



Självständigt arbete (30 hp)

Författare	Program/Kurs
Christian Lagerstedt	HOP2
Handledare	Antal ord: 9969 (+bilagor 2002)
Annick Wibben	Kurskod
	2UK045
MIND THE GAP – KOMPATIBEL LÄGESBILD I GRÅZONEN	
Abstract: <p>This study examines how grey-zone ambiguity is understood and handled in the process of establishing compatible situational awareness within Sweden's decentralized total defence system, focusing on the energy supply sector. Using an abductive content analysis with an interpretive approach, it adopts an exploratory case study design based on scenario-driven focus group discussions, applying Distributed Situation Awareness, Hybridity Blizzard Model and Fort logic.</p> <p>The findings illustrate a paradox: while the sector gives expression to strong operational robustness, it is perceived as strategically vulnerable due to vertical information gaps. Local actors prioritize restoration over attribution, which is interpreted as a risk where coordinated hybrid actions are absorbed into routine disturbances. The absence of proactive top-down intelligence sharing is understood as a factor that constrains the development of compatible situational awareness across levels.</p> <p>The study indicates that resilience in the grey zone depends on the quality of vertical information links enabling strategic interpretation of ambiguous events.</p>	
Keywords: Grey-zone, Hybrid threats, Total defence, Situational awareness, Energy supply sector, Resilience.	

Innehållsförteckning

1. INLEDNING.....	3
1.1 DEN NYA STRATEGISKA ICKE-FREDEN.....	3
1.2 ATT DEFINIERA DET OTYDLIGA	4
1.3 PROBLEMSTÄLLNING OCH FORSKNINGSFRÅGA	5
1.4 SYFTE OCH FORSKNINGSFRÅGA	6
2. TIDIGARE FORSKNING	7
2.1 HOTBILDEN I GRÅZON	7
2.2 FÖRSVAR I GRÅZON.....	7
3. TEORI.....	9
3.1 HYBRIDITY BLIZZARD MODEL	9
3.2 TYPOLOGY OF TOTAL DEFENCE STRATEGIES	11
3.3 DISTRIBUTED SITUATION AWARENESS	12
4. METOD.....	13
4.1 FORSKNINGSANSATS OCH DESIGN.....	13
4.2 DE KONTEXTUELLA RAMVERKEN: HOTBILD OCH FÖRSVARSTRATEGI	14
4.3 DEN ANALYTISKA LINSEN: DISTRIBUTED SITUATION AWARENESS.....	14
4.4 DATAINSAMLING: SCENARIOSAMTAL MED FOKUSGRUPPER	15
4.5 ANALYSMETOD: EN PROCESS I TVÅ STEG.....	16
4.6 ETISKA ASPEKTER.....	17
4.7 AVGRÄNSNINGAR	17
5. EMPIRI OCH ANALYS.....	18
5.1 ANALYS MOT DISTRIBUTED SITUATION AWARENESS (DSA)	18
5.1.1 <i>Observera-fasen</i>	18
5.1.2 <i>Orientera-fasen</i>	21
5.1.3 <i>Besluta-fasen</i>	23
5.1.4 <i>Agera-fasen</i>	24
5.1.5 <i>Sammanfattande analys mot DSA</i>	25
5.2 ANALYS MOT HOTBILD OCH FÖRSVARSTRATEGI	26
6. SLUTSATS, DISKUSSION OCH FORTSATT FORSKNING	28
7. REFERENSER.....	34
BILAGA 1 HYPOTETISKT SCENARIO	38
BILAGA 2 INTERVJUGUIDE.....	40

1. Inledning

Den säkerhetspolitiska situationen i Sveriges närområde har under de senaste åren försämrats avsevärt, drivet av strategiska händelser som Rysslands annektering av Krim 2014 och den fullskaliga invasionen av Ukraina 2022. Denna utveckling har på nytt placerat nationell säkerhet och försvar högst upp på den politiska agendan. Den moderna hotbilden mot Sverige är bred, komplex och allvarlig, och karaktäriseras av en allt otydligare gränsdragning mellan fred och krig. Denna osäkerhet har lett till ett ökat fokus på fenomen som hybridhot, hybridkrigföring och gråzonsproblematik.

Dessa hot är samordnade och synkroniserade, riktade mot staters sårbarheter, och syftar till att skapa oro, splittring och polarisering. Denna kontext involverar hela samhället, militärt som civilt och kräver en helhetsstrategi, ”whole-of-society approach” (Wrange m.fl. 2024, s. 513). Det som i Sverige benämns Totalförsvaret.

1.1 Den nya strategiska icke-freden

Det svenska totalförsvaret har genomgått betydande förändringar till följd av en utvecklad hotbild, fokus har skiftat från storskaliga konventionella angrepp till dagens komplexa hybridhot. Systemet skapades på 1940-talet som ett svar på det totala krigets krav på hela samhällets engagemang (Asp 2023, s. 7). Under kalla kriget vilade strategin på väpnad neutralitet och en helhetssyn, *whole-of-society* (Alvinus & Hedlund 2024, s. 603), fördelat på fyra huvudpelare: militärt, civilt, ekonomiskt och psykologiskt försvar (Jonsson m.fl. 2019, s. 13). Strukturen var dimensionerad för storskaliga angrepp genom en decentraliserad mobiliseringsorganisation med regional samordning (Asp 2023, s. 32).

Efter kalla kriget följde en omfattande nedmontering och en strategisk time-out fram till 2014, då existentiella hot betraktades som osannolika. Under denna period omorienterades det militära försvaret mot internationella insatser, medan den civila sidan inriktades på fredstida krisberedskap.

Rysslands aggression 2014 markerade en vändpunkt där väpnat angrepp åter blev den dimensionerande hotbilden (Försvarsdepartementet 2015, s. 60). Kriget i Ukraina visar att konflikter om territorium med militära medel återigen är en realitet i Europa och där Ryssland inte följer den regelbaserade världsordningen enligt FN-stadgan. Totalförsvarsplaneringen återupptogs därefter utifrån Försvarsmaktens operativa planläggning (Försvarsdepartementet

2017, s. 16). Hotbilden efter 2014 utmärks av en dubbel komplexitet av konventionella och hybrida hot. De senare syftar till att destabilisera samhället genom att sudda ut gränsen mellan krig och fred i gråzonen (Asp 2023, s. 193).

1.2 Att definiera det otydliga

Den säkerhetspolitiska omvärlden präglas därmed av en ökad begreppslig osäkerhet. Flera överlappande termer används för att beskriva liknande fenomen, ofta utan en enhetlig internationell definition (Olsén m.fl. 2020, s. 11-12).

Gråzon definieras i grunden som ett tillstånd eller en arena mellan krig och fred kännetecknad av stor osäkerhet (Jonsson m.fl. 2019, s. 41). Syftet med agerandet i gråzonen är att vinna strategiska fördelar utan att situationen eskalerar till öppet krig (Jonsson 2018, s. 15). Gråzonsproblematik fokuserar istället på de strategiska otydligheter som uppstår för försvararen. Genom att angriparen agerar dolt nära gränsen för upptäckt, försvaras beslutsfattande och möjligheten att attribuera (vem som utfört handlingen) händelserna till en antagonist (Försvarsberedningen 2017, s. 66).

Hybridhot beskriver de specifika metoderna och aktiviteterna. Det avser koordinerade och synkroniserade icke-militära medel, såsom cyberattacker, ekonomisk press och desinformation, riktade mot systemviktiga sårbarheter (Asp 2023, s. 192-193; Borch & Heier 2025, s. 39). Hybridkrigföring betecknar den integrerade strategin eller kampanjen där dessa medel kombineras (Borch & Heier 2025, s. 14). Medan hybridhot ofta nyttjas under tröskeln för krig, är hybridkrigföring även ett påtagligt inslag i en eskalerad krigssituation (Jonsson m.fl. 2019, s. 40).

Användningen av begreppen skiljer sig åt: internationella aktörer som NATO och EU betonar hybrida termer, medan svenska organ som Försvarsberedningen och MSB främst använder gråzonsproblematik (Olsén m.fl. 2020, s. 11-13). Ryssland nyttjar istället begrepp som asymmetrisk eller icke-linjär krigföring (Olsén m.fl. 2020, s. 12).

Denna uppsats fokuserar främst på gråzonsproblematiken då den bäst fångar utmaningen i att identifiera handlingar i gränslandet mellan fredstida krishantering och höjd beredskap. Antagonister utnyttjar medvetet systemets skarvar, de administrativa och juridiska mellanrummen mellan sektorer där ansvaret riskerar att falla mellan stolarna (Borch & Heier

2025, s. 165). Denna inneboende tvetydighet skapar ett stort tolkningsutrymme som försvårar förmågan att snabbt etablera en gemensam lägesbild och vidta motåtgärder (Jonsson m.fl. 2019, s. 38).

1.3 Problemställning och forskningsfråga

Inom ramen för totalförsvaret utgör säker elförsörjning en grundläggande och existentiell funktion för samhällets överlevnad (Jonsson 2020, s. 1). Eftersom nästan all samhällsviktig verksamhet, inklusive transporter, finansiella tjänster, hälso- och sjukvård samt Försvarsmaktens operativa förmåga, är kritiskt beroende av fungerande el och elektronisk kommunikation. Därför blir energiförsörjningssektorn ett prioriterat och attraktivt mål ur ett antagonistiskt perspektiv (Försvarsdepartementet 2017, s. 165). Svenska kraftnät (2024, s. 3, 29), som är systemansvarig myndighet, framhåller att de största antagonistiska hoten mot svensk elförsörjning kommer från kvalificerade statsaktörer som Ryssland, Kina och Iran. Angripare kan dessutom utnyttja sårbarheter som utkontraktering, osäkra leverantörskedjor och utländskt ägande av kritisk infrastruktur för att få inflytande över produktions- och distributionsresurser.

Den svenska totalförsvarsstrategin bygger på en decentraliserad ledningsstruktur och ansvarsprincipen, vilket innebär att ansvaret för att upprätthålla samhällsviktig verksamhet i krig i stor utsträckning ligger hos enskilda aktörer, inklusive privata energibolag (Jonsson m.fl. 2023, s. 44-45). Framgången för totalförsvaret kräver därmed att dessa aktörer, särskilt på regional nivå där samverkan mellan det civila och militära försvaret ska ske, förmår att samordna sig effektivt (Försvarsdepartementet 2017, s. 87). Den största utmaningen i gråzonen ligger dock i svårigheten att attribuera händelserna till en antagonist. Eftersom otydligheten skapar ett stort tolkningsutrymme, försvåras förmågan att snabbt skapa en gemensam lägesbild och vidta kraftfulla motåtgärder (Jonsson m.fl. 2019, s. 38).

Även om den operativa målsättningen är en gemensam lägesbild, utgår analysen från Stanton m.fl. (2006), Distributed Situation Awareness (DSA), en teori lämpad för komplexa, decentraliserade strukturer. DSA betonar kompatibel situationsmedvetenhet (kompatibel-SA) framför delad SA. Försök att uppnå fullständig delad SA kan leda till en betydande börda av onödig kommunikation, vilket försämrar snabb respons. Kompatibel-SA innebär att aktörer har olika mål och därmed olika, men kompatibla, SA-krav anpassade efter sin specifika roll (Stanton m.fl. 2006, s. 1290).

1.4 Syfte och forskningsfråga

Syftet med uppsatsen är att analysera hur aktörer inom totalförsvarets nuvarande decentraliserade ledningsstruktur skapar förståelse för att hantera den tolkningsutmaning som gråzonsproblematiken innebär. Fokus ligger därmed på hur aktörer skapar förståelse kring situationer i gråzonen. Studien undersöker empiriskt samspelet mellan de strategiska kraven på motståndskraft och de praktiska förutsättningarna hos aktörer inom energiförsörjningssektorn att identifiera, tolka och samordna händelser i gränslandet mellan fred och krig. Genom denna analys avser uppsatsen att bidra till en fördjupad förståelse för hur informationsdelning och samverkan kan påverka möjligheten att etablera en synkroniserad och strategiskt sammanhållen respons mot hot i gråzonen. Studien syftar inte till att förklara kausala samband eller generalisera till totalförsvaret som helhet, utan till att tolka hur aktörer skapar mening i en specifik kontext.

För att uppnå detta syfte besvarar studien följande forskningsfråga:

Hur förstås och hanteras gråzonsproblematikens tvetydighet i processen att etablera en kompatibel lägesbild inom totalförsvarets decentraliserade ledning av energiförsörjningen?

2. Tidigare forskning

2.1 Hotbilden i gråzon

Som beskrivet saknas en enhetlig definition av den hybrida hotbilden, vilket skapat en omfattande akademisk debatt. Fridman (2017, s. 42-44) tydliggör att begreppet hybridkrigföring definieras olika i väst och Ryssland. Ursprungsidén i väst baseras på Hoffmans (2007, s. 8) definition där konventionella och icke-konventionella styrkor nyttjas genom oregelbunden taktik, såsom terrorism och kriminell oordning, koordinerat för att uppnå synergieffekter.

Rysslands definition, *gibridnaya voyna*, är nästan den omvända och fokuserar på icke-militära metoder för att splittra länder inifrån. Det ska förtydligas att detta är den ryska synen på den upplevda hybridkrigföringen som väst utövar mot Ryssland (Fridman 2017, s. 48-49). Enligt Oscar Jonsson (2019, s. 5) skiftade den ryska synen 2012–2014, då icke-militära medel började betraktas som våldsamma och gränsen mellan krig och fred suddades ut och informations- och kommunikationsteknologi samt färgrevolutionerna bidrog till att icke-militära medel fick större betydelse än militära.

Inom Nato och EU tolkas rysk hybridkrigföring betydligt bredare. Weissmann (2021, s. 3, 61, 271) och Elonheimo (2021, s. 121) ser det som samordnade aktiviteter med både militära och icke-militära maktmedel under nivån för väpnad eskalation. Man siktar medvetet på systemets ”skarvar” och glappet mellan myndigheters ansvarsområden. Detta inkluderar politiska, diplomatiska och ekonomiska maktmedel, men även psykologiska verktyg som desinformation för att undergräva förtroendet för myndigheter. De militära maktmedlen omfattar illegal underrättelseinhämtning, sabotage, subversion och krigsförberedelser. Galeotti beskriver detta som en ”weaponisation of everything” (2022, s. 10). Dessa metoder syftar till att utmana sammanhållning och beslutsfattande i öppna, digitaliserade västerländska demokratier.

2.2 Försvar i gråzon

Forskningen visar en stor samstämmighet kring att gråzonsproblematik bäst bemöts genom en samhällsomfattande, adaptiv strategi fokuserad på resiliens. Tillberg, Berndtsson, & Tillberg (2025, s. 41) påtalar att idén med totalförsvaret är att kombinationen av civil och militär förmåga skapar resiliens och förmågan att avskräcka en potentiell angripare genom att höja

kostnaden för aggression. Elonheimo (2021, s. 124) argumenterar för att omfattande säkerhet kräver samarbete och situationsmedvetenhet, där förbättrad informationsdelning bland nyckelmyndigheter är fundamentalt för att upprätthålla en delad lägesbild.

Enligt den strategiska "Fort-logiken" (Ångström & Ljungkvist 2024, s. 508-509) kräver de ständigt närvarande hybridhoten en radikal decentralisering av totalförsvaret. Strategin innebär att alla samhällsaktörer och medborgare måste vara vaksamma eftersom hybridkrigföring betyder att "allt är beväpnat", vilket kräver en upplösning av gränsen mellan civila och militära roller. Samtidigt varnar Alvinus & Hedlund (2024, s. 609) för att totalförsvaret riskerar att bli en "koloss på lerfötter" på grund av tre övergripande svagheter: oförmåga (resursbrist och oklara mandat), ovilja (misstro och tidsbrist) och bristande synkronisering. Denna brist på synkronisering leder till en brist på helhetssyn, där aktörer fokuserar enbart på det egna ansvarsområdet.

Svensk krisberedskap vilar på principerna om ansvar, likhet och närhet. Trots att dessa ska utgöra grunden skapar det decentraliserade sektorsansvaret ofta organisatoriska stuprör som försvårar nödvändig samverkan (Alvinus & Hedlund 2024, s. 613-614). Borch & Heier (2025, s. 166-167) betonar att skapandet av en gemensam lägesbild genom ett nätverksbaserat tillvägagångssätt är avgörande för att anpassa responsen mot hybrida hot. Problemet är att administrativa gränser och oskrivna regler mot att korsa sektorsgränser skapar gråzoner där hybridhoten kan verka. Antagonister riktar sig medvetet mot dessa skarvar och luckor i ansvaret (Weissmann, Nilsson & Palmertz 2021, s. 185).

Den svenska totalförsvarsstrategin står inför en stor utmaning då kravet på snabb och samordnad respons kolliderar med systemets decentraliserade struktur. Gråzonsproblematiken kännetecknas av tvetydighet och svårighet i attribuering (Elonheimo 2021, s. 115), vilket tvingar den angripna staten att agera reaktivt i en belastad informationsmiljö. För att möta detta krävs en snabbare beslutscykel samt förmåga att upprätthålla situationsmedvetenhet och tempo, vilket är avgörande för att navigera i den snöstorm av hot som hybridkrigföring innebär.

Sammanfattningsvis behandlar tidigare forskning främst gråzonsproblematik på en övergripande strategisk nivå. Det finns dock begränsad empirisk kunskap om hur aktörer inom specifika samhällssektorer tolkar och hanterar denna tvetydighet i praktiken. Denna studie bidrar genom att undersöka hur förståelse skapas i gråzonen inom energiförsörjningssektorn, med särskilt fokus på etableringen av kompatibel lägesbild.

3. Teori

Syftet är att förstå det komplexa sambandet mellan hotbild, försvarsstrategi och operativ lägesbild för beslutsfattande. Därför länkas tre ramverk samman, medan *Typology of total defence Strategies* belyser den decentraliserade ledningens utmaningar i Fort-logiken, förklarar *Hybridty Blizzard Model* (HBM) hybridhotens svårtolkade natur. Tillsammans med *Distributed Situation Awareness* (DSA) möjliggör teorierna en analys av hur samordnad situationsmedvetenhet formas i spänningen mellan decentraliserad strategi och operativ praktik. I denna studie används de teoretiska begreppen som analytiska verktyg för att tolka empirin. De utgör således inte empiriska kategorier i materialet, utan fungerar som analytiska linser som ger en bild av hur aktörerna skapar förståelse. Detta innebär att studien inte syftar till att pröva teorierna, utan att använda dem för att skapa en fördjupad förståelse av hur aktörer tolkar och hanterar gråzonsproblematik.

3.1 Hybridty Blizzard Model

HBM presenteras av Weissmann (2021. s. 266-271) som ett dynamiskt ramverk för att öka förståelsen för hybridhot och hybridkrigföring. Genom metaforen snöstorm (Blizzard) visualiseras ett komplext säkerhetslandskap där försvararen angrips från alla vinklar av otaliga små attacker som är svåra att lokalisera eller separera. Modellen (se fig. 1) analyserar förhållandet mellan angripare och försvarare ur både ett kort- och ett långsiktigt perspektiv.

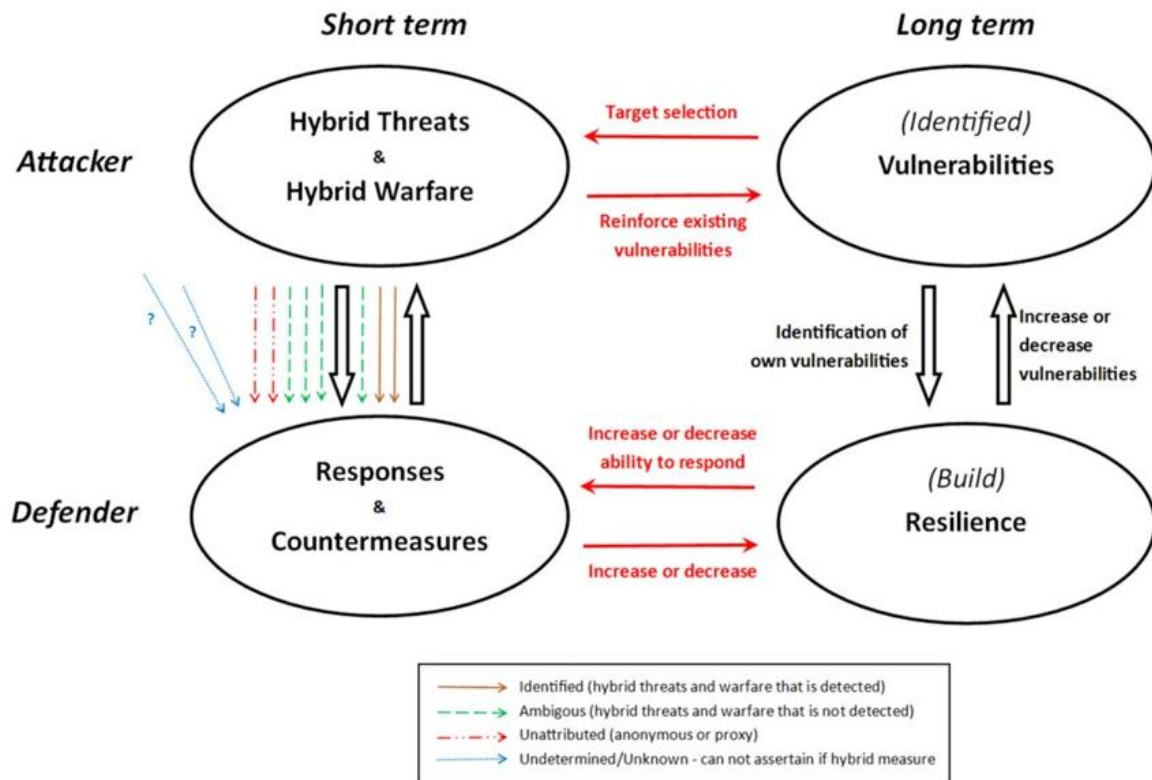


Fig. 1 Hybridity Blizzard Model. (Weissmann 2021, s. 268)

Det kortsiktiga perspektivet utgörs av en pågående duell mellan angriparens operativa åtgärder och försvararens omedelbara motåtgärder. Angriparen agerar här i gråzonen för att vinna fördelar genom att utnyttja svagheter och skarvar mellan aktörer, med målet att hålla sig under tröskeln för upptäckt och attribuering. Parallellt fokuserar det långsiktiga perspektivet på kampen mellan försvararens sårbarheter och dennas uppbyggda motståndskraft (resilience). Angriparen identifierar aktivt sårbarheter för målval, medan försvararens resiliens avgör förmågan att agera i det kortsiktiga skedet.

Kärnan i hybridproblematiken är situationens inneboende kaos och tvetydighet. En stor utmaning är att avgöra om en händelse är en antagonistisk attack eller ett naturligt fel, så kallade *false-positives*. För att möta detta krävs ett detektionssystem som möjliggör tidig upptäckt och identifiering av dolda aktiviteter eller oattribuerade hot. Eftersom hybridhot riktar sig mot långsiktiga sårbarheter i gränsområden mellan sektorer, krävs ett motståndskraftigt samhälle där samarbete sker över traditionella gränser. Effektivitet i både respons och motåtgärder

förutsätter pragmatism, flexibilitet och inkludering av militära, politiska, ekonomiska, civila och informationsmässiga sfärer.

Försvarens förmåga att agera kortsiktigt är helt beroende av en operativ lägesbild. I den osäkra gråzonen måste den strategiska hotbilden kombineras med den operativa lägesbilden för att möjliggöra en synkroniserad tolkning. Detta förutsätter att spridda indikationer kopplas samman, ofta från sensorer och system som tidigare inte varit integrerade, och tillämpa ett helhetsperspektiv. Centralt för bedömningen är att värdera antagonists identitet, avsikt och maktmedel kontra de egna känsliga sårbarheterna. Sammanfattningsvis syftar HBM till att hjälpa aktörer att navigera i snöstormen genom att bygga resiliens via totalförsvarets principer och främja ett inkluderande samarbete mellan offentliga och privata aktörer på alla nivåer.

3.2 Typology of total defence Strategies

Ångström och Ljungkvist (2024, s. 505-509) presenterar en typologi (se fig. 2) som visar att totalförsvaret inte är en homogen strategi, utan att dess logik varierar utifrån hur hotet om totalt krig uppfattas. Typologin vilar på två dimensioner: graden av civil-militär uppdelning, separata kontra suddiga roller, samt graden av ledning och kontroll, centraliserad kontra decentraliserad. Strategin har utvecklats från kalla krigets decentraliserade celler (1948–1972), via invasionstidens centraliserade stuprör (1972–1993) och terrorhotets kluster (1994–2014), till dagens Fort-logik.

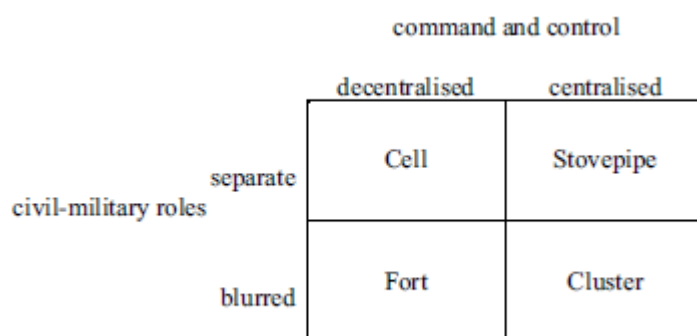


Fig. 2 Typology of total defence Strategies. (Ångström & Ljungkvist 2024, s. 506)

Den nuvarande Fort-logiken (2014–2022) är utformad för att möta hybridkrigföring och gråzonsproblematik (Ångström och Ljungkvist 2024, s. 515-517). Logiken vilar på antagandet att hotet är omnipresent och att totalförsvaret ständigt måste vara påslaget. Strategin kräver en

radikal decentralisering där civil-militära roller flätas samman eftersom allt är beväpnat (*weaponisation of everything*). Varje offentlig myndighet, privat företag och enskild medborgare förväntas agera som ett självförsörjande fort. Genom att sprida ansvaret för vaksamhet och motståndskraft till alla samhällsnivåer skapas en genomgående resiliens som kan hantera samtidiga och tvetydiga hot. Detta system syftar till att avskräcka angripare genom att höja kostnaderna för aggression, men det förutsätter i slutändan att den enskilde individen är beredd att identifiera och möta antagonistiska metoder i gränslandet mellan fred och krig.

3.3 Distributed Situation Awareness

Stanton m.fl. (2006, s. 1288-1289) utvecklade Distributed Situation Awareness (DSA) som en systemorienterad teori för att analysera lägesbilden (SA) i komplexa och dynamiska miljöer. DSA ser kognition som ett systemfenomen där kunskap är distribuerad bland systemets aktörer, vilka inkluderar både mänskliga operatörer och tekniska system (Stanton m.fl. 2006, s. 1290). Denna kunskap organiseras i ett nätverk av kunskapsobjekt som aktiveras i takt med att uppgifter och situationen utvecklas (Stanton m.fl. 2006, s. 1291).

För systemets effektivitet är nätverkslänkar, kommunikationen och informationsöverföringen mellan aktörerna, mer avgörande än själva noderna (Stanton m.fl. 2006, s. 1308). Istället för att eftersträva en fullständigt delad lägesbild betonar DSA kompatibel-SA, vilket innebär att aktörer har olika men samstämmiga SA-krav baserat på sina unika mål och roller (Stanton m.fl. 2006, s. 1291). En välfungerande DSA vilar på meta-SA, vilket innebär att aktörerna har kännedom om hos vem den specifika kunskapen finns (Stanton m.fl. 2006, s. 1291). Genom meta-SA kan aktörer kompensera för brister hos varandra, vilket gör SA till den faktor som binder samman löst kopplade system till en fungerande helhet (Stanton m.fl. 2006, s. 1308).

DSA-teorin vilar på sex grundläggande teser (Stanton 2016, s. 2-3):

1. Lägesbilden innehas av mänskliga och icke-mänskliga aktörer.
2. Olika aktörer har olika uppfattningar av samma scenario.
3. Överlappningen av lägesbilden mellan aktörer beror på deras respektive mål.
4. Kommunikation mellan aktörer kan vara implicit (underförstådd, ej uttalad).
5. SA är den faktor som binder samman löst kopplade system.
6. En agent kan kompensera för försämrade SA hos en annan agent.

4. Metod

4.1 Forskningsansats och design

Studien tillämpar en abduktiv innehållsanalys med en tolkande ansats, vilket syftar till att förstå aktörers subjektiva meningsskapande snarare än att förklara fenomenet genom kausala samband (Esaiasson 2017, s. 213; Schwartz-Shea & Yanow 2012, s. 27). Denna ansats är nödvändig då hybridhotens natur i gråzonen skapar en miljö av tvetydighet, vilket kräver en djupgående tolkning av hur aktörer i elförsörjningssektorn konstruerar mening för att kunna identifiera och agera mot oklara hot (Schwartz-Shea & Yanow 2012, s. 32-33). Genom ett abduktivt tillvägagångssätt tillåts en iterativ växelverkan där analysen pendlar mellan empiri och teori (Schwartz-Shea & Yanow 2012, s. 27). DSA, HBM och Fort-logiken används här som teoretiska linser för att tolka den insamlade empirin, i syfte att identifiera förklaringar som gör de observerade mönstren begripliga (Schwartz-Shea & Yanow 2012, s. 27).

Designen (se fig. 3) är utformad som en explorativ fallstudie med fokus på energiförsörjningssektorn. Studien ska förstås som en mindre, explorativ studie av ett specifikt fall, med syfte att belysa ett fenomen snarare än att generalisera till totalförsvaret som helhet. Eftersom studien har en tolkande och abduktiv ansats syftar slutsatserna inte till statistisk generalisering, utan till att generera kontextspecifik kunskap och fördjupade insikter i komplexa fenomen (Schwartz-Shea & Yanow 2012, s. 32).

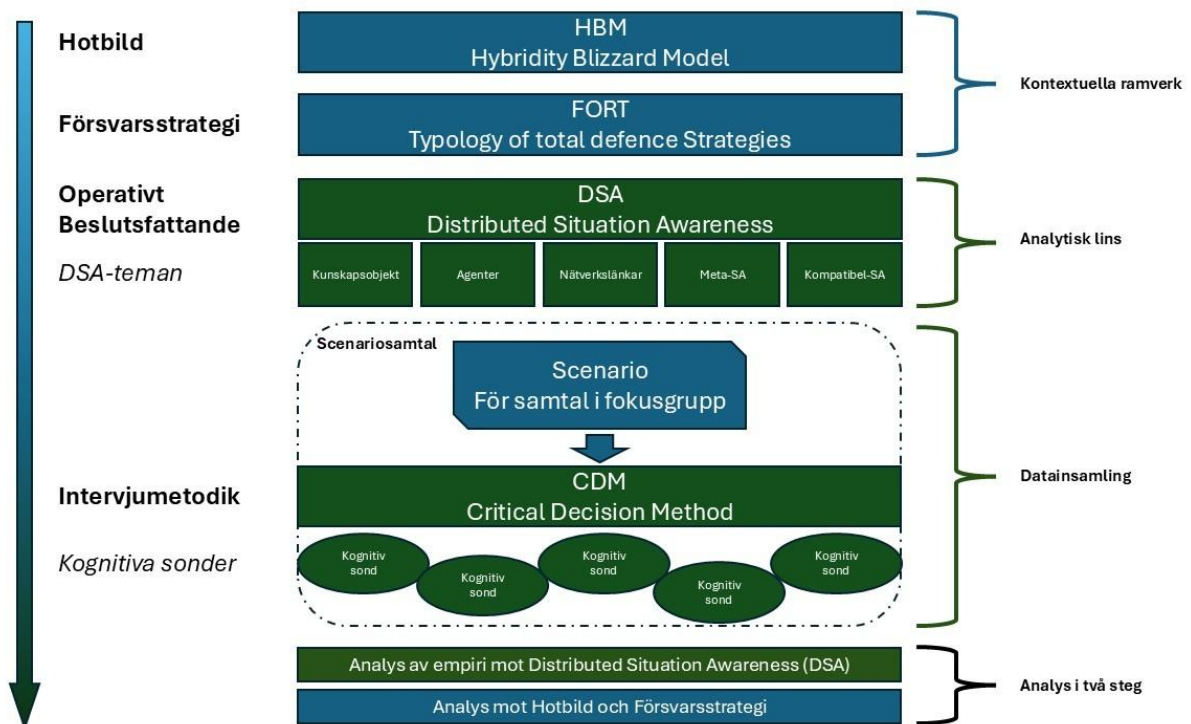


Fig. 3 Design av studiens genomförande

4.2 De kontextuella ramverken: Hotbild och Försvarsstrategi

HBM utgör studiens diagnostiska hotbilda-ramverk för att analysera hanteringen av tvetydiga händelser och behovet av synkroniserad tolkning. Fort-logiken fungerar som den normativa linsen för att granska hur totalförsvarets radikala decentralisering ramar in och skapar förutsättningar för den situationsmedvetenhet som krävs för samordnade motåtgärder. Tillsammans sätter dessa ramverk scenen för att undersöka spänningen mellan lokal autonomi och strategiska krav.

4.3 Den analytiska linsen: Distributed Situation Awareness

Genom DSA operationaliseras lägesbild till ett systemfenomen för att kartlägga hur aktiverad kunskap kommuniceras mellan systemets aktörer. Analysen fokuserar på att spåra hanteringen av en situation steg för steg och värdera länkarnas betydelse för att uppnå en kompatibel lägesförståelse. Fem centrala teman har extraherats från ramverket för att strukturera undersökningen: kunskapsobjekt, aktörer, nätverkslänkar, meta-SA samt kompatibel-SA (se fig. 4).

Tema	Analytisk Funktion
Kunskapsobjekt	Den specifika information som behövdes för hantering av händelse.
Aktörer	Innehavarna av <i>Kunskapsobjekten</i> . Mänskliga operatörer och teknologiska system.
Nätverkslänkar	Kommunikationsvägar och informationsöverföringar mellan <i>aktörerna</i> .
Meta-SA	<i>Aktörernas</i> medvetenhet om vem som vet vad.
Kompatibel-SA	Bedömning av <i>aktörers</i> olika SA är tillräckligt kompatibla för en samordnad åtgärd.

Fig. 4 Teman extraherade från DSA.

4.4 Datainsamling: Scenariosamtal med fokusgrupper

Studien tillämpar ett strategiskt urval baserat på centralitetsprincipen för att identifiera nyckelaktörer inom elförsörjningssektorn (Esaiasson 2017, s. 269). Urvalet innebar att personer med funktioner som var mest relevanta för studiens problemställning prioriterades för att säkerställa en bred variation av erfarenheter (Esaiasson 2017, s. 267). Vid rekryteringen framkom en uttalad vilja att delta, driven av ett intresse att låta en extern part belysa verksamheten för framtida utveckling. Det empiriska materialet samlades in via scenariosamtal om 60–120 minuter, med tre fokusgrupper på nationell, regional och lokal nivå. Genom att nyttja gruppdynamiken genereras data som tydliggör hur aktörer tillsammans bearbetar gråzonsutmaningar och skapar en kollektiv förståelse (Bryman, Bell & Harley 2025, s. 553). Det hypotetiska scenariot (Bilaga 1) fungerade som katalysator för retrospektiv reflektion kring faktiska erfarenheter, samtidigt som det möjliggjorde öppen diskussion utan att beröra operativt känsliga detaljer.

Intervjumethodik: Critical Decision Method (CDM)

Samtalen struktureras kring de fyra CDM-stegen: briefing, identifiering av beslutspunkter, sondering och kontroll (Klein, Calderwood & MacGregor 1989, s. 465-467). Under briefing användes intervjuguiden för att tydliggöra samtalets ramar och hjälpa informanterna att relatera scenariot till tidigare verkliga situationer. Istället för traditionella intervjufrågor fungerade de kognitiva sonderna som stöd för reflektion, där en informants insikter ofta genererade nya perspektiv hos de andra deltagarna. Som moderator var rollen främst att ställa förståelseinriktade följdfrågor, då den aktiva gruppdynamiken i sig drev processen att belysa systemets underliggande logik.

CDM Steg	Syfte
1. Briefing	Introducera scenariot (ett hypotetiskt fall) samt ramar för samtalet.
2. Identifiering av beslutspunkter	Strukturerad enligt OODA-loopen, där beslutsfattande krävs av aktören.
3. Sondering av beslutspunkter	Huvuddelen av intervjun där kognitiva sonder används för att få fram den kunskap som aktiverades.
4. Kontroll	Verifierar tolkningen av händelsekedjan.

Fig. 5 Intervjustruktur Critical Decision Method (CDM)

Beslutspunkter enligt OODA-loopen

För att skapa en händelsebaserad struktur i samtalen nyttjades OODA-loopens fyra faser som beslutspunkter. OODA (Observe, Orient, Decide, Act) är en cykel i fyra steg för beslutsfattande i dynamiska miljöer (Brehmer 2008, s.46, 60). I studien nyttjas OODA-loopen för att ge samtalen och den efterföljande analysen en struktur som underlättar förståelsen av hur informanterna tolkar och hanterar situationer. Detta hjälper läsaren att följa hur en händelse utvecklas från observation till praktisk handling. Frågorna utformades med koppling till de fastställda DSA-teman som kognitiva sonder för att tydliggöra vilken kunskap som aktiverades hos studiens aktörer vid de olika faserna i händelseförloppet (Se bilaga 2 Intervjuguide).

4.5 Analysmetod: En process i två steg

Analysen genomfördes som en abduktiv process i två steg utifrån ordagrant transkriberat material som lästs upprepade gånger för en helhetsbild. Inledningsvis genomfördes en riktad innehållsanalys på empirin från scenariosamtalen mot de fem teman som extraherats från DSA-ramverket. Detta gjordes i varje fas av OODA-loopen i syfte att systematiskt kartlägga hur den operativa lägesbilden formas eller brister. De mönster som framkommit vid analysen mot DSA tolkades därefter abduktivt mot den strategiska kontexten genom ramverken HBM och Fortlogiken samt tidigare forskning.

4.6 Etiska aspekter

Studien har bedrivits i enlighet med Vetenskapsrådets principer för god forskningssed, där skyddsintresset har givits företräde på grund av ämnet hybridhot mot kritisk infrastruktur (Vetenskapsrådet 2024, s. 12).

Forskningen har strikt efterlevt kraven på information, samtycke, konfidentialitet och nyttjande (Vetenskapsrådet 2024, s. 62,66). Informanterna informerades skriftligt och muntligt om studiens syfte och sitt frivilliga deltagande, vilket inkluderade rätten att när som helst avbryta sin medverkan och att granska egna citat före publicering (Vetenskapsrådet 2024, s. 63).

För att värna informanternas integritet och nationella säkerhetsintressen har empirin generaliserats och anonymiserats, endast deltagarnas arbetsområde redovisas (Vetenskapsrådet 2024, s. 86).

<u>Fokusgrupp</u>	<u>Informanter</u>
Nationell	N1, N2, N3
Regional	R1, R2
Lokal	L1, L2

I enlighet med nyttjandekravet och god ordning används insamlade data exklusivt för studiens genomförande och förvaras på lösenordsskyddad enhet för att raderas efter att uppsatsen blivit bedömd (Vetenskapsrådet 2024, s. 42,84). Gällande reflexivitet har jag beaktat min outsiderposition för att minimera bias. Studiens trovärdighet stärks genom rikligt stöd av representativa citat, vilket möjliggör för läsaren att bedöma tolkningarnas rimlighet. Studiens trovärdighet stärks även genom en transparent redogörelse för analysens olika steg och den abduktiva pendlingen mellan empiri och teori.

4.7 Avgränsningar

Ett hypotetiskt scenario innebär en medveten begränsning eftersom det inte helt kan återskapa den stress och det informationsbrus som kännetecknar en faktisk gråzonsincident. Studiens styrka ligger dock mindre i att förutsäga exakt beteende eller identifiera systemets konkreta begränsningar och mer i att synliggöra de kognitiva processer, kommunikationsmönster och underliggande antaganden som aktiveras. För detta syfte var CDM-metoden särskilt väl lämpad, då den möjliggjorde insikt i systemets underliggande logik även utan en verklig händelse som utgångspunkt.

5. Empiri och analys

5.1 Analys mot Distributed Situation Awareness (DSA)

Detta kapitel presenterar empiri från scenariosamtal med nationella, regionala och lokala aktörer. Intervjun utgår från ett hypotetiskt scenario (Bilaga 1 Hypotetiskt scenario) och resultaten struktureras efter OODA-loopens fyra faser för att spegla hur lägesbild och beslut växer fram dynamiskt under ett händelseförlopp. Genom ramverket för DSA belyses samverkan mellan kunskapsobjekt, aktörer och nätverkslänkar. Analysen integrerar även meta-SA samt kompatibel-SA. Genom att följa intervjuernas struktur förtydligas hur tyngdpunkten mellan olika DSA-teman skiftar och hur innehavare av kunskap och mandat förändras under skeendets gång. Analysen utgår från informanternas beskrivningar och tolkas genom de teoretiska ramverken, vilket innebär att resultaten bör förstås som tolkningar av aktörernas meningsskapande snarare än objektiva beskrivningar av systemet.

5.1.1 Observera-fasen

Intervjuerna indikerar samstämmigt att den initiala observationen av avvikelser i elsystemet i första hand tolkas som ett resultat av tekniska övervakningssystem. Dessa terminerar i de dygnet runt-bemannade driftcentralerna på nationell, regional och lokal nivå.

När icke-rutinmässiga händelser identifieras eskaleras de vidare till nyckelaktörer som organisatoriskt är placerade utanför den tekniska driftledningen: på den nationella nivån till en Tjänsteman i beredskap (TiB) och på regional eller lokal nivå till en Vakthavande ingenjör (VHI).

Genom respondenternas resonemang tolkas skillnaden mellan dessa roller i deras fokus vid hantering av indikationer: VHI har en mer direkt teknisk koppling till händelsen, medan TiB ansvarar för en övergripande helhetssyn och koordinering på nationell nivå för att undvika detaljfokus. Denna struktur är utformad för att möjliggöra att systemet kan hantera både teknisk komplexitet och strategisk inriktning samtidigt.

Det framgår av samtalen att de mänskliga iakttagelserna utgör ett nödvändigt komplement till tekniska övervakningen. På nationell nivå rapporteras dessa främst av egen personal i fält eller externa aktörer. På regional och lokal nivå fungerar även allmänheten som en viktig extern observatör genom att rapportera misstänkta händelser direkt till aktören eller polisen. Regional aktör lyfter fram att allmänheten i dag har en ökad förståelse för både omvärldsläget och verksamhetens betydelse, vilket har stärkt rapporteringsviljan.

Ofta är vi ganska bra förankrade i de här små orterna. De känner någon som arbetar hos oss. Man kan ju fundera, varför har man så god förståelse som allmänhet? Det ena är att man har bred förståelse för omvärldsläget, men det andra är att man förstår hur det kan påverka vår verksamhet... (R1).

Genom DSA-ramverkets lins framträder bilden av att aktörerna på samtliga nivåer förfogar över robusta kunskapsobjekt för att hantera tydliga tekniska fel. Lokala aktör betonar att observationer och hantering av tekniska avbrott och fel är en integrerad del av deras normala verksamhet, till skillnad från många andra samhällsfunktioner. "Vi har ju avbrott hela tiden. Inte hela tiden, men rätt så frekvent... Vi lever ju i den här modellen hela tiden...vi har det i DNA på ett annat sätt" (L1).

För att identifiera vaga signaler som inte framstår som naturliga tekniska fel uppfattas senior kompetens och erfarenhetsbaserad kunskap avgörande på samtliga nivåer för att tolka vaga kunskapsobjekt. Regional aktör (R2) beskriver exempel där erfarna operatörer kan notera när händelseförlopp avviker från det förväntade och reagerar på det som inte händer. "Ett larm har inte rört sig på länge, fast den borde ha gjort det" (R2). Det påtalas av både regional och lokal aktör att det finns betydande svårigheter att identifiera dessa signaler som hybridhot i ett tidigt skede, då man saknar nödvändig underrättelseinformation från högre nivå och myndigheter.

Samarbetet på nationell nivå med myndigheter som Polisen och MSB fungerar väl genom formaliserade processer för operativ samordning. Genom strukturerade veckomöten kalibreras normalbilden mot TiB:s omvärldsbevakning, vilket stärker förmågan att tolka och sammanställa kunskapsobjekt. TiB samverkar därefter med centrala aktörer inom elförsörjningen för att jämföra och förankra lägesbilder. Informationsutbytet sker dock med försiktighet, då materialet ofta utgör öppen information som riskerar att bli föremål för utlämning. "Men det är fortfarande öppen information så att det ska kunna begäras ut. Rent krasst. Så vi är ju ändå lite försiktiga med hur vi delar information åt båda hållen" (N1).

Regional och lokal nivå ser sig själva som systemets faktiska ögon och öron i fält. Avsaknaden av indikationer "uppifrån" gör det enligt R1 svårare att vidta proaktiva åtgärder med ökad vaksamhet, vilket skulle möjliggöra fler rapporter uppåt i systemet.

...man behöver inte veta exakt vad det handlar om men bara att man i det här området under den här tidsperioden, höjd vaksamhet. Då kan man ju rapportera in om man ser någonting specifikt... vi är en upptäckande förmåga för hela Sverige. Om man lägger

ihop det i deras sammanställning, kan det då göra oss bättre, till att vara de här bra ögon och öron. Då bidrar vi till hela systemets förstärkning (R1).

Vid fysiska incidenter och tekniska fel som kräver åtgärd på plats är tekniker i terrängen centrala aktörer. Möjligheten att tillvarata kunskapsobjekt på plats utnyttjas inte fullt ut för rapportering uppåt. Detta har av lokal aktör identifierats som ett förbättringsområde. L1 beskriver att orsaken är att det saknas en naturlig rutin och en formaliserad rapporteringsstruktur för personalen i fält att systematiskt föra in sina observationer i systemet. För att motverka detta planeras införandet av standardiserade rapporteringsmallar. Utmaningen ligger i att fånga upp svaga signaler, såsom mindre sabotage eller avvikande detaljer. ”det där kabelskåpet som är lite snett och vint och saboterat lite i halsen” (L1). L2 förtydligar att detta kan framstå som vanlig skadegörelse men potentiellt dölja en fientlig intention vilket är svårt att tolka på plats om man inte har tillgång till aktuell hotbild från t ex Polisen.

Alla pratar om riskerna, de är vi väl medvetna om i form av stora investeringar i regionen och så vidare. Och det drar till sig kriminalitet, det är alla medvetna om. Men vi får aldrig signalerna konkret på frågorna. Vad ska vi vara extra noga på? Vad förekommer? Nej, det finns ingenting. Så det är ett hålrum (L2).

Här uppstår friktion då det saknas enhetliga, krypterade sambandssystem mellan de olika aktörerna. Med hänvisning till ”ordonnans”, delvis skämtsamt men med ett tydligt allvar, illustrerar R1 hur bristen på robusta och säkra kommunikationskanaler i extremfall kan göra fysisk budbärare till det enda återstående alternativet för säker informationsöverföring.

Analys av Observera-fasen mot DSA

Informanterna beskriver att sektorn hanterar rutinmässiga driftstörningar väl, men upplevs ha svårigheter att tolka vaga kunskapsobjekt som inte framstår som naturliga tekniska fel. I dessa lägen uppfattas senior kompetens och erfarenhetsbaserad kunskap som en framgångsfaktor för att identifiera subtila avvikelser. Systemets operativa aktörer löser problem autonomt genom ett decentraliserat arbetssätt, men deras bidrag till lägesbilden hämmas av att de sällan får strategisk hotbildsinformation från högre nivåer. Informanterna använder begreppet uppdragstaktik för att beskriva sitt arbetssätt, vilket i denna studie tolkas som ett uttryck för decentraliserat beslutsfattande nära verksamheten. Informanternas beskrivningar pekar på ett upplevt informationsglapp, där avsaknaden av enhetliga sambandssystem inom nätverkslänkarna tolkas som en central sårbarhet i systemet. Informanterna beskriver att bristen

på proaktiv delning "top-down" upplevs minska vaksamheten i fält, vilket kan tolkas som en bidragande faktor till att färre observationer av distribuerade kunskapsobjekt rapporteras "down-up" från terrängen, vilket framstår som en begränsning för den nationella lägesbildens fullständighet utifrån informanternas beskrivningar.

5.1.2 Orientera-fasen

När en initial avvikelser har observerats övergår processen i ett skede av aktiv verifiering och tolkning.

Lokala och regionala aktörer menar att det "i princip alltid" (L1) krävs fysisk kontroll och utsänd personal för att fastställa händelseförloppet. Denna verifiering utgör startpunkten för vidare tolkning, där personal i ledningscentralen, montörer och VHI samverkar för att bedöma information och skapa en rimlig lägesuppfattning. Framgången i processen är delvis personberoende och vilar ofta på VHI:s erfarenhet och tekniska kompetens. Skulle händelsen eskalera är det enligt L1 inga problem att få tag på ledningsgruppen för beslutsstöd, även de som för tillfället inte har formell beredskap. "...vid större haverier, framför allt på värmesidan, så är det inga problem att få tag på halva ledningsgruppen om man behöver beslutsstöd" (L1).

De formella länkarna för att kommunicera uppåt utanför egen koncern är enligt lokal aktör inte tydliga, vilket i praktiken gör att man tvingas förlita sig på informella nätverkslänkar för att kompensera denna brist. "Särskilt om vi lämnar koncernen och ska kommunicera uppströms på elsidan så blir det mer och mer personberoende faktiskt" (L1).

På regional och lokal nivå har denna sårbarhet identifierats och därför pågår ett arbete med att formalisera rollfördelningen genom Nato-inspirerad stabsstruktur (1-9). Syftet är att tydliggöra roll och funktion, vilket L2 beskriver som en nödvändig utveckling. "Men det tycker jag vi har uppmärksammat ändå som en sårbarhet och mer tänka rollkort och olika saker. Jag tänker nu Nato-modellen, för att mer och mer tänka funktion och roll" (L2). L1 understryker att denna strukturella förändring stöds av kraven på kontinuitetsplanering i den nya cybersäkerhetslagen NIS-2, vilket leder till att kritiska processer formaliseras.

Detta kontrasteras mot den nationella nivåns mer formaliserade meta-SA, som vilar på strukturerad myndighetssamverkan som till exempel deltagande i MSB:s veckovisa samverkanskonferenser. Här tillämpas kollektivt analysarbete via stabsprocesser och analytiska verktyg, vilket tydligt skiljer fakta från antaganden. Genom representanter från alla kritiska

verksamhetsdelar möjliggörs en systematisk faktagranskning som enligt N2 resulterar i en kvalitetssäkrad, gemensamt förankrad lägesbild och inriktning.

I materialet framträder att samtliga aktörer beskriver användning av iterativa arbetsformer för att kontinuerligt ompröva och värdera osäker information. På nationell nivå sker detta genom att anpassa stabsbemanningen efter behov, medan regional och lokal nivå använder regelbundna pulsmöten i syfte att både sprida och inhämta aktuell information.

Regional aktör belyser att bristen på underrättelseinformation från myndigheter och nationell nivå har resulterat i ett större behov av mer aktivt arbete från den egna säkerhetsfunktionen med att analysera händelserapporter för att upptäcka mönster och avvikelser i kunskapsobjekten. Genom att identifiera avvikande trender tidigt kan enligt R1 resurserna användas mer träffsäkert, vilket stärker förmågan att hantera svårtolkade situationer. ”Det kan vara allt ifrån att stärkt säkerhetsövervakning, bemanning eller uppmärksamhet” (R1).

...vi lägger ju resurser för vår verksamhet, både för att fånga upp information och föra vidare, men också för att skydda det som är samhällsviktigt. Och för att kunna göra det med bra resurser, får vi bara en indikation och vet att här kan vi kraftsamla, då kan vi göra mycket resurseffektivare insatser... (R1)

På regional nivå förstärks denna problematik av att extern underrättelseinformation från SÄPO (Säkerhetspolisen), Försvarmakten och Länsstyrelsen inte når fram proaktivt, utan måste aktivt efterfrågas. R1 belyser den slutenhet som finns i systemet: ”Men vi är nog lite hemliga i vår egen bubbla precis som de andra aktörerna är hemliga, men vi försöker få dem att dela mer ... Man behöver få ut informationen till den som faktiskt behöver ha den” (R1).

Endast nationella aktörer har tillgång till krypterade kanaler mot relevanta myndigheter, medan lokal nivå förlitar sig på Rakel. Detta bedöms dock vara sårbart i ett scenario med telekrig: ”Rakel kommer säkerligen inte funka så bra vid telekrig” (L1).

Analys av Orientera-fasen mot DSA

Enligt ansvars- och närhetsprincipen agerar lokala aktörer autonomt där sakkunskapen finns, och pågående formalisering av roller syftar till att stärka meta-SA genom att minska personberoendet. Samtidigt framträder brister i nätverkslänkarna som en central systemutmaning. Avsaknaden av säkra vertikala kanaler för strategiska kunskapsobjekt innebär att Meta-SA kan, utifrån informanternas beskrivningar, tolkas som ojämnt fördelad mellan nivåerna och i hög grad beroende av informella kontakter. Detta kan tolkas som att möjligheten

att utveckla kompatibel-SA över nivåer begränsas. Orientera-fasen visar att kunskapsobjekt och aktörer inom respektive aktörs kärnverksamhet är robusta, men att systemets gemensamma förståelse kan tolkas som hämmat av fragmenterad meta-SA.

5.1.3 Besluta-fasen

På den nationella nivån ligger Beslutsmandatet formellt hos organisationens högste chef och dess ledningsgrupp. Staben agerar som ett stöd genom att föreslå åtgärder för ledningsgruppen. Beslutsmandatet kan delegeras, men N1 understryker att det finns en "självkorrigerande regel" som innebär att "Ju mer värden som är kopplade till eller påverkar myndigheten, desto högre upp klättrar det i hierarkin". På den nationella nivån har man "våldigt starka möjligheter att peka med en hand" (N1), och genomföra tvingande beslut som kan gå emot regionala och lokala aktörers vilja.

Beslutsfattandet lokalt och regionalt är decentraliserat och bygger på ett stort handlingsutrymme, vilket ger operativa roller som tekniker, operatörer och VHI tydliga mandat nära verksamheten. Mindre fel hanteras direkt, medan VHI ansvarar för eskalering till affärsområdeschef, företagsledning eller krisledning vid behov. Strukturen ger förutsättningar för snabba åtgärder och återställning av funktion genom att beslut fattas där den operativa kunskapen är störst. Mandaten har tydliga gränser: beslut med nationella konsekvenser, exempelvis avstängning av elproduktion eller infrastruktur, eskaleras till högsta ledning. Vid höjd beredskap sker en övergång till nationell styrning där myndigheter prioriterar verksamheten utifrån övergripande samhällsintressen.

Informanterna ger uttryck för att den gemensamma förståelsen (kompatibel-SA) inom elsektorn är relativt god, med kännedom om nationella prioriteringar och mandat. Både regional och lokal nivå accepterar omedelbart nationellt mandat att beordra bortkoppling. Lokal aktör konstaterar att "vi har 15 minuter på oss att koppla ifrån" (L1) enligt lagen och att det finns en gemensam förståelse för målsättningen: "Även om vi inte vill släcka ner ett område så förstår vi att det finns anledning till det" (L1).

Samtliga aktörer betonar vikten av flexibilitet i Besluta-fasen. Den lokala aktören ser dock en risk för handlingsförlamning vid snabba, självständiga beslut under osäkerhet. Ett arbetssätt som bygger på stort individuellt handlingsutrymme förutsätter handlingskraft, men denna kan undergrävas om felbedömningar riskerar att leda till repressalier. Som L2 uttrycker det: "man hyllas ju när det går bra, men det kan ju också skapa en handlingsförlamning om vi har någon form av repressalier...".

Analys av Besluta-fasen mot DSA

Besluta-fasen präglas av en dubbel logik, centraliserat mandat och decentraliserad handlingsfrihet. Den nationella nivån innehar ett övergripande styrmandat med befogenhet att fatta tvingande beslut, medan lokala och regionala aktörer har ett betydande handlingsutrymme att agera nära verksamheten. Detta kan tolkas som att systemets aktörer har tydliga beslutsmandat inom sina respektive roller. Samtidigt framträder en risk när vaga kunskapsobjekt och osäkra situationer sammanfaller med upplevd risk för personligt ansvar, rädslan för repressalier kan skapa beslutsförlamning och därmed påverka tempo och handlingskraft. Den så kallade "självkorrigerande regeln" säkerställer dock att beslut med nationell betydelse eskaleras uppåt, vilket kan tolkas som att kompatibel-SA är relativt stark avseende operativa mål, trots svagheter i nätverkslänkarna.

5.1.4 Agera-fasen

Agera-fasen utgör den sista delen i OODA-loopen där beslut omsätts i praktisk handling, vilket i sin tur genererar nya observationer och sluter systemets feedback-loop.

Lokalt och regionalt är agerandet utpräglat decentraliserat och vilar på aktörernas yrkesstolthet och tekniska expertis. Aktörerna i fält beskrivs som snabba exekutörer som via uppdragstaktik autonomt fokuserar på att återställa funktionen. L2 understryker detta fokus: "De är ju supersnabba. För deras uppgift är ju att få tillbaka funktionen så fort som möjligt".

På nationell nivå distribueras strategiska beslut till linjeorganisationen för verkställande genom "soft power" (N1), där staben koordinerar processen snarare än att detaljstyra den tekniska driften. Lokal nivå påtalar även vikten av individuell resiliens för hela systemets motståndskraft.

Jag sa till L2 i måndags att den viktigaste skriften vi har är den här gula (Om krisen eller kriget kommer/MSB förf. *anm.*) som har kommit i brevlådan. Om inte L2 kan klara sig en vecka då kan inte hen komma hit och fatta bra beslut. Det är det viktigaste vi har (L1)

Om en åtgärd inte leder till avsett resultat betraktar den nationella nivån förmågan att ompröva inriktning och justera beslut som en avgörande styrka. Enligt N1 betonar den interna utbildningen i stabsmetodik vikten av att inte låsa analysen vid en enskild hypotes. Den

nationella nivån framhåller en ständig beredskap att ”ta ett steg tillbaka och välja en ny väg” (N1) när ny information tillkommer.

Oavsett om en händelse är ett tekniskt fel eller beror på antagonistisk påverkan, inverkar inte detta på det omedelbara agerandet, då det överordnade målet är snabb funktionsåterställning. På nationell nivå uttrycks detta tydligt: ”Spelar det någon roll för agerandet? Nej, inte i något fall egentligen” (N1). Motsvarande syn återfinns på lokal nivå, där fokus entydigt ligger på funktionsåterställning: ”För oss är det lika illa, oavsett om det är en statlig aktör eller ett tekniskt fel” (L1). Regional nivå delar denna uppfattning, R2 framhåller att även om gråzonsagerande är komplext, återställande av funktion är alltid det primära oavsett vad eller vem som tillskrivs händelsen. Lokal aktör menar att personalens grundinställning ofta utgår från att händelser är tekniska fel. ”Men jag tror inte att deras första tanke är att det är ett hot eller ett sabotage, utan det är tekniskt ett fel” (L2). Lokal och regional nivå anser att de har begränsad kapacitet för strategisk tolkning, varför bedömningen i praktiken överläts till aktörer som Säkerhetspolisen och Försvarsmakten. Då bedömningsresultat sällan återkopplas nedåt i systemet kan detta bidra till ökad osäkerhet i gråzonslägen.

Analys av Agera-fasen mot DSA

I materialet framträder en bild av att Agera-fasen domineras av aktörer och lokalt självständigt agerande, där den enskilde medarbetaren utgör kärnan i systemets operativa motståndskraft. Informanterna beskriver att individuell resiliens och personlig grundberedskap möjliggör snabbt återställande av funktion. Samtidigt framträder en strukturell begränsning, då handling prioriteras före attribuering. Fokus på vad som hänt snarare än varför kan tolkas som att sannolikheten minskar att synkroniserade antagonistiska mönster identifieras. Svaga nätverkslänkar och ett vertikalt informationsglapp kan innebära att aktörer saknar strategiska kunskapsobjekt som kunde bredda tolkningen. Meta-SA förblir därmed splittrad och kompatibel-SA begränsas till operativa mål, vilket kan innebära att nästa OODA-loop riskerar att inledas utan fördjupad strategisk förståelse.

5.1.5 Sammanfattande analys mot DSA

Genom den riktade innehållsanalysen, där DSA-teman vägleder tolkningen av informanternas utsagor, framträder en bild av att energisektorn uppvisar operativ styrka, samtidigt som nätverkslänkarna belyser ett hinder i form av vertikalt splittrad informationsspridning. I Observera-fasen framgår av materialet att relevanta kunskapsobjekt genereras, men vaga

signaler tolkas inte mot en övergripande strategisk hotbild. I Orientera-fasen beskriver informanterna en hög sakkunskap, men brister i meta-SA och nätverkslänkar gör att tolkningen förblir lokalt avgränsad. Besluta-fasen präglas av tydliga mandat och ett fungerande decentraliserat beslutsfattande, men osäkerhet kan påverka beslutsviljan. I Agera-fasen är tempot högt och funktionsåterställning prioriteras, men attribuering nedtonas. Sammantaget framträder i materialet en bild av att operativ robusthet samexisterar med vad som kan tolkas som strategisk blindhet. Avsaknaden av fungerande vertikal informationsintegration kan tolkas som att varje ny OODA-loop riskerar att inledas från en icke-antagonistisk baslinje, vilket försvårar upptäckten av koordinerade hybridhot.

5.2 Analys mot Hotbild och Försvarsstrategi

Analysen indikerar en spänning mellan operativ robusthet och vertikala informationsglapp. Informanternas beskrivningar pekar på att begränsad proaktiv informationsdelning kan försvåra möjligheten att tolka avvikelser som delar av en samordnad antagonistisk helhet.

Fort-logikens spänning: Operativ robusthet kontra strategisk blindhet

Informanterna beskriver sektorn som operativt robust, präglad av en stark yrkesidentitet och ansvarskänsla för sitt samhällsviktiga uppdrag. Krishantering beskrivs som en integrerad del av verksamheten, där det "sitter i DNA" (L1). Detta kan förstås som förenligt med Fort-logikens betoning på decentraliserad resiliens och självförsörjande aktörer. Ångström och Ljungkvist (2024) beskriver den nuvarande svenska strategin som just en sådan radikal decentralisering.

Samtidigt framträder brister i nätverkslänkarna, där informanterna beskriver ett vertikalt informationsglapp som begränsar tillgången till strategisk hotbildsinformation. Svenska kraftnät (2024, s. 20) uppmanar aktörer att vara vaksamma på sin normalbild, men utan strategisk återkoppling försvåras möjligheten att tolka avvikelser som del av en samordnad kampanj.

En central styrka är att beredskap i hög grad betraktas som ett individuellt ansvar, där personlig resiliens utgör en viktig del av systemets operativa förmåga. Ångström och Ljungkvist (2024, s. 508) framhåller att denna decentralisering förutsätter just ett sådant individuellt ansvarstagande.

Gråzonsproblematikens utmaning: Attribuering i snöstormen

Informanterna beskriver en strategisk sårbarhet i att attribuering ges en begränsad roll i det operativa arbetet, där fokus ligger på att återställa funktion snarare än att förstå orsaken. Detta kan dölja synkroniserade antagonistiska angrepp och i frånvaro av proaktiv

informationsdelning bidra till vad HBM benämner "false-negatives" (Weissmann 2021, s. 270), där sådana handlingar integreras i vardagliga driftstörningar.

Detta kan förstås som en risk att OODA-loopen bryts, vilket kan begränsa systemets möjlighet att utveckla en fördjupad strategisk förståelse. "Nyckeln är att utveckla ett detekteringssystem som samtidigt är medvetet om både falska positiva och falska negativa resultat" (Weissmann 2021, s. 15). I detta sammanhang framstår erfarenhetsbaserad kunskap som central för att tolka vaga signaler som tekniska system kan missa.

I Observera-fasen lyfter regionala och lokala aktörer fram att bristen på vertikal underrättelseinformation från nationell nivå försvårar möjligheterna till attribuering. Om den begränsade informationsdelningen beror på sekretessbedömningar bör informationen kunna bearbetas och anpassas till mottagarens nivå. Det aktörerna efterfrågar är i första hand indikationer på höjd vaksamhet, exempelvis inom ett visst geografiskt område eller under en avgränsad tidsperiod. Sådan information skulle stärka deras förmåga att vidta proaktiva åtgärder för att skydda den samhällsviktiga verksamhet de ansvarar för. Vidare framhålls att ökad närvaro i terrängen och höjd vaksamhet sannolikt skulle gynna både informationsinhämtning och rapportering uppåt i systemet.

Militära underrättelse- och säkerhetstjänsten (Försvarsmakten 2024, s. 30) konstaterar att underrättelseverksamhet i ökande grad riktas mot civila förmågor och civil infrastruktur som Försvarsmakten är beroende av. Mot denna bakgrund framträder ett gemensamt intresse mellan civila och militära aktörer av att relevant underrättelseinformation delas proaktivt med berörda aktörer.

Att överbrygga skarvarna

Informanterna beskriver att brister i kompatibla sambandssystem och informationsdelning mellan nivåer utgör en central svaghet i sektorn. Detta kan begränsa möjligheten att dela strategiska indikationer och skapa en sammanhållen lägesbild.

Samtidigt framträder att dessa brister förstärks av organisatoriska och juridiska gränser mellan aktörer, vilket gör att systemets "skarvar" förblir sårbara i gråzonen. Informationsdelningen kan även påverkas av aktörernas förståelse för varandras behov samt av sekretessregler, vilket kan bidra till en försiktighet i att dela underrättelseinformation.

Borch & Heier (2025) visar att den specialisering som följer av Fort-logiken skapar administrativa mellanrum som kan utnyttjas av hybrida aktörer. För att hantera detta lyfts behovet av ett nätverksbaserat arbetssätt och ett "dubbelt grepp", där aktörer förmår se bortom den egna sektorns gränser.

Informanternas beskrivningar pekar på att avsaknaden av formaliserade vertikala länkar gör informationsflödet beroende av enskilda individer snarare än av organisationens struktur. Detta kan förstås som att meta-SA förblir personbunden, vilket gör kompatibel situationsmedvetenhet sårbar för organisatoriska gränser och personalomsättning.

Samtidigt framträder att informella relationer kan underlätta samverkan mellan aktörer (Alvinus & Hedlund 2024, s. 605). Analysen pekar därmed på en spänning mellan behovet av formalisering och värdet av personbaserade nätverk i utvecklingen av kompatibel situationsmedvetenhet.

6. Slutsats, diskussion och fortsatt forskning

Studiens syfte har varit att analysera hur aktörer inom totalförsvarets decentraliserade ledningsstruktur förstår och hanterar gråzonsproblematikens tvetydighet i arbetet med att etablera en kompatibel lägesbild inom energiförsörjningssektorn. Mot bakgrund av studiens begränsade empiriska underlag, bestående av tre fokusgrupper baserade på ett hypotetiskt scenario, bör resultaten förstås som tolkande insikter i hur aktörer skapar mening kring gråzonsproblematik, snarare än som generaliserbara slutsatser om totalförsvaret som helhet.

I materialet framträder en bild av att energisektorn ger uttryck för en hög operativ robusthet, samtidigt som den av informanterna kan tolkas som strategiskt sårbar.

Operativ robusthet och upplevd strategisk sårbarhet

Studien indikerar att energisektorn, enligt informanternas beskrivningar, ger uttryck för en hög operativ robusthet. Informanterna beskriver att teknisk professionalitet, uppdragstaktik och lokal resiliens bidrar till att störningar hanteras snabbt och effektivt. Detta kan tolkas som förenligt med Fort-logikens ideal om självförsörjande enheter.

Samtidigt framträder i materialet en samlad bild av vad som kan tolkas som en strategisk sårbarhet kopplad till brister i vertikal informationsintegration.

Gråzonsproblematikens tvetydighet innebär att enskilda händelser sällan framstår som antagonistiska i sig. För att sådana händelser ska kunna tolkas som delar av en koordinerad

kampanj framstår vertikal informationsintegration som betydelsefull. Informanterna beskriver att strategiska indikationer i begränsad utsträckning delas proaktivt från nationell nivå, vilket kan innebära att lokala aktörers möjlighet att uppfatta avvikelser som något annat än tekniska fel begränsas.

Utifrån studien av energiförsörjningssektorn framträder en bild av ett system som kan tolkas som operativt effektivt, men som samtidigt av informanterna upplevs som strategiskt fragmenterat i gråzonen.

Informationsparadoxen

Studien indikerar vad som kan förstås som ett systemiskt Moment 22. I ljuset av den riktade innehållsanalysen och HBM-ramverket pekar informanternas beskrivningar på att avsaknaden av strategisk information top-down kan tolkas som en hämmande faktor för lokala aktörers möjlighet att inta höjd vaksamhet. Detta kan i sin tur innebära att rapportering down-up begränsas, vilket gör att den nationella lägesbilden riskerar att förbli ofullständig och att möjligheten att koppla ihop indikationer enligt HBM försvåras.

Detta kan förstås som en självförstärkande cirkel där frånvaron av informationsdelning riskerar att leda till en begränsad upptäcktsförmåga. I HBM-termer kan detta innebära en risk för systematiska *false-negatives*, där antagonistiska handlingar integreras i vardagliga driftstörningar utan att attribueras. Studiens abduktiva ansats belyser att den decentraliserade strukturen inte framstår som problemet i sig, snarare indikerar informanternas resonemang en spänning där kombinationen av decentralisering och restriktiv informationsdelning tolkas som problematisk för vaksamheten. Studiens resultat pekar mot att informationsintegration framstår som en viktig förutsättning för att decentraliseringen ska fungera i enlighet med Fort-logikens ideal. Utan sådan integration kan autonomi riskera att omvandlas till isolering.

Empirin indikerar att lokala aktörer i hög grad prioriterar funktionsåterställning framför attribuering. Detta framstår som rationellt ur ett operativt perspektiv, men kan samtidigt tolkas som strategiskt riskabelt. När OODA-loopen förkortas från Observera direkt till Agera utan en fördjupad Orientera-fas, kan systemet förlora möjligheten att bygga kognitiv motståndskraft. Systemet återställs, men lär sig inte nödvändigtvis.

Strategisk riktning

Resultaten kan tolkas som att informationsparadoxen är kopplad till behovet av en kulturell och institutionell förskjutning, inte från sekretess till öppenhet, utan från reaktiv

informationsdelning till selektiv, proaktiv indikationsdelning. Informanterna beskriver att lokala aktörer inte efterfrågar detaljerad underrättelseinformation, utan snarare inriktning, indikation samt tids- eller områdesspecifik vaksamhet.

Uppsatsens titel, *Mind the Gap*, adresserar det avgörande beroendet mellan operativ detektion och strategisk resiliens. I gråzonen framstår motståndskraften inte enbart som beroende av teknisk redundans, utan av förmågan att skapa en samstämmig lägesförståelse som förenar nivåerna i systemet. Detta kan tolkas som att den operativa lägesbilden inte enbart är en fråga om taktiskt agerande, utan även en strategisk förutsättning för att bygga ett samhälle som kan identifiera och hantera antagonistiska metoder.

Mind the gap framträder därmed inte enbart som en retorisk uppmaning, utan kan förstås som en strategisk förutsättning.

Försvarmaktens växande beroende av det civila försvaret

Studiens resultat kan förstås mot bakgrund av det strukturella skifte som skett sedan kalla kriget. Försvarmakten har i dag avvecklat stora delar av sina egna försörjningsresurser och framstår som i hög grad beroende av civila infrastrukturer för mobilisering, uthållighet och operativ effekt.

Energiförsörjningen utgör en grundförutsättning för ledningssystem, transporter och samhällelig stabilitet. Informanternas beskrivningar kan förstås som att begränsad förmåga att detektera och rapportera koordinerade hybridhot kan påverka Försvarmaktens handlingsfrihet redan i gråzonen, innan ett väpnat angrepp inletts.

I ljuset av Galeottis (2022) "weaponisation of everything" blir civila sårbarheter operativa mål i en förbekämpningsfas mot svensk militär förmåga. Motståndskraft framstår därmed inte enbart som beroende av teknisk redundans, utan av förmågan att skapa kompatibel situationsmedvetenhet över civila och militära gränser. Detta belyser hur Försvarmaktens roll kan förstås i relation till vertikal informationsintegration, där selektiv och proaktiv indikationsdelning framstår som en faktor som kan stärka civila detektionsförmåga och därigenom den operativa handlingsfriheten.

Samhälleliga och etiska implikationer

Studien belyser ett fundamentalt etiskt dilemma mellan öppenhet och säkerhet. Resultaten pekar på att ökad medvetenhet om hoten hos privata aktörer är en central aspekt i att bygga

motståndskraft, samtidigt som identifiering och kommunikation av sårbarheter kan ge en potentiell antagonist information som förbättrar deras angreppsmetoder.

Här väcks frågan om studiens egna resultat innebär en säkerhetsrisk. Genom att tydliggöra existensen av ett vertikalt informationsglapp och ett beroende av informella, personbaserade nätverk synliggörs svagheter som en antagonist potentiellt kan exploatera. Resultaten indikerar vad som kan förstås som en brist på underrättelser ner i systemet, vilket kan bidra till minskad vaksamhet och därigenom begränsad rapportering uppåt.

Ur ett samhällsperspektiv framstår det som betydelsefullt att dessa sårbarheter synliggörs. Att låta bristerna förbli dolda kan förstås som förenat med större risker än att diskutera dem öppet, då det är i dessa administrativa mellanrum som hybridhot kan verka. Att höja medvetenheten framstår som ett centralt steg i att stärka motståndskraften.

Totalförsvarets decentralisering kan innebära att individer på lokal nivå förväntas fatta beslut under strategisk osäkerhet. Ett sådant system kan förstås som beroende av en samhällelig etik som accepterar att handlingskraft under osäkerhet kan innebära risk för fel. Utan en sådan acceptans finns en risk att totalförsvaret begränsas i sin praktiska handlingsförmåga.

Teoretisk och metodologisk reflektion

Användandet av DSA som analytisk lins har varit ändamålsenligt för att synliggöra att en gemensam lägesbild i ett decentraliserat system inte handlar om identisk information hos alla aktörer, utan om kompatibilitet för att nå gemensamma mål. Genom att kombinera detta med HBM har studien kunnat belysa hur tvetydighet i gråzonen används som ett strategiskt verktyg för att försvåra försvararens beslutsfattande.

Studiens abduktiva ansats har varit central för att möjliggöra en iterativ växelverkan mellan empiri och teori. Genom ett induktivt, utforskande fokus fångades aktörernas tysta kunskap och subjektiva erfarenheter av gråzonsproblematik. Allt eftersom mönster framträdde i analysen tillämpades deduktiva element genom ramverken DSA, HBM och Fort-logiken för att tolka dessa mönster. Denna process möjliggjorde en tolkning där lokala observationer kunde relateras till en bredare kontext.

Med Fort-logiken som normativ lins tydliggörs den strategiska rationaliteten bakom totalförsvarets nuvarande uppbyggnad. Teorins fokus på radikal decentralisering kunde bidra till att förstå den operativa robusthet som uppstår när lokala aktörer agerar som självförsörjande enheter med ett stort handlingsutrymme nära verksamheten.

Även om decentraliseringen är långt gången i enlighet med närhetsprincipen, är de civil-militära gränserna fortfarande tydliga snarare än oskarpa. Analysen indikerar ett betydande informationsglapp och brist på enhetliga samband mellan civila aktörer och myndigheter som Försvarsmakten, vilket kan begränsa möjligheten till integration. Analysen indikerar att utvecklad samverkan och proaktiv delning av strategiska kunskapsobjekt framstår som centrala aspekter i att stärka systemets samlade förmåga.

Reflektionen synliggör en grundläggande spänning, där strategin eftersträvar motståndskraft genom vaksamma fort, men där DSA-analysen indikerar att denna isolering samtidigt riskerar att skapa informationsöar. Metodologiskt har studien därmed kunnat problematisera om Fort-logikens krav på autonomi i praktiken försvårar den kompatibla-SA som framstår som central för att hantera koordinerade hybridangrepp.

Metodvalet CDM har varit centralt för att fånga aktörernas intuitiva beslutsfattande och tysta kunskap, vilket kan tolkas som att senior erfarenhet utgör en viktig del av systemets detektionsförmåga. En kritisk reflektion bör dock riktas mot den medvetna avgränsningen att använda ett hypotetiskt scenario. Valet gjordes för att undvika att röra vid skarpa sårbarheter eller tekniska detaljer som omfattas av försvarssekretess. Metodologiskt kan detta framstå som en begränsning, då ett scenario inte fullt ut kan återskapa det informationsbrus, den press och stress som kännetecknar en verklig gråzonsincident. Det finns en risk att informanterna i en trygg intervjumiljö överskattar systemets förmåga, medan en verklig incident med samtidiga händelser skulle kunna utmana nätverkslänkarna och meta-SA mer än vad studien haft möjlighet att visa. Samtidigt har scenariot fungerat som en nödvändig katalysator för att synliggöra de underliggande kognitiva mönstren och de strukturella glapp som annars riskerar att förbli osynliga i vardagsdriften.

Fortsatt forskning

Då studien indikerar på vad som kan förstås som ett informationsglapp mellan civila och militära aktörer, vilket kan begränsa utvecklingen av kompatibel situationsmedvetenhet i gråzonen, väcker detta frågor som sträcker sig bortom energisektorn. Resultaten bör förstås som kontextbundna insikter från energisektorn och utgör ett bidrag till vidare utforskning av fenomenet i andra sektorer.

Vidare forskning kan med fördel fokusera på hur civil-militär informationsintegration kan utvecklas. Resultaten pekar mot att utvecklingen av en mer heltäckande situationsmedvetenhet i systemet kan vara kopplad till en kulturell förskjutning från en restriktiv *need to know*-logik till en mer delningsorienterad ansats, präglad av *dare to share and compare*.

Förslag på frågeställningar för vidare forskning:

1. Hur kan olika modeller för vertikal informationsdelning påverka relationen mellan sekretess, tillit och kompatibel situationsmedvetenhet i totalförsvaret?
2. Vilka kognitiva och organisatoriska hinder kan påverka utvecklingen av ett dubbelt grepp hos beslutsfattare, och hur relaterar detta till förmågan att etablera kompatibel situationsmedvetenhet mellan myndigheters ansvarsområden?

Redovisning av generativ AI i skrivprocessen:

Under arbetet med denna studie har författaren använt verktyget *NotebookLM* i syfte att förbättra studiens läsbarhet och språk. Efter användningen granskade och redigerade författaren innehållet och tar fullt ansvar för innehållet i den publicerade uppsatsen.

7. Referenser

Alvinius, A. & Hedlund, E. (2024). A Colossus on Clay Feet? Mechanisms of Inertia in Civil-Military Collaboration within the Context of Swedish Total Defense. *Defence studies* 24(4): s. 601–623.

Asp, V. (2023). *Förutsättningar för krisberedskap och totalförsvar i Sverige*. 2023 uppl. Stockholm: Försvarshögskolan.

Borch, O. J. & Heier, T. (red.). (2025). *Preparing for Hybrid Threats to Security: Collaborative Preparedness and Response*. Taylor & Francis.

Brehmer, B. (2008) Hur man åstadkommer en snabbare OODA-loop: överste Boyds syn på ledning. *Kungliga Krigsvetenskapsakademiens handlingar och tidskrift*. (4), 42–68.

Bryman, A., Bell, E. & Harley, B. (2025). *Brymans samhällsvetenskapliga metoder*. 4. uppl. Liber.

Elonheimo, T. (2021). Comprehensive Security Approach in Response to Russian Hybrid Warfare. *Strategic studies quarterly: SSQ* 15(3): s. 113–137.

Esaiasson, P. (2017). *Metodpraktikan: konsten att studera samhälle, individ och marknad*. 3. uppl. Stockholm: Norstedts juridik.

Fridman, O. (2017). Hybrid Warfare or Gibridnaya Voyna? *RUSI Journal* 162(1): s. 42–49.

Försvarsberedningen (2017), *Motståndskraft. Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021-2025*, Ds 2017:66, Stockholm: Försvarsdepartementet.

Försvarsmakten (2024). *MUST Årsöversikt 2024*.

<https://www.forsvarsmakten.se/contentassets/546bbe13064a4c739e1cbc4b5e4571f7/2024-must-arsoversikt.pdf> (Hämtad 2026-01-28).

Galeotti, M. (2022). *The Weaponisation of Everything: A Field Guide to the New Way of War*. Yale University Press.

Hoffman, F. G. (2007). *Conflict in the 21 century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.

Jonsson, D. K. (2018). *Gråzonproblematik och hybridkrigföring – påverkan på energiförsörjning*. Totalförsvarets forskningsinstitut (FOI). FOI-R--4590--SE.

Jonsson, D. K. (2020). *Preparing for Greyzone Threats to the Energy Sector*. Royal United Services Institute (RUSI).

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

Jonsson, D. K., Ingemarsdotter, J., Johansson, B., Rossbach, N. H., Wedebrand, C. & Eriksson, C. (2019). *Civilt försvar i gråzon*. Totalförsvarets forskningsinstitut (FOI). FOI-R--4769--SE.

Jonsson, O. (2019). *The Russian Understanding of War: Blurring the Lines between War and Peace*. Georgetown University Press.

Klein, G. A., Calderwood, R. & MacGregor, D. (1989). Critical Decision Method for Eliciting Knowledge. *IEEE transactions on systems, man, and cybernetics* 19(3): s. 462–472.

Olsén, M., Melander, A. & Eckersand, U. (2020). *Samverkan och ledning i gråzon*. Totalförsvarets forskningsinstitut (FOI). FOI-R--4959--SE.

Regeringen (2015). *Försvarspolitisk inriktning – Sveriges försvar 2016-2020*. Proposition 2014/15:109.

Schwartz-Shea, P. & Yanow, D. (2012). *Interpretive research design: concepts and processes*. Routledge.

Stanton, N. A. (2016). Distributed Situation Awareness. *Theoretical issues in ergonomics science* 17(1): s. 1–7.

Stanton, N. A., Stewart, R., Harris, D., Houghton, R. J., Baber, C., McMaster, R., Salmon, P., Hoyle, G., Walker, G., Young, M. S., Linsell, M., Dymott, R. & Green, D. (2006). Distributed Situation Awareness in Dynamic Systems: Theoretical Development and Application of an Ergonomics Methodology. *Ergonomics* 49(12–13): s. 1288–1311.

Svenska kraftnät (2024). *Öppen antagonistisk hotbild för elförsörjning*. SvK 2024/2196. <https://www.svk.se/49ad62/siteassets/3.sakerhet-och-beredskap/sakerhetsskydd/dokument/oppen-antagonistisk-hotbild-for-svensk-elforsorjning.pdf> (Hämtad 2026-01-28).

Tillberg, L. V., Berndtsson, J. & Tillberg, P. (2025). Navigating Collaboration: Understanding Civil-Military Interactions in Swedish Total Defence From a Security Network Perspective. *Scandinavian Journal of Military Studies* 8(1): s. 40–56.

Vetenskapsrådet (2024). *God forskningssed*. Stockholm: Vetenskapsrådet. <https://www.vr.se/download/18.4c9f221a191e4edf9053a474/1727853946433/God%20forskningssed%20VR%202024.pdf> (Hämtad 2026-01-28).

Weissmann, M. (red.). (2021). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. I. B. Taurus.

Weissmann, M., Nilsson, N. & Palmertz, B. (2021). Att möta hybridhot och hybridkrigföring. *Kungliga Krigsvetenskapsakademiens handlingar och tidskrift* (4): s. 185.

Wrange, J., Bengtsson, R. & Brommesson, D. (2024). Resilience through Total Defence: Towards a Shared Security Culture in the Nordic–Baltic Region? *European journal of international security* 9(4): s. 511–532.

Ångström, J. & Ljungkvist, K. (2024). Unpacking the Varying Strategic Logics of Total Defence. *Journal of strategic studies* 47(4): s. 498–522.

Bilaga 1 Hypotetiskt scenario

Scenario för intervju med fokusgrupp

Tidpunkt: Fredagen den 19 december 2025.

Bakgrundsläge: Världen befinner sig i ett mycket ansträngt säkerhetspolitiskt läge. Kriget i Ukraina pågår, och Ryssland anser sig vara i en strategisk konflikt med det kollektiva Väst. Diplomatin har nått en kritisk punkt: USA medlar mellan Ryssland och Ukraina, samtidigt som EU arbetar intensivt med att juridiskt möjliggöra att frysta ryska tillgångar lånas ut till Ukraina – ett steg Moskva ser som ekonomisk krigföring. USA har nyligen infört ytterligare sanktioner mot ryska oljebolag. Som svar har kustbevakningsoperationen "Baltic Sentry" skärpts, vilket effektivt begränsar den ryska "skuggflottans" oljetransporter samt kabelbrott i Östersjön.

Naturfenomen och Sårbarhet: Hela Nordeuropa och stora delar av kontinenten befinner sig i greppet av en ovanligt sträng och utdragen köldperiod. Den höga efterfrågan på el driver upp förbrukningen till rekordnivåer. På grund av produktionsbortfall och begränsad importkapacitet råder det just nu stor elfeffektbrist i stora delar av det nordiska synkronområdet. Experter varnar för att Europa kan tvingas till manuell fränkoppling av elförbrukning om effektbalansen inte kan upprätthållas.

Hybridaktiviteter Hösten 2025: Under hela hösten har gråzonshoten eskalerat. Dessa aktiviteter syftade till att kartlägga sårbarheter och skapa osäkerhet, men var då inte främst inriktade mot energisektorn:

- **Cyberattacker:** Mindre cyberangrepp och överbelastningsattacker (DDoS) har rutinmässigt riktats mot myndigheter och finansiella tjänster i Norden och Baltikum.
- **Sabotage/Störning:** En rad kabelbrott på undervattensinfrastruktur (telekomkablar) i Östersjön har rapporterats och attribuerats till antagonistisk aktivitet.
- **Störningssändning:** Omfattande GPS/GNSS-störningar har förekommit över Östersjön och i Arktis, vilket påverkat tidssynkroniseringen.
- **Underrättelseinhämtning:** En ökning av drönarflygningar över militära och skyddsvärda civila objekt (inklusive vissa kraftverk och hamnar) har noterats, troligtvis som en del av krigsförberedelser.

Den Akuta Krisen December 2025 (Fokus på Energisektorn):

Som en direkt reaktion på Västs ökade ekonomiska och militära påtryckningar (sanktioner, Baltic Sentry, frysta tillgångar), har den antagonistiska aktiviteten nu skiftat fokus specifikt till att destabilisera energiförsörjningen i syfte att "frysa Europa" och underminera dess beslutsfattande.

Under de senaste 48 timmarna har ett flertal koordinerade hybridangrepp riktats mot system inom energi- och dess kritiska beroenden:

1. **Cybermanipulation (IT/OT):** En mycket sofistikerad cyberattack har lyckats penetrera och plantera skadlig kod i styrsystemen (SCADA/OT) hos flera regionala elnätoperatörer i södra Sverige. Operatörerna rapporterar in falska data om reservkraftstillgång, lastbalansering och effektflöden. Detta skapar en allvarlig tolkningsutmaning då det är nästan omöjligt att avgöra om felrapporter är naturliga fel (false-positive) eller avsiktlig manipulation.

2. Logistik/Drivmedel: Flera strategiskt viktiga drivmedelsdepåer som är kritiska för reservkraften har drabbats av fysiskt sabotage, vilket har försvårat tankningen av reservkraft och utrustning för räddningstjänsten. Vissa sabotage har dolts som olyckor eller vanlig kriminalitet.
3. Betaltjänster/Information: Cyberattacker mot betaltjänster och kommunikationssystem har återuppstått, vilket har lett till omfattande störningar i detaljhandeln och drivmedelsförsäljningen. Detta har i sin tur orsakat panik och hamstring av de knappa drivmedelsresurserna, vilket ytterligare försvårar situationen för utryckningsfordon och viktig leveranslogistik.
4. Personal och Förtroende: Desinformation via sociala medier intensifieras. Falsa narrativ sprids om att regeringen i hemlighet prioriterar utländska allierade (enligt DCA-avtalet med USA) när det gäller att distribuera drivmedel och reservdelar, medan svenska hushåll och kritisk infrastruktur (som sjukhus) får frysa. Samtidigt har nyckelpersonal inom energisektorn, som ansvarar för återställande av funktionalitet, blivit måltavlor för hot och trakasserier via sociala medier, vilket skapar psykologisk press och hotar personalens uthållighet.

Bilaga 2 Intervjuguide

Intervjun struktureras efter Critical Decision Method (CDM), som är en retrospektiv intervjustrategi utformad för att fånga aktiverad kunskap under icke-rutinmässiga händelser.

Intervjuerna struktureras kring följande fyra CDM-steg:

CDM Steg	Syfte	Detaljerad Genomförande
1. Briefing	Introducera scenariot (ett hypotetiskt fall) samt ramar för samtalet.	Intervjupersonalen får en översikt över händelsen som ska analyseras samt hur intervjun är strukturerad.
2. Identifiering av beslutspunkter	Kartlägga händelseförloppet.	Intervjuaren har valt ett hypotetiskt fall i syfte att undvika blottlägga skarpa sårbarheter och fastställer de kritiska punkterna till de 4 faserna enligt OODA-loopen, där beslutsfattande krävs av agenten.
3. Sondering av beslutspunkter	Huvuddelen av intervjun där kognitiva sonder används.	Här appliceras specialfrågor för att bryta ner beslutet och få fram den kunskap som aktiverades.
4. Kontroll	Slutlig verifiering av händelseförloppet.	Intervjuaren verifierar tolkningen av händelsekedjan.

1. Briefing

Inom ramen för totalförsvaret utgör säker elförsörjning en grundläggande och existentiell funktion för samhällets överlevnad (Jonsson, 2020). Eftersom nästan all samhällsviktig verksamhet – inklusive transporter, finansiella tjänster, hälso- och sjukvård samt Försvarsmaktens operativa förmåga – är kritiskt beroende av fungerande el och elektronisk kommunikation. Därför blir energiförsörjningssektorn ett prioriterat och attraktivt mål ur ett antagonistiskt perspektiv (Försvarsdepartementet, 2017). Svenska kraftnät (2024), som är systemansvarig myndighet, framhåller att de största antagonistiska hoten mot svensk elförsörjning kommer från kvalificerade statsaktörer som Ryssland, Kina och Iran. Angripare kan dessutom utnyttja sårbarheter som utkontraktering, osäkra leverantörskedjor och utländskt ägande av kritisk infrastruktur för att få inflytande över produktions- och distributionsresurser.

Den svenska totalförsvarsstrategin bygger på en decentraliserad ledningsstruktur och ansvarsprincipen, vilket innebär att ansvaret för att upprätthålla samhällsviktig verksamhet i krig i stor utsträckning ligger hos enskilda aktörer, inklusive privata energibolag (FOI, 2023). Framgången för totalförsvaret kräver därmed att dessa aktörer, särskilt på regional nivå där samverkan mellan det civila och militära försvaret ska ske, har förmåga att samordna sig effektivt (Försvarsdepartementet, 2017). Den största

utmaningen i gråzonen ligger dock i tvetydigheten och svårigheten att attribuera händelserna till en antagonist. Eftersom otydligheten skapar ett stort tolkningsutrymme, försvåras förmågan att snabbt skapa en gemensam lägesbild och vidta kraftfulla motåtgärder (FOI, 2019).

Med utgångspunkt i denna problematik blir det avgörande att analysera hur väl totalförsvarets nuvarande decentraliserade ledningsstruktur förmår att hantera den synkroniserings- och tolkningsutmaning som gråzonsproblematiken innebär. Genom att fokusera på energiförsörjningssektorn kan vi empiriskt undersöka samspelet mellan teoretiska krav och den praktiska förmågan att identifiera och synkronisera tolkningen av antagonistiska aktiviteter i gränslandet mellan fred och krig i syfte att skapa en gemensam lägesbild.

Ramar för intervjun:

Samtalet ska belysa hur lägesbild skapas i praktiken inom ramen för gråzonsproblematik och strategisk icke-fred. Fokus ligger på att förstå erfarenheter och upplevelser, inte att testa kunskap.

Vi vill utforska:

- Hur processen för att skapa en lägesbild fungerar i en miljö präglad av gråzon och otydlig hotnivå.
- Hur decentraliserad ledning inom totalförsvaret påverkar arbetet.
- Hur ansvarsprincipen och närhetsprincipen spelar in i denna kontext.
- Hur den övergripande gråzonssituationen påverkar synen på hot- och lägesbild.

Intervjun ska undvika:

- Frågor som kan kopplas till faktiska sårbarheter.
- Tekniska detaljer om system eller förmågor.

Tonvikten ligger på resonemang snarare än specifika detaljer.

Scenario: Enligt Bilaga 1 Hypotetiskt scenario

2. Identifiering av beslutspunkter

Intervjun utgår från ett hypotetiskt scenario för att undvika att röra vid operativt känsliga detaljer. Med scenariot som bas identifieras de kritiska beslutspunkterna i de fyra faserna av OODA-loopen – där respondenten förväntas fatta beslut.

Faserna är:

- **Observera:** Första indikationen på att något avviker; insamling av information.
- **Orientera:** Bearbetning, tolkning och meningsskapande för att skapa förståelse av situationen.
- **Besluta:** Formulering av en hypotes och val av möjliga åtgärder; framtagande av handlingsplan.
- **Agera:** Genomförandet av beslutet, vilket i sin tur skapar nya förutsättningar.

Om samtalet naturligt pekar mot andra relevanta beslutspunkter utanför OODA-ramverket kommer även dessa att inkluderas.

3. Sondering av beslutspunkter

Observera

1. Första observationen

- Hur brukar den första indikationen på att något inte står rätt till upptäckas?
 - Via tekniska system?
 - Genom mänsklig observation?
 - På något annat sätt?

2. Tidiga signaler

- Finns det vanligtvis svaga eller tidiga signaler som kan uppmärksammas innan en större avvikelse uppstår?
- Hur uppfattas och hanteras sådana mindre störningar?

3. Variabler som påverkar upptäckten

- Finns det perioder eller situationer när vaksamheten är högre och observationer sker snabbare?
 - Exempelvis vid återkommande teknikproblem, underrättelser/förvarningar eller i samband med känslig verksamhet?

4. Bemanningens effekt

- Hur påverkar bemanningssituationen möjligheten att upptäcka avvikelser?
 - Till exempel skillnader mellan dagtid och kväll/helg?
 - Skillnader mellan mer erfaren och mindre erfaren personal?

Orientera

1. Verifiering av den första observationen

- Hur brukar den initiala observationen verifieras?
 - Finns det system som är så felsäkra att verifiering inte behövs?
 - Sker verifiering alltid, ibland eller beroende på typ av avvikelse?
 - Är det upp till den tjänstgörande personalen att avgöra?

2. Tillgång till information

- Upplever ni att all relevant information finns lätt tillgänglig i detta skede?
- Har ni god kännedom om vem som besitter vilken information (Meta-SA)?

3. Begripliggörande

- Hur går arbetet med att skapa en rimlig förståelse av situationen till, även när alla detaljer inte är klara?
 - Hur "etiketteras" händelsen i tidigt skede?
 - Hur påverkar erfarenhet och tidigare kunskap tolkningen?
 - I vilken grad sker meningsskapande genom interaktion och social kontakt inom gruppen?

4. Bedömning av hotbild

- Hur skiljer ni mellan olika typer av avvikelser eller incidenter?
 - Icke-rutinmässiga händelser
 - Naturliga fel eller slumpmässiga störningar
 - Möjliga antagonistiska angrepp

5. Bemanningens betydelse

- Hur påverkar personalens erfarenhet, kompetensnivå och bemanningsläget förmågan att orientera sig?

6. Stöd av manualer och riktlinjer

- Finns det manualer för att hantera oväntade händelser?
 - Är de kända inom verksamheten?
 - Är de övade?
 - Är de aktuella och uppdaterade?

7. Tillgång till bakre stöd

- Vilken typ av bakre stöd finns att tillgå i orienteringsfasen?
 - Till exempel expertkunskap eller erfarenhet från andra delar av organisationen.

8. Kontaktvägar och informationsutbyte (Meta-SA)

- Vilka aktörer kontaktas för att få in mer information respektive för att delge information?
 - Internt?
 - Externt inom sektorn?
 - Externt utanför sektorn?

9. Kommunikationens genomförande

- Hur kommuniceras information i detta skede?
 - Internt och externt
 - Öppet eller krypstat
 - Via tal eller data
 - Genom gemensamma eller kompatibla ledningsstödsystem
- Finns det flaskhalsar eller begränsningar i kommunikationen?

10. Lägesbild i relation till andra pågående händelser

- Vilken information får ni om andra samtidigt säkerhetspåverkande händelser eller störningar?
 - Tillhandahålls den automatiskt?
 - Måste ni aktivt efterfråga eller söka upp den?
- Sträcker sig denna information även utanför den egna sektorn?

Besluta

1. Beslutsmandat och nivåer

- Var ligger normalt beslutsmandatet i en situation som denna?
 - Beror det på hur omfattande beslutet är?
 - Fattas beslut närmast verksamheten eller på en mer central nivå?
 - Var bedömer ni att den bästa lägesbilden (SA) finns när beslut tas?

2. Beslutsstöd genom manualer och regelverk

- Finns det manualer, riktlinjer eller regelverk som stödjer beslutsfattandet?
 - Är dessa kända av personalen?
 - Är de övade i praktiken?
 - Är de aktuella och uppdaterade?

3. Bakre stöd och kompletterande kompetens

- Vilket stöd finns att tillgå i beslutsprocessen?
 - Tillgång till expertkunskap och erfarenhet?
 - Finns möjlighet till delegerat mandat vid behov?

4. Hotbilds- och riskförståelse

- Hur bedöms påverkan och möjliga konsekvenser av beslutet?
- Hur arbetar man med riskmedvetenhet i detta skede?

5. Kontaktvägar och informationsutbyte (Meta-SA)

- Vilka kontakter tas inför ett beslut?
 - För att inhämta nödvändig information?
 - För att delge beslut eller underlag?
 - Vilka aktörer, internt och externt – även utanför sektorn – behöver informeras?

Agera

1. Tidpunkt och förutsättningar för agerande

- Hur bedömer ni när det är optimalt att agera i en sådan situation?
 - Vilka faktorer påverkar tidpunkten för insats eller åtgärd?
- Vilka aktörer är involverade i genomförandet, och vilka mål styr deras agerande?
- Om olika aktörer har skilda mål – hur hanteras dessa skillnader i praktiken?

2. Effekter av åtgärder och nya omständigheter

- Hur följer ni upp vilken effekt en åtgärd eller insats har haft?
 - Åtgärdades störningen eller uppstod nya effekter?
- Hur skapar ni en ny och uppdaterad förståelse av situationen efter genomfört agerande?
 - Hur vidareutvecklas meningsuppdragsskapande efter att man agerat?
- I vilken grad försöker ni tolka motståndarens eventuella intentioner, mål eller troliga nästa steg?

3. Flexibilitet och anpassningsförmåga

- Hur arbetar ni med att behålla flexibilitet efter att ett beslut verkställts?
- Hur säkerställer ni att organisationen kan anpassa sig löpande och undvika stagnation när nya omständigheter uppstår?

4. Kontroll

Syftet med detta steg är att säkerställa att den insamlade informationen korrekt speglar respondentens upplevelser och kognitiva processer under den icke-rutinmässiga händelsen.

Verifiering av information

- Intervjuaren går igenom den rekonstruerade händelsekedjan och de beslut som identifierats, och kontrollerar att dessa överensstämmer med respondentens faktiska upplevelse.
- Det säkerställs att det empiriska materialet är korrekt, komplett och representativt för hur respondenten faktiskt resonerade och agerade i situationen.

Gemensam genomgång och bekräftelse

- Intervjuaren sammanfattar de centrala punkterna och ber respondenten bekräfta att beskrivningarna stämmer.
- Tillsammans klargörs:
 - Vilken aktör eller funktion som bar den avgörande (aktiverade) kunskapen (Meta-SA).
 - Om kommunikationsvägarna (länkarna) som användes var tillräckliga för att skapa en kompatibel och delad lägesbild.