Aktiv bevakning 1.0

Koncept för framtida bevakning

NIKLAS HALLBERG, SINNA LINDQUIST, PETER NILSSON

FOI-R--5497--SE
ISSN 1650-1942 December 2023

Niklas Hallberg, Sinna Lindquist, Peter Nilsson

Aktiv bevakning 1.0

Koncept för framtida bevakning

Titel	Aktiv bevakning 1.0 – Koncept för framtida bevakning
Title	Active Surveillance 1.0 – Concept for future surveillance
Rapportnr/Report no	FOI-R--5497--SE
Månad/Month	December
Utgivningsår/Year	2023
Antal sidor/Pages	37
ISSN	1650-1942
Uppdragsgivare/Client	Försvarsmakten
Forskningsområde	Ledningsteknologi
FoT-område	Ledning och MSI
Projektnr/Project no	E716160
Godkänd av/Approved by	Linda Sjölin
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Bild/Cover: FOI

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Omvärldsutvecklingen såväl som utvecklingen inom Sverige har bidragit till en ökad och diversifierad hotbild, vilket medför att det finns behov av att utveckla bevakningsförmågan. En effektiv bevakning förutsätter att tidigt kunna upptäcka hot och ha förmåga att avvärja dessa. För att erhålla en proaktiv bevakningsförmåga förutsätts nya tekniska lösningar och att lyckas integrera dessa med arbetsmetoder och organisation samt nya sätt att tänka kring bevakning som en mer proaktiv aktivitet. Målet med studien är ett koncept, kallat Aktiv bevakning, som kan bidra till utvecklingen av bevakning och bevakningssystem. Utformningen av konceptet genomfördes i en iterativ process.

Konceptet för Aktiv bevakning beskrivs i form av en bärande idé, en systemskiss, elva principer och nio förmågor. Den bärande idén är en bevakning som analyserar tillstånd och företeelser relaterat till det skyddsvärda objektet för att proaktivt identifiera indikationer på att något negativt avseende det skyddsvärda som bevakas är på väg att inträffa. För att aktivt kunna avstyra negativa händelser och bryta de negativa händelseförloppen finns ett antal möjliga åtgärder.

Konceptet beskriver en vision av framtida bevakning, kring vilka intressenter kan samlas och diskutera. Därmed är visionen inte är alltför rigid, utan att kan förändras allt eftersom ny kunskap erhållas.

Nyckelord: Koncept, principer, förmågor, aktiv bevakning

Summary

Developments in the world as well as within the nation have contributed to an increased and diversified threat picture, which means that there is a need to develop the surveillance capability. Effective surveillance requires being able to detect threats early and having the ability to ward them off. In order to obtain a proactive surveillance capability, new technical solutions are required and to succeed in integrating these with work methods and organization as well as new ways of thinking about surveillance as more proactive. The objective of this study is a concept that can contribute to the development of surveillance and surveillance systems. The design of the concept was carried out in an iterative process.

The concept of active surveillance is described in the form of a basic idea, a system outline, eleven principles and nine capabilities. The basic idea is a to analyze conditions and phenomena related to the protected object in order to proactively identify indications that something negative regarding the protected object being surveillance is about to occur. In order to actively control negative events and break the negative course of events, there are a number of possible measures.

The concept constitutes a description of a vision of future surveillance, around which stakeholders can gather and discuss. Thus, the vision is not too rigid, but can change as new knowledge is obtained.

Keywords: Concepts, principles, capabilities, active surveillance

Innehållsförteckning

1 Inledning 7
2 Bakgrund 9
2.1 Säkerhetsskyddslagen, skyddslagen och skyddsförordningen .. 9
2.2 Bevakning och teknisk bevakning 9
2.3 Sociotekniska system 10
2.4 Left of Bang 11
2.5 Ledningskoncept 45 12
2.6 Framtida bevakningscentral 13
2.7 Förmågor 13
2.8 Tekniska förutsättningar 14
3 Metod 20
4 Konceptet Aktiv bevakning 21
4.1 Bärande idé 21
4.2 Systemskiss 21
4.3 Principer 23
4.4 Bevakningsförmågor 28
5 Diskussion och slutsatser 31
6 Referenser 33

1 Inledning

Den politiska omvärldsutvecklingen såväl som utvecklingen inom landet har medfört att hoten mot det svenska samhället har ökat. Samtidigt kan antagonistiska aktörers drivkrafter och intentioner vara svåra att fullt ut förutse, upptäcka och förstå. Det finns ett intresse hos vissa av dessa aktörer att genom att påverka skyddsvärda objekt orsaka skada på det svenska samhället, förstöra viktig materiel samt tillförskansa sig utrustning som finns i dessa objekt.

Globaliseringen och vårt öppna samhälle i kombination med tekniska framsteg har skapat nya möjligheter att negativt påverka det som är skyddsvärt (Försvarsberedningen, 2019). Utvecklingen av obemannade farkoster, som numera görs av många olika aktörer och, som finns allmänt tillgängliga, skapar en avsevärt mer komplex bevakningsmiljö. Samtidigt skapar den tekniska utvecklingen förutsättningar till att effektivisera och öka förmågan att bevaka skyddsvärda objekt. Utvecklingen inom områden som sensorteknologi, trådlös kommunikation, datorstöd och obemannade farkoster ger möjligheter till mer omfattande bevakning, som helt eller delvis kan automatiseras.

Den ökade och diversifierade hotbilden innebär att förmågan att upptäcka och avvärja hot behöver utvecklas både vad gäller omfattning och effektivitet. Inom försvarsområdet nyttjas konceptet *gråzon* som glidande skala med fred och krig som ytterligheter för att kunna indikera aktuellt läge. På motsvarande sätt behövs det inom bevakningsområdet, att gå ifrån det binära förhållningssätt som innebär larm respektive icke-larm till förmån för att kunna gradera och värdera observationer, händelser och incidenter. Om bevakningsförmågan ska utvecklas för att kunna hantera en komplex miljö och hotbild krävs ökade resurser i form av personal såväl som teknik.

Det finns en ökad hotbild mot Försvarsmaktens skyddsvärda objekt såsom byggnader, anläggningar, personal och verksamheter. Att inte kunna hantera dessa hot kan få allvarliga konsekvenser, alltifrån att kriminella nätverk kan tillskansa sig vapen och sprängmedel till att Försvarsmakten inte fullt ut kan uppfylla sitt uppdrag att skydda ”Sverige och försvara landets frihet” samt bidrar till att ”skapa fred och säkerhet på andra håll i världen”. Detta ökande hot mot Sverige som nation och de skyddsvärda objekt som finns, gör det angeläget att påskynda arbetet med att säkerställa en ändamålsenlig och effektiv bevakningsförmåga. Denna förmåga måste proaktivt kunna avvärja stöld, otillbörlig användning förstörelse och försvårande av behörigt tillgänglighet av det skyddsvärda.

En effektiv bevakning förutsätter att tidigt kunna upptäcka att något är på gång som kan utgöra ett hot mot det som är skyddsvärt samt att ha förmåga att i ett tidigt skede avvärja hotet för att minimera skador och konsekvenser. Det som begränsar möjligheterna till tidig förvarning är de tekniska lösningar som används och de metoder som de tekniska lösningarna skapar, men också sättet att

tänka kring bevakning som reaktivt. Det finns därmed ett behov av att utveckla existerade system för bevakningen av skyddsvärda objekt, såväl tekniskt som organisatoriskt, för att bli mer proaktiv i bevakningen.

Målet med arbetet som beskrivs i denna rapport är ett koncept som ska bidra till utformningen av bevakning och bevakningssystem, med förmågan att skydda det som är skyddsvärt. Beskrivningen av konceptet ska även bidra till att utveckla sättet att beakta och diskutera proaktiv bevakning på. Konceptet omfattar idéer och principer som behöver beaktas vid utformning av framtida bevakningssystem och förmågor för att uppnå proaktivitet. Det koncept som föreslås i denna rapport benämns *Aktiv bevakning*.

2 Bakgrund

Detta kapitel beskriver förutsättning, perspektiv och andra konceptbeskrivningar som konceptet Aktiv bevakning grundas på, vilket innefattar säkerhetsskyddslagen, skyddslagen och skyddsförordningen, bevakning och teknisk bevakning, sociotekniska system, konceptet *Left-of-bang*, Ledningskoncept 45, koncept för framtida bevakningscentraler samt tekniska förutsättningar.

2.1 Säkerhetsskyddslagen, skyddslagen och skyddsförordningen

Säkerhetsskyddslagen, skyddslagen och skyddsförordningen utgör viktiga ingångsvärden för utvecklingen för utvecklingen av bevakningssystem. Säkerhetsskyddslagen (21018:585)[1] innehåller bestämmelser om vissa skyddsåtgärder mot sabotage, terroristbrott, spionerі och grovt rån (stöld) för byggnader, anläggningar, områden och andra objekt. Skyddslagen (2010:305)[2] gäller då ett skyddsvärde etablerats som ett skyddsobjekt. Ett beslut om skyddsobjekt innebär att obehöriga inte har tillträde, varken i person eller med hjälp av obemannad farkost. Om det bedöms som tillräckligt för att tillgodose skyddsbehovet, kan tillträdesförbudet efter beslut ersättas av ett avbildningsförbud eller förbud mot att bada, dyka, ankra eller fiska.

I Säkerhetsskyddsförordningen (2021:955)[3], som är ett komplement till skyddslagen, fastställs att ”Områden, byggnader och andra anläggningar eller objekt där säkerhetsskyddsklassificerade uppgifter förvaras eller annars behandlas, eller där säkerhetskänslig verksamhet i övrigt bedrivs, ska vara försedda med funktioner för att upptäcka, försvåra och hantera obehörigt tillträde och skadlig inverkan utifrån ett identifierat säkerhetsskyddsbehov.” Den som hanterar säkerhetsskyddsklassificerade uppgifter eller bedriver säkerhetskänslig verksamhet är därmed skyldig att bevaka och skydda dessa skyddsvärden.

2.2 Bevakning och teknisk bevakning

Bevakning syftar primärt till att skydda skyddsvärda byggnader, anläggningar och objekt mot sabotage, terroristbrott, spionerі och grovt rån (stöld) enligt

[1] Säkerhetsskyddslag (2018:585), https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-2018585_sfs-2018-585/

[2] Skyddslag (2010:305), https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/skyddslag-2010305_sfs-2010-305/

[3] Skyddsförordning (2010:523), https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/skyddsforordning-2010523_sfs-2010-523/

skyddslagen. Bevakning kan även omfatta skyddsvärden som inte regleras i skyddslagen och mot andra typer av hot. Centralt för bevakning är att säkerställa att ingen obehörig får tillträde samt att behörig personal bereds tillträde under kontrollerade former.

I vissa dokument framställs teknisk bevakning som ett alternativ till manuell bevakning (Försvarsmakten, 2015). De tekniska bevakningssystemen har traditionellt baserats på den civila sektorns inbrottslarmsystem. Men om bevakningen ska omfatta samtliga typer av hot som anges i skyddslagen så behöver bevakningssystem hantera ett bredare spann av hot än de som förekommer i den civila sektorn. I denna rapport betraktas teknisk bevakning som bevakning som genomförs med stöd av tekniska system. Bevakningen syftar till att säkerställa att de som inte har behörighet hindras tillträde och de som har behörighet ges tillträde.

2.3 Sociotekniska system

Tankarna kring sociotekniska system har sitt ursprung 1950-talets brittiska kolindustri, då vikten av att beakta och förstå hela organisationen, istället för enbart fokusera på att föra in nya tekniska verktyg, blev tydlig (Trist, 1981). I sin allra enklaste form kan sociotekniska system ses som bestående av människor och teknik, men även organisation, processer, mål, kultur, intressenter och regelverk behöver ofta beaktas (Davis m.fl., 2014). Målet, utifrån sociotekniskt designperspektiv, är välfungerade och effektiva verksamheter, i vilka det råder en god arbetssituation för de som ingår i systemet. Detta förutsätter att tekniska såväl som sociala aspekter beaktas vid utveckling och förändring.

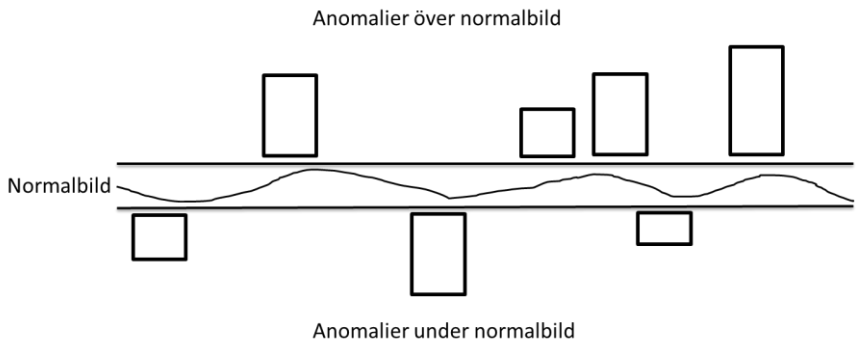
Sociotekniska system är komplexa system, vilket medför att effekterna av att införa tekniska stödsystem är svåra att förutse (Snowden, 2002; Hasan & Kazlauskas, 2009). Detta gör att traditionella, så kallade vattenfallsbaserade, systemutvecklingsmetoder är mindre lämpliga för utveckling av denna typ av system. Istället behöver ett antal förhållningsätt anammas som medger att utvecklingen genomförs i mindre utvecklingssteg, i vilka lärdomar kan dras av vad som leder till en målbild och att dessa nyttiggörs i kommande utvecklingssteg, som exempelvis i en iterativ process (Rogers m.fl., 2023) och inkrementell utvecklingsprocess (Dove m.fl., 2023).

För konceptet Aktiv bevakning kommer ett sociotekniskt perspektiv att genomsyra utvecklingen av konceptet samt dess utformning.

2.4 Left of Bang

Konceptet *Left of Bang* (LoB) har sina rötter i den amerikanska marinkåren och syftar till att tidigt kunna upptäcka svaga signaler som förebådar att någonting allvarligt är på väg att hända (Van Horne & Riley, 2021). Till exempel beskrivs vikten av att kunna känna av skillnader i stämningen på en marknad i Afghanistan för att förstå att en eventuell attack är förestående. LoB-begreppet används även inom den militära domänen som ett generellt begrepp för att hålla sig på rätt sida av en händelse och se till att ”smällen” inte händer. LoB innebär att erhålla en så tidig förvarning som möjligt, beskrivet som en tidslinje där målet är att upptäcka signaler på förestående hot innan själva ”bangen” händer.

För att kunna agera enligt LoB behövs en lägesbild som beskriver en normalbild (baslinje) och förändringar (anomalier) av normalbilden (Figur 1). Anomalierna kan antingen vara över normalbilen, vilket innebär *saker som händer men som vanligtvis inte händer*, eller *någon typ av närvaro (tex. person och sak) som vanligtvis inte brukar närvara* alternativt under normalbilden vilket motsvara *saker som inte händer men som brukar hända* eller *någon typ av närvaro som inte är närvarande men som brukar närvara*.



Figur 1: En lägesbild med normalbild och med förändringar (anomalier) i relation till normalbilden.

För att förstå vad som är normalbilden respektive anomalier används vedertagna och generella metoder för att studera och beskriva omgivningen med de människor och aktiviteter som händer runt en given plats. Dessa beskrivningar ingår sedan i det system som ska stödja operatörer att fatta beslut i varje given situation.

LoB är relevant för konceptet Aktiv bevakning då det poängterar vikten av att vara proaktiv. I detta igår att förstå normalbilden för att i sin tur förstå eventuella anomalier, i syfte att upptäcka när något är på väg att hända, ligga steget före en antagonist och kunna agera innan något allvarligt inträffar.

2.5 Ledningskoncept 45

Ledningskoncept 45 utvecklades inom ramen för Försvarsmaktens Huvudstudie Ledning (Försvarsmakten, 2021). Syftet med konceptet är inrikta transformationen av Försvarsmaktens ledningssystem, operativt från och med 2045. Konceptet innefattar en bärande idé och åtta principer. Den bärande idén är en ledning som är effektfokuserad, agil och resilient, som ger förutsättningar för att agera enskilt och tillsammans med andra (Granåsen m.fl. 2021). *Effektfokuserad ledning* innebär ett fokus mot *vad som ska uppnås* snarare än hur och med vad. *Agil ledning* innebär att proaktivt och kontinuerlig optimera ledningssystem. *Resilient ledning* innebär en inneboende motståndskraft hos ledningssystem att hantera störningar.

Agilitet och resiliens hos ledningssystem möjliggör att sömlöst flytta förmågan att leda en insats mellan olika staber, ledningsplatser och ledningsnivåer. Ur ett agilt perspektiv kan detta göras proaktivt, utifrån det som bedöms vara det mest lämpliga i den givna situationen. Från ett resilient perspektiv görs detta reaktivt när förmåga att leda vid en ledningsplats gått förlorad.

De åtta principerna är:

1. *Ledning över domän- och stridskraftsgränser* – Ledningssystem kan leda verkansresurser från samtliga stridskrafter för att verka mot motståndare i samtliga domäner.
2. *Uppdragsstyrning som ledningsform* – Ledning sker utifrån uppdragsstyrning, i vilken graden av restriktioner som ges i ett uppdrag anpassas efter behovet av samordning.
3. *Anpassning av ledningsförmåga* – Ledningssystemets förmåga anpassas avseende kapacitet och kompetens så att det motsvarar verkansystemets behov av ledning.
4. *Anpassning av ledningsorganisation* – Ledningsorganisationen anpassas efter uppgift, uppdrag och andra förutsättningar.
5. *Anpassning av ledningsmobilitet* – Ledningsplatser kan vara fasta eller rörliga samt växla däremellan.
6. *Anpassning av ledningsplatsers geografiska spridning* – Ledningsplatsers spridning kan växla mellan att vara samlad och spridd över ett större område, med anpassning till situationen.
7. *Interoperabilitet* – Väl definierade gränssnitt möjliggör samverkan mellan nationella stridskrafter, med andra nationers militära styrkor och med icke-militära organisationer.

8. *Kontinuerlig utveckling* – Ledningssystemet förbättras kontinuerligt genom att tillföra ny och avveckla uttjänt teknik samt förändra arbetssätt och organisation vid behov.

Ledningskoncept 45 är relevant att beakta för konceptet Aktiv bevakning eftersom det skulle harmonisera Försvarsmaktens inriktning för bevakning, skydd och ledning.

2.6 Framtida bevakningscentral

Lindquist m.fl. (2022) beskriver ett koncept för framtida bevakningscentraler, i vilket en bevakningscentral ses som den fysiska eller virtuella plats varifrån bevakningen sker. Enligt konceptet ska framtidens bevakningscentraler ha förmåga att inhämta information, skapa och upprätthålla lägesbild och besluta om åtgärd samt leda denna. De ska vara proaktiva för att förekomma negativa händelser, detta genom att bland annat aktivt eftersöka relevant information. De ska fungera i alla konfliktnivåer och kunna hantera komplexa kombinationer av flera händelser, vilket förutsätter att de kan upptäcka och tolka svaga signaler och incidenter för att förstå situationer och händelser. De ska vara analytiker-orienterade, vilket innebär att de tekniska systemen stödjer människor att förstå situationer och fatta beslut.

Konceptet föreskriver tre roller vid bevakningscentraler: beslutsfattare, analytiker och tekniker. Personalen på bevakningscentraler ska kunna övervaka larmtablåer, verifiera inkommande larm, styra kameror och granska videoflöden och genomföra fjärrpatrullering. De ska även följa omvärldsläget, inhämta lägesbild från andra aktörer, ta emot rapporter, kontrollera tillträdet samt kontinuerligt utveckla bevakningsmetodik och procedurer. Ledningsfunktionen vid bevakningscentraler ska planera bevakningen med hänsyn till omvärldsläget samt prioritera mellan larm, incidenter och händelser. De personer som arbetar med bevakningen måste ha en förståelse för det aktuella bevakningsobjektet. För att lösa tilldelade uppgifter måste de som är involverade i bevakningen ha kunskap och kompetens avseende sitt mandat att fatta beslut om åtgärd, de tekniska systemen och deras funktioner, genomförandet av analyser samt säkerställa att de tekniska systemen fungerar.

Detta koncept bidrar till konceptet Aktiv bevakning med en beskrivning av hur framtida bevakningscentraler är tänkt att fungera.

2.7 Förmågor

Det finns ett omfattande intresse för att nyttja förmågor som grund för utveckling (Antunes, & Borbinha, 2013). En utmaning med att arbeta med förmågor som grund för utveckling är att det inte finns någon allmänt accepterad och fastställd definition av begreppet (Lindbom & Tehler, 2020). Ordet förmåga används för

att definiera resurser som exempelvis brandbilar och ambulanser såväl som den effekt som ska kunna åstadkommas. I denna rapport används begreppet *förmåga* som förmågan att kunna åstadkomma något, exempelvis förmåga att förhindra obehörigt tillträde eller förmåga att upptäcka förberedelser till sabotage.

Olsén m.fl. (2023) utvecklade modell i form av en struktur med förmågor som stöd för att utveckla och vidmakthålla aktörsgemensam krishanteringsförmåga. Denna modell består av förmågor som avser att kunna åstadkomma något, exempelvis att upprätta och vidmakthålla en lägesbild. Förmågorna är även generiska i den mening att de är oberoende av vilken typ av händelse som inträffat, när den har skett, var den har inträffat samt vilka aktörer som deltar i hanteringen.

Modellen omfattar 14 förmågor som är indelade kärnförmågor, stödjande förmågor och förutsättningsskapande förmågor. Kärnförmågorna utgör den aktörsgemensamma krishanteringsförmågan, det vill säga det som ger systemets existensberättiganden. De stödjande förmågorna bidrar till upprätthållandet av kärnförmågorna. De förutsättningsskapande förmågorna skapar förutsättningarna för att genomföra aktörsgemensam samverkan.

Denna modell bidrar till utvecklingen av konceptet Aktiv bevakning med en struktur och ett antal förmågor vilka användas för att utveckla en förmågemodell för teknisk bevakning.

2.8 Tekniska förutsättningar

Det finns ett antal tekniker som kan bidra till en mer effektiv bevakning. I detta kapitel redovisas några av dessa och den påverkan som det skulle kunna ha för att realisera teknisk bevakning.

2.8.1 Artificiell intelligens

Utvecklingen inom området *artificiell intelligens* (AI) går snabbt och AI-baserade system bidrar till att lösa alltmer komplexa uppgifter. Framsteg inom AI-området har medfört en snabb utveckling inom många områden såsom automation, analys av stora datamängder och diagnostik. Men det finns även utmaningar inom AI-området vilka innefattar otillräcklig mängd av träningsdata för att erhålla ett önskat beteende, säkerställa att beteendet är det förväntade, transparens avseende hur AI-system kommer fram till resultat samt att skydda dessa system mot avsiktlig vilseledning (Luotsinen, 2018; Svenmarck, 2018; Nilsson, 2017). Andra utmaningar som lyfts fram utgörs av höga kostnaderna för utveckling och underhålla av AI-modeller (Chen & Das, 2023), sårbara mot attacker mot ingående AI-modell, (Kamrani, m.fl., 2023) och att de nyttjas för att fabricera innehållet i texter, bilder, video och ljud (Rosell, m.fl., 2022).

Vid införandet av AI-baserade system bör det beaktas hur relationen mellan människans och system ska utformas avseende beslutsfattande. Det finns modeller som beskriver detta: In-the-loop, On-the-loop och Out-of-the-loop (Freedberg, 2019). *In-the-loop* innebär att en människa fattar beslutet att agera utifrån information och förslag som ett AI-system tillhandahåller. *On-the-loop* innebär att ett AI-baserat system även kan fatta beslut och ge order om verkan, men att en människa övervakar processen och har möjlighet avbryta och stänga ner systemet. *Out-of-the-loop* innebär att en människa ger en instruktion till ett AI-baserat system och därefter överlåter genomförandet, inklusive beslutsfattanden, helt till systemet, utan att övervaka.

För teknisk bevakning kan AI bidra till en effektivare insamling och snabbare analys av information än vad som sker idag, och även skapa planer för till exempel rondering (Livermore, 2019). För konceptet Aktiv bevakning ger AI en möjlighet att analysera stora mängder historisk information för att förstå nuläget, men också om den framtida lägesbilden.

2.8.2 Analys och visualisering av stora datamängder

Allt snabbare datorer i kombination med alltmer sofistikerade AI-tekniker kommer att öka förmågan att analysera och dra slutsatser från stora datamängder, vilka kan bestå av heterogen data (ex. text, bilder, video och ljud). Denna förmåga kan bidra till en ökad situationsförståelse och att kunna uppfatta svaga signaler av att något är på väg att hända (Haridas, 2018). Det finns ett stort antal tekniker och verktyg för visualisering av och interaktion med stora datamängder, avseende dess innehåll såväl som datakvalité (Jändel, m.fl., 2016).

För teknisk bevakning kan omfattande data samlas in från exempelvis sensorer, satellitbilder, signalspaning och social media. Med rätt verktyg för analys och visualisering skapas förutsättningar för en bättre situationsförståelse och för att tidigt kunna identifiera och tolka svaga signaler, vilket är en del av konceptet Aktiv bevakning.

2.8.3 Multimodal analys (bild- och ljudanalys)

Multimodal analys innebär att flera olika typer av sensorer eller källor kombineras. Skälen till att vilja nyttja multimodal analys varierar. Ett skäl kan vara svaga signaler, dvs. att ingen enskild sensor kan klara av att upptäcka det som söks men att data från olika sensortyper kan vägas samman till en rikare analys med högre träffsäkerhet. Exempel på detta kan vara att elektrooptiska sensorer inom olika våglängdsområden kombineras eller att radar, lidar (Light Detection and Ranging) och elektrooptiska sensorer kombineras. Multimodal analys kan dock vara svårt eftersom dataformat varierar mellan olika sensortyper och därför inte är direkt jämförbara. Multimodal analys innebär också att kunna dra slutsatser ur kombinationer av olika former av data, såsom bild, ljud och text

(Blasch, m.fl., 2014). Detta innebär att förståelsen för en företeelse skulle kunna erhållas då flera typer av data kombineras i en analys. Ett exempel är att samanalyserna information som finns om en specifik individ i texter, bilder, filmer och ljudinspelningar för att erhålla kunskap om dennes förehavanden och eventuella framtida handlingar.

2.8.4 Extended Reality

Det finns olika former av virtuella miljöer och kombinationer av virtuella inslag i verkliga miljöer, som användare kan närvara i och integrerar med. *Extended Reality (XR)* är ett samlingsnamn för samtliga dessa former som kombinerar det verkliga och det virtuella (Fast-Berglund m.fl., 2018). De vanligaste XR-formerna utgörs av Virtual Reality (VR), Augmented Reality (AR) och Mixed Reality (MR). *VR* innebär att innehållet är datorgenererat och att användare är frikopplade från den verkliga miljö som de befinner sig i. *AR* används för att förstärka uppfattningen av verkligheten, genom att den verkliga miljön överlagras med datorgenererade objekt och information. Förstärkningen kan innefatta olika sinnesmodeliteter, syn, hörsel och känsel. Till exempel kan skyltar med främmade språk överlagras alternativt läsas upp med det egna språket. Inom *MR* kombineras den verkliga miljön med det datorgenererade materialet. Det som skiljer MR från AR är att inom MR kan datorgenererade objekt påverka objekt i den verkliga värden. MR och AR används dock ofta med samma betydelse.

Inom området *digitala tvillingar* (eng. digital twins) skapas virtuella avbilningar av fysiska objekt (Zang m.fl., 2022). En digital tvilling är en digital modell, med koppling till det motsvarande fysiska objektet. Denna koppling innebär att påverkan på och förändringar av det fysiska objektet respektive den virtuella tvillingen överförs direkt mellan dessa. Det är också möjligt att simulera påverkan på den virtuella tvillingen utan att det fysiska objektet skada.

För teknisk bevakning kan XR-baserade tekniker bidra till utbildning och träning av bevakningspersonal. Vid skyddsvärda objekt skulle AR kunna nyttjas för att överlagra information om t.ex. objekt, dolda ting, bevakningssystem. VR och en digital tvilling av en anläggning skulle kunna nyttjas för att genomföra virtuella patrulleringar, med känsla av att vara på plats och möjlighet att direkt påverka objekt i anläggningen.

2.8.5 Internet of Things

Internet of Things (IoT) är ett samlingsbegrepp för enheter som är anslutna till internet, med vilket de kan utbyta information och styra andra enheter respektive styras av andra enheter. Antalet IoT-enheter ökar i snabb takt och inom den civila marknaden är det enbart fantasin som sätter gränser för vad som ansluts till internet. Även inom den militära sektor pågår det initiativ som baseras på IoT (Suri m.fl., 2016). Det finns även anpassningar av IoT:s arkitekturer till militära

tillämpningar såsom Internet of Military Things (IoMT), Military Internet of Things (MIoT), Battle Internet-of-Things (IoBT) och Internet of Intelligent Battle Things (Kott m.fl., 2016; Yushi m.fl., 2012; Castiglione m.fl., 2017; Kott, 2018). Det finns flera fördelar med att nyttiggöra civil IoT-teknik för militära tillämpningar, exempelvis för informationsinhämtning och ökad automatisering. Att integrera civil IoT-teknik med militära system är dock problematiskt, till exempel avseende IT-säkerhetsaspekter och interoperabilitet (Tortonesi m.fl, 2016).

För teknisk bevakning kan IoT-tekniker nyttjas för att integrera olika typer av sensorer och på så vis skapa dynamiska heterogena sensornätverk med plug-and-play funktion.

2.8.6 Obemannade farkoster

Obemannade farkoster kan vara helt fjärrstyrda eller i varierande grad autonoma (Rantakokko, 2019). De kan vara luft-, mark- och sjöbaserade och ha förmåga att hantera vitt skilda uppgifter såsom transport av gods, informationsinhämtning, utgöra kommunikationsnod och verkan. De kan uppträda enskilt eller i form av svärmar.

För teknisk bevakning kan obemannade farkoster nyttjas för att inhämta information, följa inkräktare och påvisa närvaro. För att inhämta information kan de nyttjas för patrullering och för dynamisk anpassning av området som övervakas. De kan även nyttjas när fast monterade sensorer inte tillåts eller om en situation är farlig för människor.

2.8.7 Bärbara beslutsstöd

Informationstekniken blir allt mindre, lättare och strömsnålare, vilket möjliggör kraftfullare bärbara beslutsstöd. Mobiltelefoner motsvarar redan i dag en kraftfullare dator, med betydande kapacitet avseende beräkningar, lagning och överföring av information. Informationsteknik har även blivit alltmer integrerad i befintliga tillhörigheter som traditionellt bärs, som klockor, ringar, armband och glasögon.

För teknisk bevakning kan mobila beslutsstöd kunna erbjuda ett större informationsutbyte mellan den fasta bevakningscentralen och personal som rör sig i det skyddsvärda objektet.

2.8.8 Samband och kommunikation

Samband och kommunikation är en grundläggande förmåga för bevakning och ledning. Förnärvarande byggs 5G (5:e generationens) mobilnät vilket kommer att medför en betydligt ökad kapacitet, jämfört med tidigare mobiltelefoninät. Runt år 2030 kommer sannolikt 6G (6:e generationens) mobilnät att börja nyttjas. 6G

förväntas öka såväl kapaciteten som hastigheten med hastigheter upp mot 1 terabit per sekund (Alpman, 2019). Laserbaserad kommunikation ger förutsättningar för att etablera samband med avsevärt högre takt i dataöverföring och som är svårt att upptäcka och störa (Kaushal & Kaddoum, 2017). En nackdel med denna typ av kommunikation är dess beroende av rätt väder och line-of-sight (Ladetto, 2016). Nederbörd och dimma kan försvåra möjligheten att nyttja laser.

För teknisk bevakning innebär den ökande förmågan till kommunikation och samband att sensorer kan vara rörliga och därmed täcka större områden. 5G-näten kommer att erbjuda en infrastruktur för IoT:er (Li m.fl., 2018).

2.8.9 Interaktionstekniker

Tangentbord, datormöss, joystickar och skärmar har traditionellt utgjort gränssnitt för tekniska system. Det finns alltfler exempel på system som medger interaktion med tal, gester och ögonrörelser, vilket anses vara mer naturligt för människor (Pettitt m.fl., 2018; Adhanom m.fl., 2023). Antalet system som nyttjar röstbaserad interaktion har ökat kraftigt. Röststyrning har också blivit också allt bättre, både avseende att uppfatta rätt och urskilja mänskliga röster i miljöer med omkringliggande ljud. Röststyrning för mobiltelefoner är relativt väl etablerat (Mittal & Singh, 2016). När det gäller gestbaserad interaktion så nyttjas detta i hög utsträckning för interaktion med touchskärmar, men det finns arbete kring att kunna styra via gester på distans utan att beröra det som ska styras (Huang m.fl., 2018). Det finns även armband och ringar som gör det möjligt att interagera med gester (Korpela & Walker, 2018). Att följa ögonrörelser har tillämpas inom många år för att utforma exempelvis piloters instrumentering och kontroller (Fitts m.fl., 1950). Ögonrörelser kan även nyttjas som indata till system för att öka kvalitet, upplösning och informationsrikedomen på de objekt som användaren för tillfället tittar på (Jacob & Karn, 2003). Interaktion med rörelser har främst använts för att stödja individer som saknat förmåga att interagera via tangentbord och mus, men studier visar även på möjligheter för icke rörelsehindrade att använda ögonrörelser som ett komplement till de mer traditionella teknikerna för interaktion (Paing m.fl., 2022; Jacob & Karn, 2003).

För teknisk bevakning kan röststyrning såväl som gestsstyrning vara av intresse. Men i de flesta tillämpningar kommer säkerligen tangentbord och datorskärmar, stationära och mobila, vara den lämpligast form för interaktionen. För teknisk bevakning kan tekniken att följa ögonrörelser nyttjas för att anpassa lägesbilden genom att öka detaljeringsgraden av och tillföra information om det som operatören för tillfället tittar på.

2.8.10 Sensorer och sensorsystem

Förenklat kan ett sensorsystem beskrivas som att det består av en eller flera sensorer samt en enhet eller flera enheter för dataanalys. Sensorernas funktion är

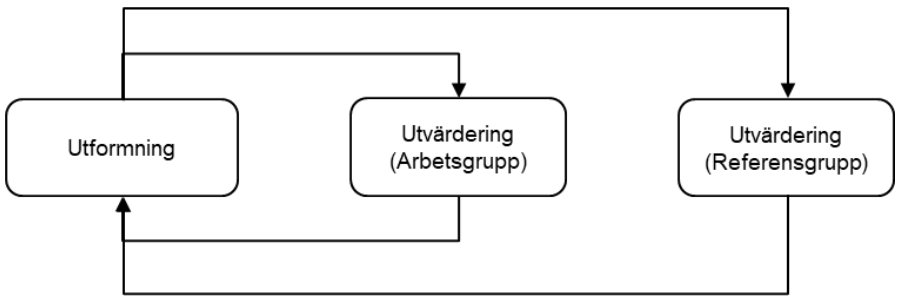
att inhämta data från omgivning. Det finns många typer av sensorer för att fånga exempelvis ljud, ljus, bild och video, värme och kyla, rök, radarvågor, tryck, vibration och rörelse. Analysenheternas funktion är att analysera den data som sensorerna producerar, för att detektera och identifiera objekt och händelser (Näsström, m.fl., 2018). De senaste årens utveckling inom AI har starkt bidragit till att öka förmågan hos sensorsystem, så att de i många fall är både bättre och snabbare än människor på att upptäcka och identifiera militära objekt (Näsström 2022).

Sensorer kan vara fasta respektive mobila. Att kombinera mobila och fasta sensorer ger potential att bidra med bättre underlag (sensordata) för att detektera hot, eftersom fasta sensorerna kan nyttjas för att ge inriktning för mobila sensorer, som då kan närma sig det som är av intresse (Nilsson, m.fl., 2020). Förmågan att styra mobila sensorer är därmed en viktig förmåga. Avancerade sensorsystem har förmåga att automatiskt upptäcka objekt och hot samt följa dessa. En utmaning är att få alltfler sensorsystem att samverka, så att exempelvis ett sensorsystem sömlöst kan överlämna följningen av ett objekt till ett annat sensorsystem. För teknisk bevakning utgör de alltmer avancerade sensorerna och sensorsystemen en grundförutsättning för att öka bevakningsförmågan.

3 Metod

Konceptet Aktiv bevakning utvecklades i en iterativ process i vilken beskrivningar, systemmodeller, scenarier, konceptidéer, förmågor och principer utvecklades och utvärderades (Figur 2). Beskrivningar och modeller syftade till för att tydliggöra begrepp och resonemang. Syftet med scenarierna var att testa framtagna modellers och konceptidéers relevans. Arbetet genomfördes i korta respektive längre interaktioner. De kortare iterationerna utgjordes av eget arbete och diskussioner i arbetsgruppen, baserat bl.a. på läsning av relevant litteratur och synteser från tidigare projekt. De längre iterationerna innefattade avstämningar med en referensgrupp.

Arbetsgruppen omfattande kompetenser avseende teknisk bevakning, ledning, människa-systeminteraktion och systemutveckling. Referensgruppen bestod av personer som under längre tid arbetat med utveckling av teknisk bevakning och personer som besitter hög grad att teknisk kompetens. Utgångspunkter för arbetet har varit att betrakta helheten som ett socioteknisk system samt konceptet för Left of Bang (LoB), Ledningskoncept 45, koncept för framtida bevakningscentral och tekniska förutsättningar.



Figur 2: Arbetet med att ta fram konceptet genomfördes i en iterativ process. I denna process utvecklades och utvärderades beskrivningar, systemmodeller, scenarier, konceptidéer, förmågor och principer.

4 Konceptet Aktiv bevakning

Konceptet för Aktiv bevakning beskrivs i form av en bärande idé, en systemskiss över bevakningssystemet med generiska funktioner, elva principer och nio förmågor.

4.1 Bärande idé

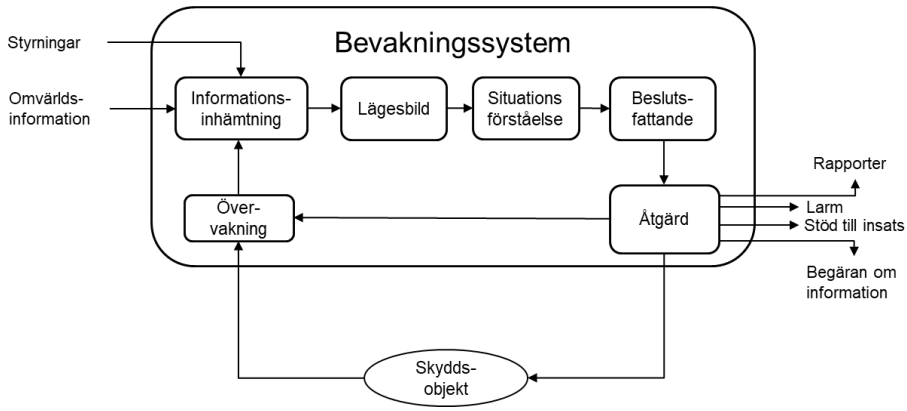
Den bärande idén med konceptet Aktiv bevakning är en bevakning som analyserar tillstånd och företeelser relaterat till det skyddsvärda objektet för att proaktivt identifiera indikationer på att något negativt avseende det skyddsvärda som bevakas är på väg att inträffa. För att aktivt kunna avstyra negativa händelser och bryta de negativa händelseförloppen finns ett antal möjliga åtgärder.

Bevakningssystem som baseras på detta koncept upptäcker, övervakar, motverkar och dokumenterar enskilda och kedjor av händelser för att proaktivt förhindra:

- Stöld av det skyddsvärda.
- Otillbörlig användning av det skyddsvärda.
- Förstörelse av det skyddsvärda.
- Försvårande av tillgänglighet till det skyddsvärda.

4.2 Systemskiss

Systemskissen avseende Aktiv bevakning beskriver de funktioner som behövs (Figur 3). För att uppnå proaktivitet behöver de ingående funktionerna vara kompetenta och snabba. Tiden, från att signaler uppfattas av sensorerna eller av omvärlden tills åtgärder är gjorda, är av betydelse för att avvärja hot och minimera konsekvenserna av försök till påverkan av skyddsvärda objektet.



Figur 3. Systemskiss för Aktiv bevakning. Funktionerna utgörs av övervakning, informationsinhämtning, lägesbild, situationsförståelse, beslutsfattande och åtgärd. Det finns en koppling mellan dessa funktioner och de förmågor bevakningssystem måste inneha.

Funktionen *övervakning* samlar in data om tillstånd och företeelser relaterat till det skyddsvärda objektet inklusive bevakningssystemet. Resultatet från denna funktion är data.

Funktionen *informationsinhämtning* tar emot data från övervakningsfunktionen och information avseende omvärlden, vilket kan innefatta både öppen och hemlig information från egna och andra källor, samt styrningar innefattande exempelvis förändringar avseende bevakningsförmåga och tillträde. Funktionen kvalitetssäkrar och säkerställer även att information är i rätt format samt lagrar informationen.

Funktionen *lägesbild* sammanställer informationen till en lägesbild. Funktionen möjliggör att lägesbilden kan beaktas från olika perspektiv, exempelvis all information relaterat till ett objekt och förändringar över tid.

Funktionen *situationsförståelse* analyserar lägesbilden för att identifiera händelser, indikationer på anomalier och att något utgör ett hot. Utifrån denna analys genomförs ytterligare analyser av hot avseende möjliga konsekvenser samt åtgärder som kan bidra till att avstyra negativa händelser och bryta händelseförlopp som kan utvecklas till ett reellt hot. Resultat av funktionen är förslag på åtgärder inklusive konsekvenser.

Funktionen *beslutsfattande* fattar beslut om de åtgärder som ska genomföras, respektive inte genomföras. Denna funktion tar hänsyn till rådande lagar och uppsatta handlingsregler.

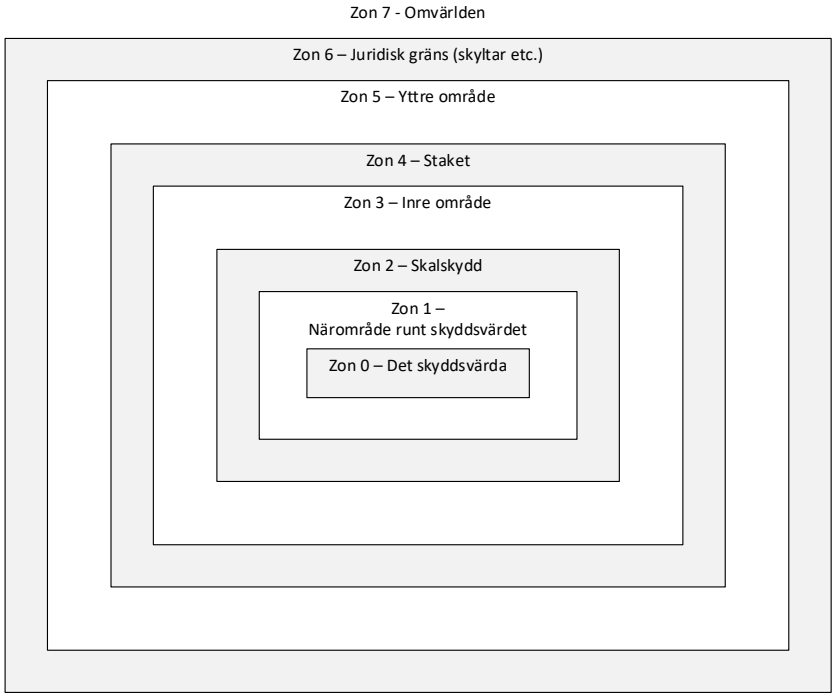
Funktionen *åtgärd* omsätter beslut till faktiska åtgärder. Detta innefattar till exempel produktion av rapporter, skickande av larm, stöd till insats och begäran om information, anpassning av övervakningen, förändra inpassering och tillgång samt att aktivera säkerhetsmekanismer vid det skyddsvärda objektet.

4.3 Principer

Detta avsnitt beskriver de elva principer som ingår i konceptet Aktiv bevakning. Principerna tydliggörs med exempel på vad dessa innebär.

4.3.1 Kvalificerad informationsinhämtning

Principen *Kvalificerad informationsinhämtning* innebär att information inhämtas från samtliga de områden som beskrivs i områdesmodellen (Figur 4).



Figur 4: Områdesmodell som illustrerar de olika områdena runt det skyddsvärda objektet, som representeras av zon 0. Denna modell utgör ett stöd för att diskutera informationsinhämtning.

Informationsinhämtning sker via inpasseringssystem och egna sensorer, andra bevakningscentraler, internetforum och sociala medier samt myndigheter. Vilken information som inhämtas är anpassat till de förutsättningar som respektive skyddsvärt objekt medger. Om ytterligare information om en händelse behövs, kan denna information aktivt efterfrågas och inhämtas. Information kan inhämtas autonomt, semi-autonomt respektive operatörsstyrt.

Exempel: En detektor upptäcker att ett fordon (en personbil) passerar in i det yttre området (zon 5) med riktning mot staketet (zon 4). Detektorn aktiverar en kamera som läser av bilens nummerplåt när denna närmar staketet och skickar en begäran om information om fordonet och dess ägare till bilregistret. Föraren lämnar fordonet och går fram till staket, tar fram en kamera och börjar fotografera mot det skyddsvärda objektet, vilket detekteras av bevakningssystemets sensorer.

4.3.2 Informationsrik lägesbild

Principen *Informationsrik lägesbild* innebär att den information som inhämtas analyseras och omgående tillförs lägesbilden. Lägesbilden beskriver tillstånd och företeelser avseende det skyddsvärda objektet, den närliggande omgivningen, omvärlden och det tekniska bevakningssystemets status. Lägesbilden kan betraktas ur ett flertal perspektiv, såsom förändringar över tid och rum.

Exempel: Allteftersom information om fordonet inkommer uppdateras lägesbilden. En lägesbild med perspektiv på detta fordon upprättas, med exempelvis information om var fordonet befunnits tidigare och om ägaren varit involverade i några tidigare brottsliga handlingar. Lägesbilden visar även om det är ägaren till fordonet som är den aktuella föraren.

4.3.3 Aktiv situationsförståelse

Principen *Aktiv situationsförståelse* innebär att utifrån nuvarande lägesbild samt historiska lägesbilder och händelser aktivt söka förståelse för orsakssamband samt förutse framtida händelser och händelseutvecklingar (Endsley & Garland, 2000). Denna analys innefattar även sannolikhet (risk) för att hot realiseras och vad detta skulle ge för konsekvenser. En aktiv situationsförståelse innebär också att förstå vilka motåtgärder som ger störst effekt till lägst kostnad, vilka konsekvenser dessa får och när dessa ska sättas in.

Exempel: Utifrån lägesbilden med perspektivet på fordonet påbörjas en analys som visar att beteendet avviker från normalbilden. En fördjupad analys sker av förarens tidigare aktiviteter och nuvarande agerande och resulterar i vilka aktiviteter som kan komma att ske samt tänkbara konsekvenser av dessa.

4.3.4 Anpassad bevakningsförmåga

Principer *Anpassad bevakningsförmåga* innebär att bevakningen anpassas till situationen. Detta kan ske genom att en befintlig bevakningsförmåga ökas respektive reduceras, men även genom att nya bevakningsförmågor tillförs respektive att befintliga bevakningsförmågor avvecklas.

Exempel 1: Det bedöms finnas ett avsevärt ökat hot mot ett skyddsvärt objekt. Den bevakningscentral som sköter bevakningen av objektet har inte tillräcklig

kapacitet. Därav beslutas att två andra bevakningscentral under en tid ska stödja bevakningen av objektet. Dessa två bevakningscentraler bidrar med ökad analysförmåga av sensorbaserad information samt med förmågan att följa diskussioner i sociala medier som berör objektet. Den senare förmågan saknades tidigare vid den ansvariga bevakningscentralen.

Exempel 2: I samband med den misstänkta bilens närvaro sker en varutransport till det skyddsvärda objektet. På grund av närvaron av den misstänkta bilen bedöms det föreligga en ökad sårbarhet. Därför beordras ökad vaksamhet och en vakt skickas ut för att möta upp transporten och övervaka avlastningen. En drönare skickas upp för att bevaka området kring det skyddsvärda objektet och därmed ökas bevakningsförmågan.

4.3.5 Aktivera motåtgärder

Principen *Aktivera motåtgärder* innebär att sätta in adekvata och effektiva motåtgärder för att förhindra, fördröja, försvåra och minimera konsekvenser. För att avgöra vilka motåtgärder som är de lämpligaste beskrivas dessa med effekter och konsekvenser. Att påvisa närvaro, låsa dörrar, utrymma områden, rökfylla lokaler samt höga ljud och skarpt ljus är exempel på åtgärder som kan förhindra och fördröja antagonister.

Exempel: Två skyddsvakter i bil beordras mot platsen där det misstänkta fordonet befinner sig, för att i ett första skede påvisa närvaro samt i ett senare skede vid behov kunna ingripa mot inkräktaren.

4.3.6 Motståndskraft

Principen *Motståndskraft* (resiliens) innebär att bevakningsförmågan står emot störningar och återhämtar sig vid bortfall. Om vissa delar av ett bevakningssystem inte fungerar som det ska, nyttjas andra delar för att täcka i möjligast mån för de delar som förlorats. Principen innebär också att arbetet med att återskapa de delar som förlorats påbörjas omgående. Motståndskraft förutsätter en robusthet och oftast någon form av redundans.

Exempel: I samband med att transporten ska genomföras sker ett strömavbrott i det område i vilket det skyddsvärda objektet finns. Orsaken till strömavbrottet är okänd, men ett antagonistisk agerade kan inte uteslutas. Under den första tiden efter strömavbrottet nyttjas batterier för att hålla bevakningssystemet igång. Men ett längre strömavbrott skulle innebära att bevakningsförmågan riskera att gå förlorad. Därför flyttas diselgeneratorer till det skyddsvärda objektet för att säkerställa strömförsörjningen och därmed bevakningsförmågan.

4.3.7 Harmoniserat sociotekniskt system

Principen *Harmoniserat sociotekniskt system* innebär en balanserad fördelning av uppgifter mellan beslutsfattare, operatörer och tekniska stödsystem, för att åstadkomma en effektiv och proaktiv bevakning. Detta förutsätter att bevakningssystemet betraktas som ett sociotekniskt system, för att vid utveckling och vidmakthållande säkerställa en god balans av arbetsmetodik, tekniska stödsystem, organisation samt operatörernas kompetens och arbetssituation. Införande av ny teknik leder till nya arbetssätt, vilket gör att utveckling av teknik och arbetssätt måste gå hand i hand. Vid utveckling och vidmakthållande av bevakningssystem ska även hänsyn tas till att etablera och stärka en god kultur, som främjar ett hållbart arbetsliv.

Exempel 1: Det tekniska systemet analyserar kontinuerligt inkommande information. När något anses som tillräckligt anmärkningsvärt påtalar systemet detta för operatören som då kan överta analysen. Systemet förbereder en incidentrapport för dokumentation av händelsen, vilken operatören kompletterar och skickar vidare.

Exempel 2: När ett nytt tekniskt stödsystem ska införas medverkar de framtida användarna till utformningen av detta. Prototyper av systemet testas med faktiska operatörer, samt eventuellt med andra intressenter eller avnämare av information. Flera scenarier nyttjas vid utvärderingen för att säkerställa att systemet inte försvårar en effektiv bevakning och orsakar en sämre arbetsmiljö.

4.3.8 Digitalisering

Principen *Digitalisering* innebär att modern informationsteknik nyttjas för att öka bevakningsförmåga. Tekniken nyttjas som stöd för att till exempel inhämta information, analysera situationen, skapa lägesbilder, upptäcka anomalier, visualisera lägesbilder och analyser samt skapa beslutsunderlag och rapporter. Vidare nyttjas informationsteknik för att spara, vidmakthålla och tillgängliggöra den information som inhämtas och skapats, bland annat för användning vid framtida analyser.

Exempel: Sensorer detekterar det misstänkta fordonet och sensorsystemen skickar vidare information till ett lägesbildssystem som kvalitetssäkrar och sammanställer informationen för en uppdatering av lägesbilden. En operatör ber lägesbildssystemet att skapa en lägesbild utifrån fordonet och visualiserar denna. Operatören har därefter möjlighet att interagerar med den visualiserade lägesbilden, bland annat genom att begära ytterligare analyser och bedömningar avseende möjliga händelseutvecklingar.

4.3.9 Transparens

Principen *Transparens* innebär att operatörer kan se hur och med vilken information som det tekniska systemet skapar lägesbilder, analyserar och

sammanfattar (Bengtsson, m.fl., 2020). Genom en god transparens kan förtroende för och tilliten till de tekniska systemen upprätthållas på en hög nivå. Transparens skapar även förutsättningar för att vidareutveckla bevakningssystemet.

Exempel: En operatör känner sig tveksam till den upprättade lägesbilden avseende det misstänkta fordonet. Därför ber operatören att det tekniska system ska redovisa vilken information och vilka analyser som ligger till grund för den information som visas i lägesbilden.

4.3.10 Interoperabilitet

Principen *Interoperabilitet* innebär att en socioteknisk interoperabilitet finns med andra bevakningssystem och informationskällor (Scheplitz, 2022). Regelverk, personalens kompetens, verksamhetsgenomförandet och standardiserade protokoll säkerställer möjligheten att kunna inhämta och delge information mellan bevakningscentraler och andra i samhället berörda aktörer. Interoperabilitet bidrar till att upprätthålla en lägesbild som är tillräckligt informationsrik för att svaga signaler och indikationer på att något är på gång som kan utgöra ett hot mot det skyddsvärda objektet upptäcks.

Exempel 1: Information inhämtas sömlöst avseende det misstänkta fordonet och dess ägare från bilregistret, samt information om strömavbrottet från ansvarig organisation för elförsörjningen.

Exempel 2: En händelse vid ett skyddsvärt objekt i en annan del av landet gör att det behövs förstärkning med personal. Eftersom gränssnitten till de tekniska systemen är lika de gränssnitt som den tillkomna personalens vanligtvis arbetar med kan de snabbt sätta sig in i sina arbetsuppgifter och fokusera på att hantera den uppkomna händelsen.

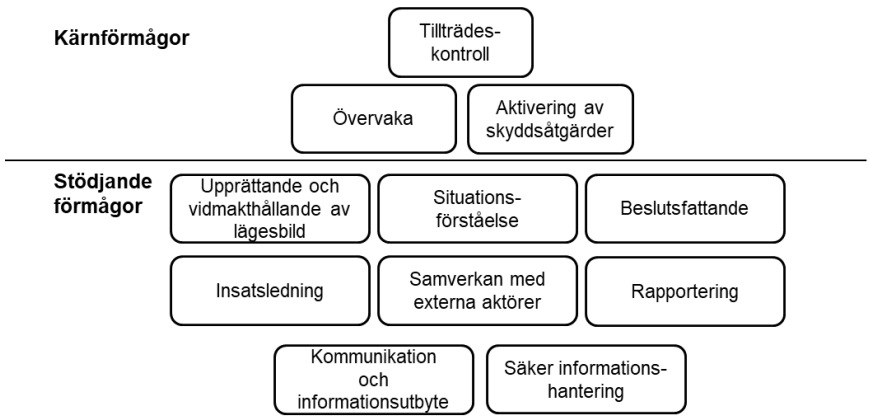
4.3.11 Kontinuerlig utveckling

Principen *Kontinuerlig utveckling* innebär att bevakningssystem utvecklas efterhand som nya förutsättningar ges. Nya tekniska system, algoritmer, hotbibliotek, arbetsformer och kompetenser kan införas efterhand som behov uppstår utan att ge avkall på bevakningsförmåga. Ett kontinuerligt lärande sker av personal och AI-baserade system.

Exempel: En ny dagsljus- och mörkerkamera ska ersätta en äldre dagsljuskamera. Personalen utbildas avseende vad bytet av kamerorna innebär inför förändringen. De nya kamerorna monteras och installeras i bevakningssystem via en ”plugg-and-play” funktion. När personalen har testat och systemet visar att de nya kamerorna fungerar så som de ska, avinstalleras och demonteras de äldre kamerorna.

4.4 Bevakningsförmågor

Detta avsnitt beskriver elva bevakningsförmågor som är relevanta att beakta vid utveckling av Aktiv bevakning. Med begreppet *förmåga* avses att kunna åstadkomma något, exempelvis att upprätta och vidmakthålla en lägesbild. Beskrivningarna av bevakningsförmågorna är generiska vilket innebär att de är oberoende av typ av bevakningssystem och skyddsvärda objekt. De elva förmågorna för Aktiv bevakning som definierats är uppdelade i kärnförmågor och stödjande förmågor (Figur 5).



Figur 5. De elva förmågorna som bidra till Aktiv bevakning, uppdelade i tre kärnförmågor och åtta stödjande förmågor.

4.4.1 Kärnförmågor

Kärnförmågorna utgör grunden i förmågan Aktiv bevakning. De tre kärnförmågorna innefattar: (1) Tillträdeskontroll, (2) Övervaka och (3) Aktivering av skyddsåtgärder.

Tillträdeskontroll avser förmågan att förebygga och hindra obehöriga att få tillträde till områden, byggnader och andra anläggningar eller objekt i vilka de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller vilka säkerhetskänslig verksamhet i övrigt bedrivs (2 kap. 3§ Säkerhetsskyddslagen)

Övervaka avser förmågan att monitorera tillstånd och företeelser, säkerställa behörighet och upptäcka incidenter, händelser och indikatorer samt att hitta mönster av dessa som indikerar negativ påverkan på det skyddsvärda objektet. För Aktiv bevakning kan detta t.ex. innebära att så tidigt som möjligt upptäcka hot mot det skyddsvärda objektet för att minimera skada.

Aktivering av skyddsåtgärder avser förmågan att aktivera åtgärder för att avvärja hot, bryta negativa händelseförlopp samt säkerställa tillträde och tillgång för behöriga. För Aktiv bevakning innebär detta att så tidigt som möjligt bryta händelseförlopp som hotar det skyddsvärda objektet samt att kunna anpassa bevakningssystemet.

4.4.2 Stödjande förmågor

De *stödjande förmågorna* är de förmågor som är nödvändiga för att upprätthålla kärnförmågorna. De åtta stödjande förmågorna innefattar: (1) Upprättande och vidmakthållande av lägesbild, (2) Situationsförståelse, (3) Beslutsfattande, (4) Insatsledning, (5) Samverkan med externa aktörer, (6) Rapportering, (7) Kommunikation och informationsutbyte samt (8) Säker informationshantering.

Upprättande och vidmakthållande lägesbild avser förmågan att samla in information, värdera informationen och skapa, alternativt uppdatera, en lägesbild. Lägesbilden innefattar information om det skyddsvärda objektet, dess omgivning, omvärlden, behörigheter, bevakningssystemets status samt vem som besökt, besöker och planerar att besöka objektet. För Aktiv bevakning skapar detta förutsättningar att tidigt upptäcka händelser och signaler som indikerar hot.

Situationsförståelse avser förmågan att upprätthålla en förståelse för situationen. Detta innefattar att upptäcka händelser och förstå vad de innebär för nuvarande situation samt att förstå vad de innebär för vad som kommer att hända (Endsley & Garland, 2000). Det innebär även en förståelse för hur eget agerade påverkar situationen. God situationsförståelse är avgörande för en välfungerande bevakning. För Aktiv bevakning skapar detta förutsättningar att förstå betydelsen av händelser och signaler för att tidigt upptäcka ett hot samt vilka åtgärder som är bästa lämpade för att avvärja hot.

Beslutsfattande avser förmågan att, utifrån situationen, värdera handlingsalternativ och fatta beslut om åtgärder. För Aktiv bevakning skapar ett effektivt beslutsfattande förutsättningar för att tidigt kunna sätta in motåtgärder för att avvärja hot.

Insatsledning avser förmågan att leda aktörer såsom insatsberedd skyddsstyrka (IBSS) och transportskyddsstyrka (TpSS) vid insatser i syfte att värna det skyddsvärda objektet. För Aktiv bevakning innebär detta att bevakningstjänstens personal ges förutsättningar att proaktivt och med precision avvärja hot och otillbörliga aktiviteter.

Samverkan med externa aktörer avser förmågan att samverka med andra aktörer vid insatser i syfte att värna det skyddsvärda objektet. För Aktiv bevakning innebär detta att kunna bidra vid insatser för att snabbt och med hög precision effektivt avvärja hot och otillbörliga aktiviteter.

Rapportering avser förmågan att dokumentera och förmedla tillstånd och företeelser till berörda med lämpligt format och form. För Aktiv bevakning innebär detta att flera enskilda aktörer, och flera aktörer tillsammans, kan upptäcka händelser och signaler av betydelse för säkerheten.

Kommunikation och informationsutbyte avser förmågan att ta emot, samla in och dela information. En viktig del i detta är att kunna etablera och vidmakthålla sociala och tekniska nätverk. Att samla in och dela information är en nödvändig förmåga för att skapa och vidmakthålla lägesbilden. För Aktiv bevakning skapar väl fungerade kommunikation och informationsutbyte förutsättningar för god lägesbild och situationsförståelse, vilket bidrar till att tidigt kunna upptäcka hot.

Säker informationshantering avser förmågan att säkerställa sekretess, integritet och tillgänglighet vid utbyte, bearbetning, nyttjande och lagring av information som kan vara känslig. Detta innebär hantering av information så att denna inte görs tillgänglig för obehöriga, att säkerställa informationens noggrannhet och fullständighet samt att informationen är tillgänglig för behöriga vid behov. Förmågan säker informationshantering avser hantering av information som förmedlas i fysisk såväl som digital form. För Aktiv bevakning innefattar denna förmåga hantering av information om exempelvis det skyddsvärda objektet, besöksloggar och behörighetsregister.

5 Diskussion och slutsatser

För att skapa en för framtiden anpassad bevakningsförmåga, behövs en vision som ger en inriktning för utvecklingsarbetet. Denna vision bör inte vara slutgiltig utan behöver utvecklas efterhand som nya insikter och kunskap erhålls. Trots denna förändlighet är visionen viktig då den ger något att förhålla sig till och diskutera utifrån. För framtidens bevakningssystem av skyddsvärda objekt har konceptet Aktiv bevakning tagits fram för att skapa en sådan vision. Konceptet Aktiv bevakning som beskrivs i denna rapport är den första versionen och syftar till att bidra till diskussioner om vad som är viktiga aspekter att beakta vid utveckling av framtida bevakningssystem. Konceptet utgör därmed ett steg i en riktning som kan nyttjas för att påbörja en sammanhållen utveckling för att nå en ändamålsenlig bevakningsförmåga.

Den centrala delen i konceptet är de bärande idéer som innebär att tidigt upptäcka hot och ha medel för att kunna avvärja dessa. För att konkretisera hur detta ska gå till utgick arbetet från funktioner och principer som tagits fram och beskrivits inom Försvarsmaktens Huvudstudie Ledning (Granåsen m.fl. 2021; Hallberg m.fl., 2019) samt förmågor som utvecklas inom det MSB[4] finansierade projektet KOMET[5] (Olsén m.fl., 2023). Dessa principer, funktioner och förmågor har under arbetet anpassats till konceptet Aktiv bevakning.

Principer i Aktiv bevakning indikerar hur ett framtida bevakningssystem är tänkta att fungera, men också dess egenskaper och hur det ska realiseras. De fyra första principerna beskriver hur systemet ska fungera, då det utifrån en kvalificerad informationsinhämtning ska skapa innehållsrika lägesbilder som leder till situationsförståelse som i sin tur bidrar till att lämpliga åtgärder kan sätta in. De fyra efterföljande principerna beskriver bevakningssystemets egenskaper, att bevakningsförmågan ska kunna anpassas, att det ska vara motståndskraftigt mot störningar, att bevakningssystemet ska vara transparant samt interoperabelt med omgivande system. De tre sista principerna förklarar hur bevakningssystemet ska realisera och vidmakthållas, som ett harmoniskt sociotekniskt system, med stöd av modern teknik och som kontinuerligt utvecklas.

Hur de principer, funktioner och förmågor som beskrivs i konceptet ska realiseras för att uppnå den bärande idén är en uppgift för framtida studier att beakta. Ett första steg skulle dock kunna vara att genomföra en analys med stöd

[4] MSB är en förkortning för *Myndigheten för samhällsskydd och beredskap*.

[5] KOMET är förkortning för *Koncept och metoder för stärkt erfarenhetshantering via tvärsektoriella övningar*.

av perspektiven DOTMPLFI[6] (Enkvist m.fl., 2016). En sådan analys kan påvisa de krav som behöver ställs på styrande dokument, organisation, träning, materiel, personal, ledarskap, utbildning, faciliteter och interoperabilitet för att erhålla en proaktiv bevakningsförmåga (Eton m.fl., 2016).

Den systemskiss som ingår i koncept ska ses som en modell vilken övergripande beskriver de funktioner som behöver ingå i ett proaktivt bevakningssystem och vad dessa funktioner bidrar med. I utvecklingsverksamheter är systemmodeller viktiga då de avgränsar vad som ska ingå i systemet och vad som inte ska ingå. Systemskissen syftar därmed till att minska risken för att missförstånd ska uppstå kring vad som avses med ”systemet”.

En slutsats från projektet är att det under utveckling av koncept behövs modeller som är enkla att relatera till och som kan användas som diskussionsunderlag i dialogen mellan olika kompetenser. Modellerna utgör en initial vision för alla involverade och skapar en samsyn för vad målet är. Att visionen utgörs av ett koncept medför att denna inte blir alltför rigid, utan att den kan förändras allt eftersom ny kunskap erhållas.

[6] Förkortningen DOTMPLFI ska läsa ut som *Doktrin*, *Organisation*, *Träning*, *Materiel*, *Personal*, *Ledarskap och utbildning*, *Faciliteter* och *Interoperabilitet*.

6 Referenser

Adhanom, I. B., MacNeilage, P., & Folmer, E. (2023). Eye Tracking in Virtual Reality: a Broad Review of Applications and Challenges. *Virtual Reality 27*, 1481–1505. https://doi.org/10.1007/s10055-022-00738-z

Alpman, M. (2019). Med 6G blir världen hyperuppkopplad. *Forskning & Framsteg, 10*. (https://fof.se/tidning/2019/10/artikel/med-6g-blir-varlden-hyperuppkopplad) (2020-03-17).

Antunes, G., & Borbinha, J. (2013). Capabilities in systems engineering: an overview. In *Exploring Services Science: 4th International Conference, IESS 2013*, Porto, Portugal, February 7-8, 2013. Proceedings 4 (pp. 29-42). Springer Berlin Heidelberg.

Bengtsson, K., Oskarsson, P-A., Svensson., J., Wikström, M., & Lif. P. (2020). *GULF - Grafisk Utformning Ledningssystem Fartyg - en förstudie*. FOI-R--5030--SE. Totalförsvarets forskningsinstitut.

Blasch, E., Nagy, J., Aved, A., Jones, E. K., Pottenger, W. M., Basharat, A., ... & Ling, H. (2014). Context aided video-to-text information fusion. In *17th International Conference on Information Fusion (FUSION)* (pp. 1-8). IEEE.

Castiglione, A., Choo, K. K. R., Nappi, M., & Ricciardi, S. (2017). Context aware ubiquitous biometrics in edge of military things. *IEEE Cloud Computing*, *4*(6), 16-20.

Chen, P. Y., & Das, P. (2023). AI Maintenance: A Robustness Perspective. *Computer*, 56(2), 48-56.

Davis, M. C., Challenger, R., Jayewardene, D. N., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied ergonomics*, *45*(2), 171-180.

Dove, R., Lunney, K., Orosz, M., & Yokell, M. (2023). Agile Systems Engineering–Eight Core Aspects. In *INCOSE International Symposium* (Vol. 33, No. 1, pp. 823-837).

Endsley, M. R., & Garland, D. J. (2000). Theoretical underpinnings of situation awareness: A critical review. *Situation awareness analysis and measurement*, 1(1), 3-21

Enkvist, T., Hansson, L-Å., & Ekenstierna, C. (2016). *Att utveckla och skriva militära koncept*, FOI Memo 5744. Totalförsvarets forskningsinstitut.

Eton, J., Redmayne, J., & Thordsen, M. (2016). *Joint Analysis Handbook (4 ed.)*. Joint Analysis and Lessons Learned Centre.

Fast-Berglund, Å., Gong, L., & Li, D. (2018). Testing and validating Extended Reality (xR) technologies in manufacturing. *Procedia Manufacturing, 25*, 31-38.

Fitts, P. M., Jones, R.E., & Milton, J.L. (1950). Eye movements of aircraft pilots during instrument-landing approaches. *Aeronautical Engineering Review, 9*(2), 24-29.

Freedberg S. J. JR. (2019) *The Art of Command, The Science of AI. Breaking Defense*. https://breakingdefense.com/2019/11/the-art-of-command-the-science-of-ai/ (2023-06-27).

Försvarsberedningen. (2019). *Värnkraft–Inriktningen av säkerhetspolitiken och utformningen av det militära försvaret 2021–2025*. Försvarsdepartementet.

Försvarsmakten (2021). *Huvudstudie Ledning – Delrapport 2021* (FM2021-24915:1). Försvarsmakten.

Försvarsmakten (2015). *Handbok Säkerhetstjänst Fysisk säkerhet* (FM2015-15165.1). Försvarsmakten.

Granåsen, M., Hallberg, N., Josefsson, A., & Ivari, J. (2021). *Ledningskoncept 2045: Resultat av 2020 års konceptutveckling*, FOI-R--5128--SE. Totalförsvarets forskningsinstitut.

Hallberg, N., Granåsen, M., Josefsson, A., & Barius, P. (2019). *Förslag till ledningskoncept för 2045 - Första versionen*. FOI Memo 6980. Totalförsvarets forskningsinstitut.

Haridas, A. (2018). *KOLAM: human computer interfaces for visual analytics in big data imagery* (Doctoral dissertation, University of Missouri--Columbia).

Hasan, H., & Kazlauskas, A. (2009). *Making sense of IS with the Cynefin framework*. https://ro.uow.edu.au/commpapers/959. (2023-09-13).

Huang. J., Jaiswal, P., & Rai, R. (2018). Gesture-based system for next generation natural and intuitive interfaces. *Artificial Intelligence for Engineering Design, Analysis and Manufacturing* 1–15.

Jacob, R. J., & Karn, K. S. (2003). Eye tracking in human-computer interaction and usability research: Ready to deliver the promises. *Mind, 2*(3), 573-605.

Jändel, M., Bivall, P., Hammar, P., Kamrani, F., Johansson, R., & John Quas, M. (2016). *Visual analytics*. FOI-R--4200--SE. Totalförsvarets forskningsinstitut.

Kamrani, F., Kanestad, L., Luotsinen, L., Pelzer, B., Sabel, J., Sandström, V., & Tegen, A. (2023) *Attacking and Deceiving Military AI Systems*. FOI-R--5396--SE. Totalförsvarets forskningsinstitut.

Kaushal, H., & Kaddoum, G. (2017). Applications of lasers for tactical military operations. *IEEE Access, 5*, 20736-20753.

Korpela, C., & Walker, A. (2018). Wearable Technologies for Enhanced Soldier Situational Awareness. In *Proceedings of the 2nd International Conference on Vision, Image and Signal Processing* (pp. 1-6).

Kott, A. (2018). Challenges and characteristics of intelligent autonomy for internet of battle things in highly adversarial environments. In *2018 AAAI Spring Symposium Series*.

Kott, A., Swami, A., & West, B. J. (2016). The internet of battle things. *Computer*, *49*(12), 70-75.

Ladetto, Q. (2016). *Defence Future Technologies: Emerging Technology Trends 2015*. Federal Department of Defence, Civil Protection and Sport DDPS armasuisse Science and Technology Research Management and Operations Research. (https://deftech.ch/wp-content/uploads/2018/07/DefenceFutureTechnologies_EmergingTechnologyTrends2015.compressed.pdf).

Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. *Journal of Industrial Information Integration*, *10*, 1-9.

Lindbom, H., & Tehler, H. (2020). Enhetlig terminologi kring begreppet förmåga i det förebyggande och förberedande arbetet över hela hotskalan. Lunds universitet.

Lindquist, S., Nilsson, P., & Nilsson, S. (2022). *Koncept för framtida bevakningscentraler*. FOI Memo 8006, Totalförsvarets forskningsinstitut.

Livermore, D. (2019). *Military trends in the near future. Global Defence Industry Intelligence*. https://www.defenceiq.com/defence-technology/articles/5-military-trends-and-predictions-2020 (2023-06-27).

Luotsinen, L. (2018). *Maskininlärning med små datamängder*. FOI Memo 6521. Totalförsvarets forskningsinstitut.

Mittal, P., & Singh, N. (2016). Speech based command and control system for mobile phones: issues and challenges. In *2016 Second International Conference on Computational Intelligence & Communication Technology (CICT)* (pp. 729-732). IEEE.

Nilsson, M. (2017). *Djupa neuronnät: sårbarheter och vilseledning*. FOI Memo 6252. Totalförsvarets forskningsinstitut.

Nilsson, S., Andersson, M., Andersson, T., Bilock, E., Deleskog, V., Hemström, F., Lindgren, D., Molin, S., Nygårds, J., Relfsson, E., & Rydell, J. (2020). *Autonom övervakning med samverkande sensorer: Slutrapport 2020* (FOI-R--5065--SE). Totalförsvarets forskningsinstitut.

Näsström, F., Allvar, J., Bissmarck, F., Deleskog, V., Hamrell, H., Hemström, F., Karlholm, J., Nordlöf, J., & Nygårds, J. (2022). *AI för spaningssensorer – Slutrapport*. FOI-R--5232--SE. Totalförsvarets forskningsinstitut.

Näsström, F., Bissmarck, F., Deleskog, V., Hemström, F., Holmberg, M., Karlholm, J., Nordlöf, J. Nygårds, J. Stenborg, K-G., & Wadströmer, N. (2018). *Intelligenta spaningsfunktioner 2016-2018, slutrapport*. FOI-R--4648--SE. Totalförsvarets forskningsinstitut.

Olsén, M., Oskarsson, P. A., Hallberg, N., Granåsen, M., & Nordström, J. (2023). Exploring collaborative crisis management: a model of essential capabilities. *Safety science*, *162*, 106092.

Paing, M. P., Juhong, A., & Pintavirooj, C. (2022). Design and development of an assistive system based on eye tracking. *Electronics*, *11*(4), 535.

Pettitt, R., Elliott, L. R., & Taylor, G. (2018). *Wearable Smart Interaction Device (SID) for Advanced Human-Robot Interaction Using Gestures and/or Speech* (No. ARL-TR-8411). US Army Research Laboratory Aberdeen Proving Ground United States.

Rantakokko, J. (2019). *Tekniköversikt autonoma och obemannade system - Del 1: Historik*. FOI-R--4680--SE. Totalförsvarets forskningsinstitut.

Rogers, Y., Sharp, H., & Preece, J. (2023). *Interaction Design: Beyond Human-Computer Interaction*, 6th Edition. Wiley.

Rosell, M., Bay, S., Bolin, U., García Lozano, M., Gustafsson, D., Johansson, F., Horndal, A., Karasalo, M., Lilja, H., Lundmark, L., Sabel, J., Stiff, H., & Valldor, E. (2022). *Semi-automatisk datadriven webbanalys: detektion av fabricerad media, trovärdighetsbedömning och cyberhotsbevakning*. FOI-R--5262--SE. Totalförsvarets forskningsinstitut.

Scheplitz, T. (2022). Ensuring Socio-technical Interoperability in Digital Health Innovation Processes: An Evaluation Approach. In *HEALTHINF* (pp. 264-275).

Snowden, D. (2002). Complex acts of knowing: paradox and descriptive self-awareness. *Journal of knowledge management*, *6*(2), 100-111.

Suri, N., Tortonesi, M., Michaelis, J., Budulas, P., Benincasa, G., Russell, S., Stefanelli, C., & Winkler, R. (2016). Analyzing the applicability of internet of things to the battlefield environment. In *2016 international conference on military communications and information systems (ICMCIS)* (pp. 1-8). IEEE.

Svenmarck, P. (2018). *Arbetslägesrapport inom transparens för AI-system*. FOI Memo 6360. Totalförsvarets forskningsinstitut.

Tortonesi, M., Morelli, A., Govoni, M., Michaelis, J., Suri, N., Stefanelli, C., & Russell, S. (2016). Leveraging Internet of Things within the military network

environment—Challenges and solutions. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)* (pp. 111-116). IEEE.

Trist, E. L. (1981). *The evolution of socio-technical systems* (Vol. 2). Toronto: Ontario Quality of Working Life Centre.

Van Horne, P., & Riley, J. A. (2021). *Left of Bang: How the Marine Corps Combat Hunter Program Can Save Your Life*. Black Irish Entertainment LCC.

Yushi, L., Fei, J., & Hui, Y. (2012). Study on application modes of military Internet of Things (MIOT). In *2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE)* (Vol. 3, pp. 630-634). IEEE.

Zhang, Z., Wen, F., Sun, Z., Guo, X., He, T., & Lee, C. (2022). Artificial intelligence‐enabled sensing technologies in the 5G/internet of things era: from virtual reality/augmented reality to the digital twin. *Advanced Intelligent Systems*, *4*(7), 2100228.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

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

www.foi.se