nivåer sker. Den förväntade effekten kopplar i sin tur till övningskonceptet och hur väl de grundläggande principerna har omsatts i övningens design, innehåll och aktiviteter samt hur väl de bidrar till att uppfylla den bärande idén och det övergripande syftet.

3.3.1 Effektmätning

Cybersäkerhetsövningar strävar efter att påverka såväl individers som verksamheters färdigheter och förmåga att hantera cyberhot och cyberangrepp. Som en relevant utgångspunkt för att mäta övningens avsedda effekt i deltagarens verksamhet föreslås Kirkpatrick-modellen (t.ex. Karjalainen m.fl., 2019). Valet motiveras av att denna modell bedöms som enkel och tydlig, har en tydlig struktur, är väletablerad samt fokuserar på såväl individ som organisation. Modellen utgår från de fyra nivåerna reaktioner, lärande, beteende samt resultat. Modellen skapades ursprungligen för att utvärdera effekter av träning (Kirkpatrick, 1996) (se Figur 8). I Kirkpatrick-modellen syftar den första nivån (reaktioner) på att fånga deltagarnas känslor och upplevelser av olika aspekter i direkt anslutning till övningen. Nivå två (lärande) avser individens (deltagarens) förbättrade färdigheter, förmågor och utvecklad kunskap som kan spåras till övningstillfället. Nivå tre (beteende) syftar till att mäta och utvärdera om övningen får avsedd effekt på individnivå, det vill säga resulterar i reella beteendeförändringar i enlighet med övningens mål. Den fjärde och sista nivån (resultat) avser positiva effekter i deltagarens ordinarie verksamhet som helhet (Kirkpatrick, 1996). Traditionellt sker en uppföljning, till exempel via deltagarenkäter, i direkt anslutning till övningstillfället, det vill säga den första nivån i Figur 8 (reaktioner). Även om detta är relevant riskerar denna uppföljning främst att fokusera på deltagarnas reaktion och upplevelse av övningstillfället,

snarare än hur övningen potentiellt påverkar deltagaren i dennes ordinarie arbetssituation.



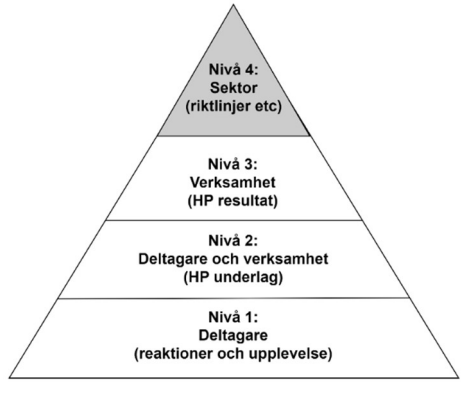
Figur 8. Kirkpatrick-modellen för utvärdering av effekter av träning. Egen figur anpassad efter Ahmad m.fl. (Ahmad m.fl., 2015, s. 4 egen översättning)

Mätning av effekten har även inspirerats av ansatsen effektmätning (t.ex. Patton, 1997). Effektmätning kan beskrivas som en systematisk utvärdering och kvantifiering av effekter av någon typ av insats för att förstå dess påverkan och effekt i olika sammanhang, till exempel på individ-, organisations- eller samhällsnivå. Med hänsyn till övningen blir därmed effektmätning en systematisk ansats för att bedöma vilken inverkan eller effekt Ragnarök har med hänsyn till uppfyllnad av övningskonceptets bärande idé och grundläggande principer. Den anpassade typ av effektmätning som kommer appliceras inom Ragnarök bygger i sin tur på följande principer: (1) ett lärande som leder till förväntad förändring, (2) att mätbara indikatorer identifieras, (3) att mätning genomförs vid olika tidpunkter samt (4) att uppföljning genomförs på olika lång sikt. För att mäta övningens effekt behövs även olika typer av underlag som i sig blir bärare för de mätbara indikatorer som mäts och följs upp. Det sammanhang mätningen genomförs i, och objektet för respektive mätning för varje steg i processen, har även en påverkan och behöver definieras tydligt. I Tabell 3 visas mätobjekt per nivå baserat på Kirkpatrick-modellen.

Tabell 3. Mätobjekt per nivå i Kirkpatrick-modellen

#	Nivå	Mätobjekt
1	Reaktioner	Deltagare
2	Lärande	Deltagare/verksamhet
3	Beteende	Verksamhet
4	Resultat	Sektor

Nivå 1 (reaktioner) i Tabell 3 avser därmed att mäta deltagarens reaktioner, vilket kan göras med hjälp av en kvantitativ och kvalitativ enkät. Nivå 2 (lärande) kan mätas genom att deltagare formulerar en handlingsplan baserat på en applicering och värdering av erfarenheteter från övning med hänsyn till den egna verksamheten. På nivå 3 (beteende) behöver den formulerade handlingsplanen följas upp så att den fått genomslag i övande verksamhets riktlinjer inom det aktuella området till exempel incidenthantering. Nivå 4 (resultat) syftar till att säkerställa att beteendeförändringar på nivå 3 även leder till sektorsövergripande förändringar i avsedd riktning, till exempel genom förändrade eller nya riktlinjer inom det aktuella området. Sett till Kirkpatrick-modellen följs övningens effekter upp enligt nivåindelningen som visas i Figur 9.



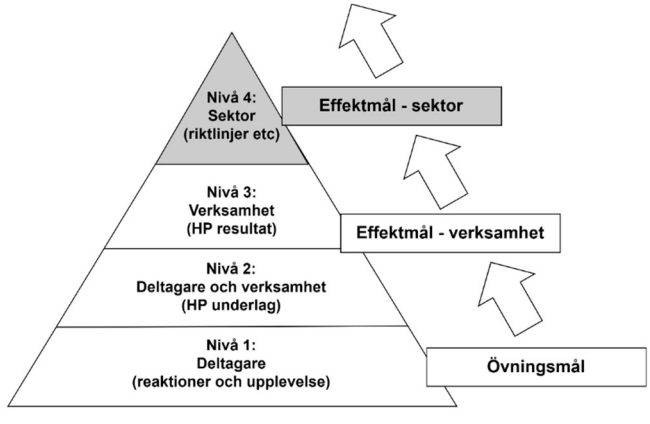
Figur 9. Nivåer för mätning av övning – anpassad Kirkpatrick-modell. Egen figur anpassad efter Ahmad m.fl. (Ahmad m.fl., 2015, s. 4 egen översättning)

Nivå 1 i Figur 9 fokuserar på övningens deltagare och mäter reaktioner och upplevelse i anslutning till själva övningstillfället. Nivå 2 fokuserar på de lärdomar och erfarenheter deltagarna tar med sig från övning och främjar fortsatt reflektion baserat på den egna verksamheten. På denna nivå startar även arbetet med att formulera ett underlag till handlingsplan som skall fokusera på bland annat identifierandet av utmaningar i verksamhetens nuvarande incidenthanteringsarbete och ge förslag till åtgärder. Denna nivå fokuserar därmed deltagarnas på lärdomar och reflekterade erfarenheter från övningen och hur dessa kan omsättas i ordinarie verksamhet. På Nivå 3 blir verksamhetsperspektivet starkare där underlaget till handlingsplan förutsätts fått förankring och acceptans för att kunna börja implementeras. Denna nivå syftar därmed till att åstadkomma den beteendeförändring i deltagarens ordinarie verksamhet som eftersöks. Den sista nivån, Nivå 4, syftar till det resultat och effekt i övande sektor som eftersöks. Detta resultat kan till exempel röra framtagande av rutiner och riktlinjer avsedda att vara gemensamma och stödja arbetet inom hela den aktuella sektorn. Observera att i Figur 9 är Nivå 4

markerad med grå bakgrund eftersom effektmätningen inom det aktuella övningen huvudsakligen kommer att fokusera på Nivå 1 till 3.

3.3.2 Sammanfattad effektlogik

Nedan presenteras en sammanfattad bild av den effektlogik som kan användas inom ramen för Ragnarök. Effektlogik syftar här till de mekanismer som främjar och säkerställer att övningens avsedda resultat och effekter uppnås. Detta för att tydliggöra vilka mål och effekter som eftersträvas, på vilken nivå målet eller effekten förväntas, samt på vilken sikt effekten förväntas realiseras. Effektlogiken bakom effektmätningen som presenterats för övningen är relativt komplex med olika typer av effektmål som formulerats på olika nivå sett till Kirkpatrick-modellen. Ragnaröks design bygger bland annat på det pedagogiska perspektivet konstruktiv anpassning. Detta perspektiv implicerar att samtliga övningsmål och effektmål tydligt skall kunna relateras till varandra och följa en tänkt progression för måluppfyllnad och förväntat resultat. Samtliga övningsmål innefattar här såväl generella som specifika mål för varje del av övningen (se avsnitt 3.1.5, 3.2.1.2, 3.2.2.2). Därmed finns en tydlig tanke att de övningsmål och effektmål som formuleras på varje nivå, vidareutvecklar tidigare nivåer samt bidrar till uppfyllnad på senare nivåer. Konstruktiv anpassning säkerställer även att samtliga övningsmål och effektmål är välgrundade och förankrade i övningen som helhet, och att eventuell redundans och luckor tydligt synliggörs och kan adresseras. Hur övningsmål och effektmål per nivå bidrar till måluppfyllnad visas på övergripande sätt i Figur 10.



Figur 10. Nivåer, övningsmål och effektmål – anpassad Kirkpatrick-modell. Egen figur anpassad efter Ahmad m.fl. (Ahmad m.fl., 2015, s. 4 egen översättning)

3.3.3 Handlingsplan

En handlingsplan kommer att användas som underlag för mätning av att Ragnarök får avsedd effekt i övande verksamhet. Användandet av en

handlingsplan motiveras av ett behov av tydlighet kring vad övande verksamhet behöver förbättra med hänsyn till sin incidenthantering. Syftet med denna förbättring har flera skäl. Med förbättrad och mer effektiv incidenthantering säkerställs verksamhetens proaktivitet. Responstid och risk minskar samtidigt som efterlevnad av regelverk och lagar säkerställs. Sammantaget ökar därmed såväl medarbetares som organisationens beredskap. Det handlar även om att bygga förtroende inom verksamheten och minimera ekonomiska förluster samtidigt som verksamheten möter dagens och morgondagens hotbild. I Tabell 4 visas exempel på relevant innehåll i en sådan handlingsplan.

Tabell 4. Exempel på avsnitt och innehåll i handlingsplan.

Avsnitt	**Innehåll**
Syfte och mål	Tydligt beskrivet syfte
	Mätbara och specificerade mål
Nulägesanalys	Beskrivning nuläge
	Identifierade problemområden och konsekvenser
Förbättringsåtgärder	Identifierade åtgärder med tydliga mål, prioritet, tidplan, ansvar, status
Uppföljning och utvärdering	Mätmetod, tidplan, kriterier för utvärdering
Beslut och ansvar	Ansvar uppföljning, datum nästa utvärdering

Baserat på en tydlig dokumentmall för handlingsplanen, reflekterar deltagaren aktivt kring sin egen verksamhets incidenthantering i ljuset av erfarenheter och lärdomar från Ragnarök. Denna reflektion resulterar i: ett tydligt beskrivet mål och syfte med handlingsplanen, en beskrivning av nuvarande hantering samt tydligt identifierade problemområden och dessas konsekvenser för verksamheten samt identifierade förbättringsåtgärder med tydlighet i målbild, prioritet, tidplan, ansvar samt status för uppföljning. Handlingsplanen avslutas sedan med en tydligt angiven uppföljning och utvärdering samt information om beslut, ansvar och datum för nästa utvärdering.

Observera att handlingsplanens innehåll kan vara känsligt. I övningskonceptet kommer därmed mätning baserat på handlingsplanen att fokusera på att detta arbete initieras och genomförs, och därmed inte innefatta vad som i sak formuleras i handlingsplanen.

3.3.4 Effektmål verksamhet

Effektmätning innefattar även formulerandet av effektmål. Dessa effektmål syftar till att tydliggöra och definiera de förändringar som eftersträvas, och användningen av effektmål kan motiveras på flera sätt. Först och främst ger effektmålen ett tydligt syfte och inriktning för en insats som fokuserar på verksamhetsförändring. Formulerandet av tydliga mål är även viktigt för förankring, gemensam förståelse och motivation för insatsen. Eftersom mätbara mål, så kallade indikatorer, kopplas till varje effektmål, ges även förutsättningar för kontinuerlig uppföljning och mätbarhet. Genom att formulera tydliga effektmål, säkerställs även att förändringsarbetet fokuserar på insatser som bidrar till måluppfyllnad. Prioritering och resursfördelning kan därmed tydliggöras och motiveras. För att mäta och följa upp resultat och påverkan i övande verksamhet, har effektmål på verksamhetsnivå formulerats (effektmål verksamhet i Tabell 5), det vill säga de verksamhetsförmågor Ragnarök avser att vidareutveckla och stärka. Dessa effektmål är tydligt relaterade till samtliga formulerade övningsmål (se avsnitt 3.1.5, 3.2.1.2, 3.2.2.2).

Handlingsplanen utgör ett viktigt underlag för uppföljning och mätning av övningens påverkan på verksamhetsnivå. Det bör därmed observeras att de effektmål för verksamheten som här presenteras är generellt utformade, och att dessa kommer att omsättas i respektive övande verksamhets formulerade handlingsplan. De beskrivna målen utgör endast exempel på hur de kan se ut, och hur de kan användas för uppföljning med olika tidsperspektiv. Tillämpning av effektmål kommer således variera beroende på verksamheternas identifierade behov av förbättring. Effektmålen är i sin tur kopplade till mätbara mål (indikatorer) samt underlag för mätning. Exempel på operationaliserade effektmål, mätbara mål samt underlag för mätning presenteras i Tabell 5.

Tabell 5. Exempel på operationaliserade effektmål och mätbara mål för verksamheten

#	Effektmål verksamhet	Mätbart mål (indikator)	Underlag för mätning
1	Stärkt ledning och styrning av arbete med cyberincidenter	Identifierade förbättringspunkter i handlingsplanen har implementerats i riktlinjer inom [*ange tidsrymd*] månader	Handlingsplan
2	Förbättrad identifiering, hantering och återhämtning från incidenter	Minskad medeltid för hantering av incidenter med [*ange procent*] skett inom [*ange tidsrymd*] månader	Enkät (intern KPI)
3	Proaktivt arbete med cyberhot och cyberincidenter	Minst [*ange procent*] upplever en förbättrad incidenthanteringsförmåga	Enkät

#	Effektmål verksamhet	Mätbart mål (indikator)	Underlag för mätning
		inom [*ange tidsrymd*] månader	
4	Kommunikation och rapportering av cyberangrepp och cyberincidenter	Andel korrekta och tidsenliga eskaleringar ska öka med [*ange procent*] inom [*ange tidsrymd*] månader	Enkät (intern KPI)
		Antal rapporteringar till berörda instanser (ex CERT-SE) ska öka med [*ange procent*] inom [*ange tidsrymd*] månader	Rapporter (CERT-SE)
5	Dela och ta del av erfarenheter av cyberincidenter mellan organisationer	Ökad erfarenhets- och informationsdelning via MISP-verktyg inom [*ange tidsrymd*] månader	Handlingsplan + enkät
6	Integrering av lärdomar för ständig förbättring	Minst [*ange procent*] av identifierade svagheter ska vara åtgärdade inom [*ange tidsrymd*] månader	Handlingsplan + enkät
7	Genomföra träning och övning kopplat till cyberincidenter	Minst [*ange antal*] övningstillfällen med [*ange antal*] deltagare ska vara genomförda inom [*ange tidsrymd*]	Övningsplan

3.3.5 Effektmål sektor

Ragnarök fokuserar primärt på resultat och effekt på Nivå 1 till 3 i Kirkpatrick-modellen (Ahmad m.fl., 2015). Detta till trots väljer vi ändå att inom ramen för denna beskrivning av Ragnarök att formulera exempel på effektmål för Nivå 4, det vill säga effekt inom övande sektor. Exempel på resultat kopplat till denna nivå är bland annat att stärka sektorn och dess aktörer generellt med hänsyn till motståndskraft mot samhällsstörningar, att identifiera behov, och främja utveckling av standardiserade rutiner, att förbättra informationsdelning mellan sektorns olika aktörer samt att verka för att sektorns aktörer kan minska skador och negativa effekter av cyberhot och cyberincidenter på generell nivå. I Tabell 6 presenteras de effektmål sektor som formulerats. För varje mål anges även ett mätbart mål (indikator) samt ett tänkbart underlag för genomförande av mätning.

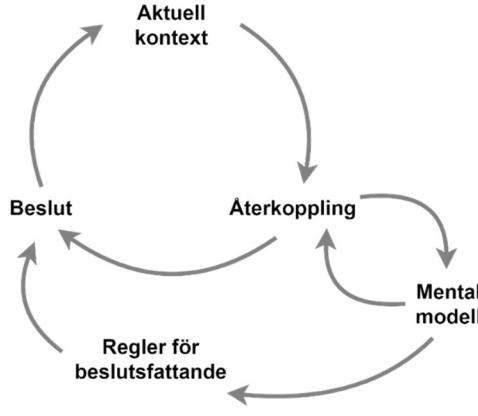
Tabell 6. Effektmål-sektor med indikatorer och exempel på underlag för mätning

#	Effektmål sektor	Mätbart mål (indikator)	Underlag för mätning
1	Hög motståndskraft mot samhällsstörningar orsakade av cyberincidenter	Genomsnittlig tid för hantering av cyberincident för sektorn som helhet	Incidenthanteringsrapport
2	Standardiserade samordnade sektorsspecifika incidenthanteringsrutiner	Grad av överensstämmelse mellan aktörers incidenthanteringsrutiner	Underlag
		Behov av sektorsspecifika incidenthanteringsrutiner	Behovsanalys
3	Minskade negativa effekter och konsekvenser av cyberincidenter	Minskade kostnader för återställning och minskning av negativa effekter	Direkt/indirekt kostnad
4	Ökad informationsdelning och lärande mellan organisationer inom sektorn	Informationsdelning som bidrag till hantering av cyberincidenter	Utvärdering
5	Förbättrad samverkan inom aktuell sektor kring incidenthantering	Aktörers upplevda samverkan	Utvärdering

3.4 Uppföljning och förbättring övning

Ragnarök genomsyras av en tanke att bedriva kontinuerligt förbättringsarbete enligt ansatsen ständiga förbättringar. Ständig förbättring är en filosofi eller ansats som främjar varaktigt förbättringsarbete i en verksamhet (Bhuiyan & Baghel, 2005). Denna ansats kan innefatta såväl inkrementella mindre förändringar, som mer radikala förändringar, men i kontexten av den aktuella övningen, syftar detta arbete huvudsakligen till kontinuerliga inkrementella mindre justeringar och förbättringar baserade på uppföljning och utvärdering i anslutning till genomförande. Eftersom övningen i sig är baserad på ett övningskoncept, finns dock även ett behov att kontinuerligt följa upp och verifiera samt eventuellt justera detta koncept eftersom övningskonceptet i sig utgör en central förutsättning för övningsdesignen. Ständig förbättring är även beroende av lärande ansats i berörd verksamhet eftersom organisatoriskt lärande främjar och stödjer ständig förbättring (Oliver, 2009). Det applicerade perspektivet på återkoppling väljer vi att basera på en dubbel-loop för lärande som kan sammankopplas med reflekterat lärande (t.ex. Argyris, 1991). Syftet med denna dubbel-loop är att möjliggöra justeringar av den mentala modell

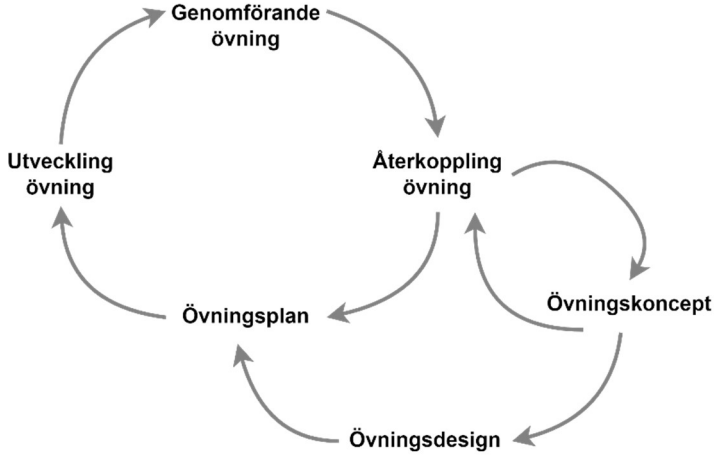
vilken ligger till grund för beslutsfattande. Figur 11 illustrerar det reflekterade lärandet i en organisatorisk kontext där beslut appliceras på aktuell kontext som i sin tur bistår med återkoppling. Denna återkoppling påverkar och påverkas i sin tur av den bakomliggande mentala modell som ligger till grund för den aktuella kontextens regler för beslutsfattande. På detta sätt reflekteras informationen som återkopplas och kan komma att påverka framtida beslut och eventuella justeringar.



Figur 11. Dubbel-loop för lärande.

I Figur 12 presenteras en vidareutvecklad dubbel-loop för övning och övningskoncept. Vid framtagandet av denna modell har mental modell översatts till övningskoncept och regler för beslutsfattande till övningsdesign. Detta motiveras genom att övningskonceptet utgör den konceptuella struktur och ram som framtagna övningar kommer utgå ifrån det vill dessas bakomliggande mentala modell. Den aktuella rationalen för praktiskt beslutsfattande under planering och utveckling av övning utgår i sin tur ifrån övningsdesignen det vill säga övergripande förutsättningar för övningen. I Figur 12 framgår att formulerande av övningsplan är en förutsättning för utveckling av övning vilken sedan följs av genomförande av övning. Därefter utvärderas övningen genom att en återkoppling sker från övningsdeltagare och från personal som genomfört övningen. Resultatet av denna återkoppling både påverkar, och påverkas av, övningskonceptets utformning och övningskonceptet påverkar i sin tur övningens design. Återkopplingen verifierar därmed övningskonceptets relevans. En övnings återkoppling ger tydliga indikatorer på vad som fungerar bra i en övning baserad på övningskonceptet, och vad som potentiellt behöver justeras. Övningskonceptet ligger sedan till grund för övningsdesignen som i sin tur utgör förutsättningarna för övningsplanen. Med denna dubbel-loop för övning och övningskoncept, det vill säga mellan återkoppling övning och övningskoncept samt mellan övningskoncept via övningsdesign till övningsplan, säkerställs

därmed återkoppling och förbättring av såväl övning som övningskoncept på ett tydligt strukturerat sätt.



Figur 12. Dubbel-loop för övning och övningskoncept.

4 Diskussion

I detta kapitel diskuteras potentiella möjligheter och utmaningar kring arbetet att gå från övningskoncept till genomförande av övning baserat på detta koncept.

4.1 Möjligheter och utmaningar

När övningskonceptet ska omsättas till en övning som baseras på övningskonceptet skulle man kunna säga att det är då det egentliga arbetet börjar, det vill säga när den mentala modellen som beskrivs i övningskonceptet skall operationaliseras i en övningsdesign och planeras, utvecklas samt genomföras i form av en verklig övning. Även om operationalisering av koncept är förknippat med vissa utmaningar överväger i föreliggande fall möjligheter och fördelar med hänsyn till konceptutveckling. Typiska möjligheter med konceptutveckling vid övning är till exempel differentiering och innovation, anpassningsbarhet till olika målgruppers behov, flexibilitet och skalbarhet, förbättrat lärande samt mätbara resultat. Konceptutveckling inom övning skapar möjlighet att designa övningar på innovativa och kreativa sätt där bakomliggande behov är drivande snarare än traditionen att utföra dessa övningar på ett visst sätt. Detta skapar möjlighet för nya typer av övningar och sätt att öva på, samt kommer förhoppningsvis på ett positivt sätt att differentiera utföraren av övningen från andra utförare. Sett till målgruppers behov finns möjlighet att möta dessa behov med skräddarsydda lösningar.

Flexibilitet och skalbarhet möjliggör till exempel anpassning till deltagargrupper av olika storlek, och skalbarhet är en förutsättning för den modularisering som krävs för att kunna kombinera olika delar av övning på olika sätt. Detta skapar även en design och struktur som till exempel passar agil utveckling. Flexibilitet och skalbarhet möjliggör även ett effektivt nyttjande av resurser. Även om konceptutveckling initialt kan ses som resurskrävande, så sker konceptutveckling oftast på längre sikt där en potentiell kostnadseffektivitet kan nås. Förutsättningarna för ett förbättrat lärande hos deltagarna ökar markant med denna typ av ansats, eftersom perspektiv på pedagogik och lärande kan integreras genom hela utvecklingsprocessen. Det konceptuella perspektivet säkerställer även en väl sammanhållen och samverkande struktur. Eftersom det förväntade lärandet kan tydliggöras ökar även möjligheterna för mätning av övningens effekter, till exempel genom formulerandet av olika typer av mål och indikatorer.

Det finns dock ett antal tydliga utmaningar som är förknippade med koncept och konceptutveckling inom övning. Dessa är till exempel osäkerhet och risk, begränsningar i resurser, pedagogik och metodik samt mätningsmässiga utmaningar. Som tidigare nämnts kräver konceptutveckling ofta mycket tid och resurser. Eftersom arbetet är tydligt kreativt och i många fall kräver kontinuerliga diskussioner och förankring, finns även en osäkerhetsfaktor med hänsyn till att

budgetera för denna typ av arbete. Arbetet med att utveckla konceptet bedrivs även med ett grundläggande antagande om hur konceptet i sig skall utformas och designas för att fungera som riktlinjer för kommande övningar. Det finns därmed en viss inbyggd osäkerhet och risk i processen eftersom man inte helt kan säkerställa att konceptet verkligen kommer att vara framgångsrikt i praktiken och erhålla acceptans hos deltagarna. Denna risk kan dock minimeras genom kontinuerligt deltagande av relevanta intressenter och målgruppsrepresentanter under konceptutvecklingsarbetet samt genom olika typer av avgränsade utvärderingar och tester.

Eftersom den typ av övningar som övningskonceptet syftar till, det vill säga övningar i incidenthantering, historiskt sett har haft ett ensidigt tekniskt fokus, innebär integrationen av det pedagogiska perspektivet en utmaning. Även om möjligheterna i detta sammanhang överväger, så utmanas samtidigt en tradition och gällande praxis kring hur denna typ av övningar brukar genomföras. Därmed kan det pedagogiska perspektivet även påverka övningskonceptet på så sätt att övningens innehåll, struktur och metodik måste justeras för att kunna integreras med den pedagogiska ansatsen. Detta kan resultera i att den övning som genomförs baserat på övningskonceptet av vissa parter kan komma att uppfattas som en icke-konventionell övning av denna typ. Det finns dock goda möjligheter att motverka detta genom att arbeta aktivt och kontinuerligt med förankring och tydlig motivering.

Eftersom det pedagogiska perspektivet på denna typ av övningar är relativt nytt finns endast begränsad kunskap inom området. Detta kan därmed medföra att mätning av lärande och effekt innebär vissa utmaningar. För att hantera utmaningen med mätning av lärande krävs en realistisk syn och målbild kring vilka typer av mätningar och indikatorer som är möjliga att följa upp. Vad som är realistiskt möjligt att mäta med hänsyn till deltagarnas lärande kommer även påverka övningskonceptets perspektiv på lärande. Ett tydligt exempel med hänsyn till föreliggande övningskoncept är att bedömning och mätning av deltagares individuella förmåga och färdighet inte kommer att genomföras. Detta är därmed något som tydligt påverkat perspektivet på lärande och förväntad effekt i arbetet med att utveckla övningskonceptet. För att mätning av resultat och effekt i deltagarnas ordinarie verksamhet skall kunna lyckas, krävs även engagemang och resurser för varje deltagare för att aktivt kunna delta i uppföljande mätning och utvärdering efter övning. Vid konceptutveckling finns ett antal komponenter som ständigt samspelar genom hela processen. Relationerna mellan dessa är därmed ömsesidiga vilket föranleder en ständig lyhördhet till exempel med hänsyn till avvägningar och begränsande faktorer. Exempel på centrala komponenter under konceptutveckling är följande:

- mål och syfte
- intressenter
- målgrupp

- metodik och pedagogik
- teknik och resurser
- struktur och innehåll
- genomförande
- utvärdering.

För tydlighet och inriktning behöver konceptet ett tydligt mål och syfte och dessa måste förankras hos relevanta intressenter. Samtidigt är det mycket viktig att tillse att såväl mål som syfte är formulerade på adekvat nivå för att minimera begränsande effekter i fortsatt arbete. Behov och krav som utgår från intressenter och målgrupp är centrala aspekter som måste tas om hand om genom hela konceptutvecklingsprocessen. Dessa komponenter är även centrala när det kommer till förankring och förhandling vid olika beslutspunkter. Metodik och pedagogik är en styrande komponent med hänsyn till hur konceptet designas, dess struktur samt integrering av metodmässiga och pedagogiska perspektiv. Teknik och resurser är även en komponent som påverkar utvecklingen av ett koncept som till stor del kommer genomföras i, och vara beroende av, en teknisk miljö. Det finns även andra resurser som potentiellt påverkar som till exempel tillgängliga kompetenser, tilldelad tid och finansiering. Sammanfattningsvis menar vi att konceptutveckling kan liknas vid en ständig balansgång. De aspekter som vägs samman kontinuerligt är intressenters krav och behov, resursmässiga förutsättningar, målgruppens behov, kreativitet och innovation samt planering och genomförbarhet.

5 Slutsatser och fortsatt arbete

Detta kapitel presenterar arbetets slutsatser i form av en summering och reflektion kring erfarenheter och lärdomar från konceptutvecklingsarbetet. Därefter presenteras två exempel på relevant fortsatt arbete med hänsyn till vidareutveckling av övningskonceptet.

5.1 Slutsatser

I rapportens titel betonas lärande och stärkt cyberförmåga. Detta är två grundläggande aspekter som tydligt format arbetet med såväl övningskoncept som exempelövningen Ragnarök. Detta arbete adresserar ett tydligt formulerat behov av kompetenshöjning inom cyberförmåga i samhället i stort. Arbetets syfte och mål har varit att utveckla ett övningskoncept som fokuserar på incidenthantering och riktar sig till samhällsviktig verksamhet i Sverige. Sett till erfarenheter och lärdomar av konceptutvecklingsarbetet väljer vi att lyfta fram följande aspekter:

- gemensam grundförståelse
- vikten av förankring och samarbete
- kommunikation och dokumentation
- dynamik, flexibilitet och struktur
- målgruppsanpassning
- tillit, förtroende och engagemang.

Med *gemensam grundförståelse* önskar vi betona vikten av att konceptutvecklingsteamet så tidigt som möjligt aktivt söker konsensus och gemensam förståelse kring det kommande arbetets nyckelaspekter. Detta kan till exempel vara att enas om en gemensam definition av begreppet koncept, ett begrepp som i sig kan ha flertalet olika tolkningar beroende på tolkningskontext. För att få en god start på arbetet är det viktigt att så tidigt som möjligt definiera konceptutvecklingsarbetets nyckelaspekter och begrepp och därefter aktivt nå gemensam grundförståelse. Detta gäller särskilt om teamet som skall utveckla konceptet är sammansatt av personer med olika organisatorisk och kompetensmässig hemvist. I detta ligger även givetvis att tydligt motivera och förklara betydelsen av det initiala arbetet, för att på så sätt skapa aktiv delaktighet och engagemang. Senare under arbetets gång kommer säkerligen begrepp komma att behöva revideras, men det är även då viktigt att konsensus söks för att undvika icke-förankrade beslut.

Vikten av förankring och samarbete kopplar tydligt till den gemensamma grundförståelsen, men fokuserar mer på konceptutvecklingsprocessen som helhet. Eftersom detta arbete är av en tydlig iterativ och kreativ karaktär, som genomförs i syfte att ta fram en konceptuell design, kommer teamet att ställas

inför ett antal olika designbeslut som måste vara väl förankrade inom teamet. Samarbete genom aktivt engagerat deltagande av samtliga medlemmar i teamet är även en viktig förutsättning för det kreativa arbete som genomförs samt för att säkerställa att samtliga teammedlemmars kompetens och erfarenheter utnyttjas på bästa sätt. Eftersom konceptutveckling handlar om att utveckla en modell med generiska egenskaper och bredare applicerbarhet än en specifik lösning, är det viktigt att vara medveten om att detta arbete kommer att kräva mycket samarbete, och att samarbete i sig kan ses som resurskrävande.

Vid samarbete är aspekterna *kommunikation och dokumentation* av yttersta vikt, och det är därmed mycket viktigt att formerna för dessa aspekter säkerställs så tidigt som möjligt i arbetsprocessen. Med hänsyn till dokumentation, vill vi understryka vikten av att dokumentera såväl det teamet gör, som designbeslut som leder till att delar väljs respektive väljs bort från det fortsatta arbetet. Eftersom konceptutvecklingsarbetet är en iterativ och kreativ process, underlättar det därmed om teamet har tillgång till tidigare designbeslut om något val under processen skulle behöva omvärderas.

Flexibilitet har varit en återkommande egenskap som eftersträvats i övningskonceptet och denna egenskap återkommer även med hänsyn till konceptutvecklingsarbetet. Vi väljer därmed att lyfta *dynamik*, *flexibilitet* och *struktur* som viktiga delar att vara medveten om, samt ta hänsyn till under detta arbete. Det kreativa arbetet med att utveckla ett koncept måste kunna stödja dynamiska och flexibla processer, miljöer och arbetssätt, men för att erhålla en god balans behöver konceptutvecklingsarbetet samtidigt en mycket tydlig plan och struktur. Ett tydligt exempel på den flexibilitet och dynamik som krävs under konceptutvecklingsarbetet, är de ständiga fokusväxlingar mellan konceptuella och operationella perspektiv på en kommande övning som baseras på övningskonceptet. Det finns alltid en styrka i praktiska exempel, men i detta sammanhang blir utmaningen att konceptualisera och aggregera dessa exempel på ett relevant sätt. Flexibilitet är även något som återfinns i det utvecklade övningskonceptet. Tillsammans med skalbarheten skapar denna flexibilitet möjligheter, till exempel i form av att separata delar av en övning kan delas upp i moduler. Bakom denna flexibilitet finns även en grundtanke kring att det koncept som utvecklas skall vara hållbart och effektivt att vidmakthålla, samt utveckla över tid. Ett övningskoncept som kräver mycket resurser för att upprätthållas kommer att motverka sitt syfte.

En mycket viktig aspekt att betona är *målgruppsanpassning*. Detta eftersom vikten av att känna till den tänkta målgruppens förväntade nytta och behov blir extra tydlig när det gäller utveckling av övningskoncept som riktar sig mot en tydligt definierad målgrupp. Övningskonceptets målgruppsanpassning anger därmed ramarna som sedan kan finjusteras vid övningsdesign. Om möjligt är det därmed att föredra att låta representanter från den tänkta målgruppen vara kontinuerligt delaktiga i konceptutvecklingsarbetet, samt så tidigt som möjligt

undersöka möjligheterna att genomföra användartest på någon utvald del av en övning. Under arbetet med att utveckla övningskonceptet ställer detta därmed krav på att konceptets delar kontinuerligt kan komma att behöva exemplifieras för att delarna, i form av konkreta exempel på delar av övning, skall kunna utvärderas av representanter ur den tänkta målgruppen. Utmaningen i detta sammanhang är därmed att arbetet syftar till att utveckla ett övningskoncept, men att den tänkta målgruppen kommer möta övningar baserade på detta koncept, och inte konceptet i sig självt.

Till sist väljer vi att betona vikten av *tillit, förtroende och engagemang*. Eftersom konceptutvecklingsarbetet bygger på aktiv delaktighet, motivation och engagemang över tid, ser vi det som mycket viktigt att arbeta aktivt med tillits- och förtroendeskapande aktiviteter inom teamet under arbetets uppstart. I detta ligger till exempel naturliga egenskaper som lyhördhet och aktivt lyssnande, en inkluderande attityd samt respektfull hantering av olika åsikter och perspektiv. Genom att arbeta medvetet och aktivt med att försöka balansera de olika intressenternas krav, behov och önskemål främjas även förtroende och engagemang över tid. Det är därmed viktigt att arbeta aktivt med denna aspekt inom konceptutvecklingsteamet, samt mot intressenter och andra deltagare under arbetet, eftersom koncept och konceptutveckling implicerar ett åtagande och engagemang på längre sikt.

5.2 Fortsatt arbete

Som förslag på fortsatt arbete med övningskonceptet väljer vi att presentera följande två frågeställningar:

1. Hur skulle övningskonceptet kunna utvärderas och förbättras på konceptuell nivå över tid?

2. Hur skulle övningskonceptet kunna utvecklas med hjälp av ett fördjupat pedagogiskt perspektiv?

Med den första frågan vill vi understryka vikten av att inte bara fokusera på övningars genomförande ur ett utvärderingsperspektiv. När övningar baserat på övningskonceptet utvecklas kommer säkerligen nya insikter, erfarenheter och lärdomar utvecklas – inte minst kring steget och processen att gå från övningskoncept, via övningsdesign, till genomförbar övning. Detta fortsatta arbete skulle även inkludera framtagandet av mekanismer för att kontinuerligt ta hand om utvärderingsresultat som underlag till förbättring av övningskonceptet. Som svar på den första frågan önskar vi därmed studera det fortsatta arbetet med övningskonceptet och dess kommande övningar och utveckla en metodik för kontinuerlig utvärdering och förbättring av övningskonceptet. Detta är även något som har berörts väldigt kortfattat i denna rapports avsnitt om uppföljning

och förbättring av övning och vi ser ett tydligt behov av att vidareutveckla detta perspektiv på uppföljning och vidareutveckling.

Den andra frågan fokuserar på hur övningskonceptet skulle kunna utvecklas och förbättras med hjälp av ett fördjupat pedagogiskt perspektiv. Ett exempel på vad detta skulle kunna innebära är att utgå från Blooms utvecklade taxonomi såsom den presenteras av Krathwohl (2002). Detta skulle innebära en möjlighet att inordna övningskonceptets övningsmål i en tvådimensionell matris baserad på en kunskapsdimension och en kognitiv processdimension. Detta skulle möjliggöra att övningsmålen kan studeras och analyseras på ett mer detaljerat sätt, samt att övningsmålens tänkta progression skulle göras transparent och tydlig. Detta arbete skulle säkerligen leda till att såväl mål som andra delar av övningskonceptet skulle komma att behöva justeras. På längre sikt skulle detta arbete även möjliggöra att övningens olika aktiviteter relateras på ett tydligt sätt till övningskonceptets övningsmål, vilket i sig skulle stärka såväl det pedagogiska perspektivet som övningskonceptets relevans och kvalitet.

6 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.

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031.

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.

Argyris, C. (1991). Teaching smart people how to learn. *Harvard business review*, *69*(3).

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.

Barab, S. A., Squire, K. D., & Dueber, W. (2000). A co-evolutionary model for supporting the emergence of authenticity. *Educational technology research and development*, *48*(2), 37–62.

Bhuiyan, N., & Baghel, A. (2005). An overview of continuous improvement: From the past to the present. *Management decision*, *43*(5), 761–771.

Biggs, J., Tang, C., & Kennedy, G. (2022). *Teaching for Quality Learning at University* (5:e uppl.). McGraw-Hill education (UK).

Bıçakcı, S., & Evren, A. G. (2024). Responding cyber-attacks and managing cyber security crises in critical infrastructures: A sociotechnical perspective. I *Management and Engineering of Critical Infrastructures* (s. 125–151). Elsevier.

Bradshaw, M. J. (2011). Effective learning: What teachers need to know. *Innovative teaching strategies in nursing and related health professions*, 3–18.

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

Cichonski, P., Millar, T., Grance, T., Scarfone, K., & others. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1–147.

Clancey, W. J. (1995). A tutorial on situated learning. *Proceedings of the International Conference on Computers and Education (Taiwan)*.

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

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

Dewar, R. S. (2018). *Cybersecurity and cyberdefense exercises*. ETH Zurich.

Enisa. (2016). *NCSS Good Practice Guide. Designing and Implementing National Cyber Security Strategies*. https://www.enisa.europa.eu/publications/ncss-good-practice-guide

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

Futter, A. (2018). ‘Cyber’semantics: Why we should retire the latest buzzword in security studies. *Journal of Cyber Policy*, *3*(2), 201–216.

Försvarsdepartementet. (2023). *Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet* (Skr. 2023/24:26). Försvarsdepartementet.

Försvarsdepartementet. (2025). *Nationell strategi för cybersäkerhet 2025–2029* (Skr. 2024/25:121).

Grance, T., Nolan, T., Burke, K., Dudley, R., White, G., & Good, T. (2006). Guide to test, training, and exercise programs for IT plans and capabilities. *National Institute of Standards and Technology Special Publication 800-84*.

Gross, D. C., Pace, D., Harmoon, S., & Tucker, W. (1999). Why fidelity? *Proceedings of the Spring 1999 Simulation Interoperability Workshop*.

Gurnani, R., Pandey, K., & Rai, S. K. (2014). A scalable model for implementing Cyber Security Exercises. *2014 International Conference on Computing for Sustainable Global Development (INDIACom)*, 680–684.

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.

Herrington, J. (2014). Introduction to authentic learning. I *Activity theory, authentic learning and emerging technologies* (s. 61–67). Routledge.

Jonsson, D. K., Eriksson, C., Ingemarsdotter, J., Rossbach, N. H., & Wedebrand, C. (2023). *Gråzonslägen i krig och fred* (FOI-R--5447--SE). Totalförsvarets forskningsinstitut.

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., & Ojala, A.-L. (2023). Authentic learning environments for in-service training in cybersecurity: A qualitative study. *International Journal of Continuing Engineering Education and Life Long Learning*, *33*(1), 128–147.

Kim, J., Kim, K., & Jang, M. (2019). Cyber-physical battlefield platform for large-scale cybersecurity exercises. *2019 11th international conference on cyber conflict (CyCon)*, *900*, 1–19.

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

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

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186.

Lindbom, H., & Tehler, H. (2020). Enhetlig terminologi kring begreppet förmåga i det förebyggande och förberedande arbetet över hela hotskalan. *Avdelningen för riskhantering och samhällssäkerhet, Lunds Universitet*.

Mallick, M. A. I., & Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News*, *190*(1), 1–69.

MSB. (2021). *Vägledning till ökad säkerhet i industriella informations- och styrsystem* (MSB718). Myndigheten för samhällsskydd och beredskap.

MSB. (2023). *Lista med viktiga samhällsfunktioner – Utgångspunkt för att stärka samhällets beredskap* (MSB1844). Myndigheten för samhällsskydd och beredskap (MSB).

Mäses, S., Maennel, K., Toussaint, M., & Rosa, V. (2021). Success factors for designing a cybersecurity exercise on the example of incident response. *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 259–268.

NCSC-SE. (2024). *Cybersäkerhet i Sverige 2024*.

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management. *NIST Special Publication 800*, *NIST SP 800-61r3*. https://doi.org/10.6028/NIST.SP.800-61r3

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

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST special publication (NIST SP 800-181)*, *800*(2017), 181.

Oliver, J. (2009). Continuous improvement: Role of organisational learning mechanisms. *International Journal of Quality & Reliability Management*, *26*(6), 546–563.

Patton, M. Q. (1997). *Utilization-focused evaluation*. Sage.

Posso, R., & Altmann, J. (2024). Trust and Trust-Building Policies to Support Cybersecurity Information Sharing: A Systematic Literature Review. *International Conference on the Economics of Grids, Clouds, Systems, and Services*, 212–228.

Prümmer, J., van Steen, T., & van den Berg, B. (2023). A systematic review of current cybersecurity training methods. *Computers & Security*, 103585.

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.

RiR 2023:8. (2023). *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig* (RiR 2023:8). Riksrevisionen.

Robbins, B. G. (2016). What is Trust? A Multidisciplinary Review, Critique, and Synthesis. *Sociology Compass*, *10*(10), 972–986. https://doi.org/10.1111/soc4.12391

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 2024:64. (2024). *Motståndskraft i samhällsviktiga tjänster Slutbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven* (SOU 2024:64; Statens Offentliga Utredningar).

Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2022). A cyber incident response and recovery framework to support operators of industrial control systems. *International Journal of Critical Infrastructure Protection*, *37*, 100505.

Švábenskỳ, V., Vykopal, J., Horák, M., Hofbauer, M., & Čeleda, P. (2024). From paper to platform: Evolution of a novel learning environment for tabletop exercises. I *Proceedings of the 2024 on Innovation and Technology in Computer Science Education V. 1* (s. 213–219).

Söderström, F. (2025). *Pedagogiska perspektiv på cybersäkerhetsövningar—En motivering samt litteraturöversikt* (FOI-R--5575--SE). Totalförsvarets forskningsinstitut. https://foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI-R--5575--SE

Uma, M., & Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *Int. J. Netw. Secur.*, *15*(5), 390–396.

Van der Kleij, R., Kleinhuis, G., & Young, H. (2017). Computer security incident response team effectiveness: A needs assessment. *Frontiers in psychology*, *8*, 2179.

Walsham, G. (1993). *Interpreting information systems in organizations*. John Wiley & Sons, Inc.

Wei, D., & Ji, K. (2010). Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights. *2010 3rd international symposium on resilient control systems*, 15–22.

Wen, S.-F., Yamin, M. M., & Katt, B. (2021). Ontology-based scenario modeling for cyber security exercise. *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 249–258.

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.

Whyte, C. (2020). Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare. *Journal of Cybersecurity*, *6*(1), tyaa013.

Yamin, M. M., & Katt, B. (2022). Modeling and executing cyber security exercise scenarios in cyber ranges. *Computers & Security*, *116*, 102635.

FOI

ISSN 1650-1942

www.foi.se