Resiliens inom kritiska infrastrukturer

- **Kartläggning och analys av kritiska infrastrukturers arbete med resiliens.**

Stina Andersson & Felicia Klint

Avdelningen för Riskhantering och Samhällssäkerhet

LTH | LUND UNIVERSITY, SWEDEN

Resiliens inom kritiska infrastrukturer

Kartläggning och analys av kritiska infrastrukturers arbete med resiliens.

Stina Andersson & Felicia Klint

Lund 2021

Resiliens inom kritiska infrastrukturer
- Kartläggning och analys av kritiska infrastrukturers arbete med resiliens.

Resilience of critical infrastructure
- Exploration and analysis of how critical infrastructures work with resilience

Författare: Stina Andersson & Felicia Klint
Handledare: Jonas Johansson

Antal sidor: 97
Illustrationer: Stina Andersson & Felicia klint

Nyckelord:
Resiliens, kritisk infrastruktur, datainsamling, analys, kvalitativ undersökning, förutseende, robusthet, återhämtning, anpassning, Räddningstjänst, Elförsörjning, Telekommunikation

Abstract
There have been much effort during the last decade towards resilience of critical infrastructures, but the research differs and resilience within critical infrastructures is still seen as a relatively new and unexplored area. The purpose of this work is to provide an understanding of how critical infrastructures in Sweden work with resilience. The objective is to create a general framework that can be used to map and analyse how critical infrastructures work with resilience. Based on previous publications, resilience was defined as a concept comprising four abilities; anticipate, resist, recover, and adapt. Using this definition as a foundation, a framework for data collection and analysis was created. The framework describes how critical infrastructures can work with the abilities of resilience based on previous literature. Three critical infrastructures within Sweden were analysed; Rescue service, Electricity supply, and Telecommunications. The analysis was based on information from two to three actors for each critical infrastructure. Information from each actor was collected through a survey, interview, e-mail contact and documents and was analysed through the framework to map how the critical infrastructures work with resilience. The results show that Rescue service works with adaptation the most and with robustness the least. Electricity supply work with anticipation and recovery the most and with adaptation the least. Telecommunications work with anticipation and recovery the most and with robustness the least. The framework is deemed adequate to provide indications of how critical infrastructures work with the abilities for resilience.

Riskhantering och samhällssäkerhet
Lunds tekniska högskola
Lunds universitet
Box 118
221 00 Lund

http://www.risk.lth.se

Telefon: 046 - 222 73 60

Division of Risk Management and Societal Safety
Faculty of Engineering
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

http://www.risk.lth.se

Telephone: +46 46 222 73 60

Förord

Detta examensarbete markerar slutet på vår utbildning på Brandingenjörsprogrammet vid Avdelningen för Brandteknik och på Riskhanteringsprogrammet vid Avdelningen för Riskhantering och samhällssäkerhet vid Lunds Tekniska Högskola. Under arbetet gång har vi fått hjälp av flera personer och vi skulle vilja ta tillfället i akt och tacka dessa.

Vi vill rikta ett stort tack till vår handledare Jonas Johansson, Universitetslektor vid Avdelningen för Riskhantering och Samhällssäkerhet, för den vägledning han gett oss och den kloka input han bidragit med under arbetets gång som gjort detta examensarbete möjligt.

En stor del av arbetet vilar på aktörers vilja att medverka i arbetet. Vi vill därför tacka samtliga aktörer och deras representanter som har besvarat enkäter, ställt upp på intervju(er), stått till förfogande när vi har haft följdfrågor och bidragit med värdefull input till rapportens analysdel. Tack för att ni tagit av er tid för att delat med er av era kunskaper, vi hoppas att ni finner rapporten intressant.

Summary

This work studies the concept resilience and analyses how resilience is applied within critical infrastructures in Sweden, with a focus on Rescue service, Electricity supply and Telecommunication. Resilience is a property that emerges from the combination of the four abilities anticipation, robustness, recovery and adaptation.

- Anticipation is the ability to detect, analyse and plan for future events and any consequences that may adversely affect the function of a critical infrastructure.
- Robustness is the ability to withstand interference and absorb any shock to minimize negative impact on the function of a critical infrastructure.
- Adaptation is the ability to return quickly and efficiently to a state where the function of a critical infrastructure is maintained.
- Recovery is the ability to change, evolve and learn from past events in order to maintain the function of a critical infrastructure.

These four abilities of resilience were identified from scientific literature within the field. Factors that contributes to the four abilities of resilience were also identified from the literature. The factors were divided into organizational and technical factors and compiled in a framework for data gathering and analysis. The developed framework was then applied to three critical infrastructures in Sweden; Emergency services, Electricity supply and Telecommunications. Information about the critical infrastructures was collected through surveys, interviews, email contact, and document search. The collected information was then analyzed using the developed framework.

The findings do not show to what extent critical infrastructures achieve resilience, but rather aim to provide indications of those abilities and factors of resilience that the critical infrastructures are focusing their work on. These findings can be used to compare how different types of critical infrastructure work with the abilities of resilience. The results showed that Rescue Services mostly focuses their work on adaptation and the least on robustness, for example Rescue service work with the factor *implementation of measures* to a greater extent than the factor *plans for unwanted events*. Electricity supply mostly focuses their work on both anticipation and recovery and the least on adaptation, for example Electricity supply work with the factor *resources for recovery* to a greater extent than the factor *exchange of experience for learning purposes*. Telecommunications mostly focuses their work on both anticipation and adaptation and the least on robustness, for example Telecommunication work with the factors *information gathering* and *resources for recovery* to a greater extent than the factor *exercises linked to robustness*. A reason why the critical infrastructures focus on different abilities for resilience could be that they are affected by different types of disruptions. In this report, the idea was to compare the findings regarding how the critical infrastructures work with the abilities of resilience to interference data. However, this did not fit within the timeframe and is therefore suggested as an area for further work.

This report analyzed the work of three different Swedish critical infrastructures regarding the four abilities of resilience. However, the developed framework for data collection and analysis is considered applicable to a variety of critical infrastructures. Furthermore, the framework for data collection and analysis makes it possible to compare how different critical infrastructures work with the abilities of resilience, hence creating an opportunity for the critical infrastructures to transfer experiences and methods across sectors.

Sammanfattning

Detta arbete har undersökt resiliens inom kritiska infrastrukturer i Sverige med fokus på Räddningstjänst, Elförsörjning och Telekommunikation. I denna rapport ses resiliens som en egenskap hos en kritisk infrastruktur som framträder ur kombinationen av de fyra förmågorna förutseende, robusthet, återhämtning och anpassning.

- Förutseende är förmågan att detektera, analysera och planera för framtida händelser och eventuella konsekvenser som kan påverka en kritisk infrastrukturs funktion negativt.
- Robusthet är förmågan att stå emot störningar och absorbera en eventuell chock för att minimera negativ påverkan på en kritisk infrastrukturs funktion.
- Anpassning är förmågan att vid en större störning snabbt och effektivt återgå till ett tillstånd där en kritisk infrastrukturs funktion återigen upprätthålls.
- Återhämtning är förmågan att förändras, utvecklas och dra lärdomar av tidigare händelser för att upprätthålla en kritisk infrastrukturs funktion.

Dessa fyra förmågor för resiliens identifierades från litteratur inom området. Vidare undersöktes dessa förmågor och beskrevs genom mer konkreta faktorer som bidrar till resiliens inom kritiska infrastrukturer. Faktorerna delades in i organisatoriska och tekniska faktorer och sammanställdes i ett ramverk för datainsamling och analys. För att testa hur det utvecklade ramverket kan användas för att undersöka hur kritiska infrastrukturer i Sverige arbetar med de fyra förmågorna för resiliens kontaktades aktörer inom tre olika kritiska infrastrukturer; Räddningstjänst, Elförsörjning och Telekommunikation. För dessa aktörer samlades information in genom enkäter, intervjuer, mejlkontakt och dokumentsökning. Den insamlade informationen analyserades sedan med hjälp av det framtagna ramverket.

Rapportens resultat visar inte till vilken grad de kritiska infrastrukturerna uppnår resiliens, utan syftar till att ge indikationer på vilka förmågor och faktorer för resiliens de kritiska infrastrukturerna fokuserar sitt arbete på. Resultatet visade att Räddningstjänst arbetar mest med förmågan för anpassning och minst med förmågan för robusthet, exempelvis arbetade den kritiska infrastrukturen med faktorn *implementering av åtgärder* i högre grad men endast med faktorn *planer inför oönskade händelser* i lägre grad. Elförsörjning arbetar mest med både förmågan för förutseende och återhämtning och minst med anpassning, exempelvis arbetade den kritiska infrastrukturen med faktorn *resurser för återhämning* högre grad men endast med faktorn *erfarenhetsutbyte i lärande syfte* i lägre grad. Telekommunikation arbetar mest med både förutseende och anpassning och minst med robusthet, exempelvis arbetade den kritiska infrastrukturen med faktorerna *informationsinsamling* och *resurser för återhämtning* högre grad men endast med faktorn *övningar kopplat till robusthet* i lägre grad. En anledning till att kritiska infrastrukturer fokuserar på olika förmågor för resiliens kan vara att de påverkas av olika typer av störningar. Resultatet användes för att jämföra de kritiska infrastrukturernas arbete med förmågorna för resiliens. I denna rapport skulle de kritiska infrastrukturernas arbete med förmågorna för resiliens även ha jämförts mot störningsdata. Detta var dock något som inte rymdes inom ramen för arbetet och är därför ett av förslagen på fortsatt arbete.

Denna rapport analyserade enbart tre olika kritiska infrastrukturers arbete med resiliens. Det utvecklade ramverket för datainsamling och analys anses dock vara applicerbart för en mångfald av kritiska infrastrukturer. Att det genom ramverket för datainsamling och analys går att jämföra hur olika kritiska infrastrukturers arbetar med förmågorna för resiliens skapar dessutom en möjlighet för de kritiska infrastrukturerna att överföra erfarenheter och arbetssätt över sektorsgränser.

Nomenklatur

DHS – Department of Homeland Security
EU – Europeiska Unionen
ISO – International Organisation for Standardization
KI – Kritisk infrastruktur
MSB – Myndigheten för Samhällsskydd och Beredskap
NE- Nationalencyklopedin
NIAC – National Infrastructure Advisory Council
NIPP – National Infrastructure Protection Plan
OECD – Organisation for Economic Co-operation and Development
TiB – Tjänsteman i Beredskap

Innehållsförteckning

1 Introduktion

Tidigare större störningar har visat på ett behov av resiliens inom kritiska infrastrukturer (Boin & McConnell, 2007). Om en störning slår ut kritiska infrastrukturer och tjänsterna som de levererar kommer samhället påverkas i hög grad. För privatpersoner som är beroende av dessa tjänster kan det innebära att man inte kan tillgodose sina basbehov så som mat, vatten och värme (MSB, 2018b). Detta kan ses i tidigare katastrofer så som orkanen Katrina i USA 2005 och cyberattacken på Ukrainas elnät 2015 (Lessin & Deal, 2008; OECD, 2019). Både cyberattacken i Ukraina och orkanen Katrina slog ut stora delar av den kritiska infrastrukturen vilket orsakade omfattande negativa konsekvenser för samhällena (Boin & McConnell, 2007; Lessin & Deal, 2008; Sullivan & Kamensky, 2017). Exempelvis lämnade orkanen Katrina tusentals människor desperata efter mat, vatten och skydd (History.com Editors, 2019; Brodie, Weltzien, Altman, Blendon, & Benson, 2006). För att undvika en kris i samhället behöver de tjänster som anses vara kritiska för människors vardag upprätthållas. Samhällets funktioner upprätthålls genom att infrastrukturer som är kritiska för samhällets funktioner arbetar med konceptet resiliens (MSB, 2019; MSB, 2013b). För att arbeta med resiliens inom de kritiska infrastrukturerna har MSB gett ut flera publikationer inom ämnet. Publikationerna är menade som stöd till aktörer som kan ha en påverkan på samhällets funktioner (MSB, 2018a; MSB, 2013a; MSB, 2011). År 2006 startades dessutom European Programme for Critical Infrastructure Protection (EPCIP), ett program på EU-nivå med målet att förbättra säkerheten inom de kritiska infrastrukturer som finns inom EU (Commision of the European Communities, 2006).

Det senaste decenniet har det skett en ökning av antalet publikationer om resiliens inom kritiska infrastrukturer (Rød & Johansson, 2020). Konceptet resiliens inom kritisk infrastruktur är fortfarande relativt nytt och outforskat och det finns en stor variation inom forskningen (e.g. Fritzon, Ljungkvist, Boin & Rhinard, 2007; DHS, 2013; Wood, 2015; Rød & Johansson, 2020). De publikationer som behandlar konceptet resiliens beskriver oftast hur resiliens uppnås, dock ger de inte övergripande beskrivningar av hur olika kritiska infrastrukturer mer konkret kan arbeta för att uppnå resiliens. Eftersom det inte finns en vedertagen definition på konceptet resiliens eller en generell beskrivning av hur resiliens kan uppnås för kritiska infrastrukturer är det möjligt att de kritiska infrastrukturernas arbete med resiliens varierar. Det är därför relevant att för kritiska infrastrukturer undersöka; hur resiliens kan definieras, hur det går att arbeta med resiliens, hur arbetet med resiliens ser ut, samt skillnader i arbetet med resiliens.

1.1 Syfte och mål

Resiliens inom kritiska infrastrukturer har betydelse för samhällets funktion och säkerhet (MSB, 2013b). Eftersom det antas finnas skillnader i hur olika kritiska infrastrukturer arbetar med resiliens är syftet med denna rapport att öka förståelsen kring hur kritiska infrastrukturer i realiteten arbetar med resiliens. Arbetet avser alltså inte att mäta nivå av resiliens hos kritiska infrastrukturer.

Målet med rapporten är att skapa ett generellt ramverk för datainsamling och analys som kan användas för att beskriva hur kritiska infrastrukturer arbetar med resiliens. Målet innefattar även att kartlägga arbetet med resiliens hos de kritiska infrastrukturerna i Sverige samt beskriva hur arbetet med resiliens mellan kritiska infrastrukturer skiljer sig åt.

1.2 Avgränsningar

Under arbetets gång har flera avgränsningar gjorts, detta på grund av tidsbegränsningar och tillgång till information samt avgränsningar som behövts göras avseende tillåten omfattning för själva rapporten. De avgränsningar som har gjorts i arbetet är:

- Arbetet avgränsas till ett urval av kritiska infrastrukturer i Sverige nämligen Räddningstjänst, Elförsörjning och Telekommunikation.
- Arbetet har inte explicit tagit hänsyn till de beroenden som finns mellan de kritiska infrastrukturerna och hur dessa beroenden kan påverka arbetet med resiliens.
- Arbetets informationsinsamling baseras på två till tre utvalda aktörer inom respektive kritisk infrastruktur. Kritiska infrastrukturer är komplexa och består ofta av ett nätverk med ett antal aktörer. Antalet medverkande aktörer är en avgränsning som varit nödvändig på grund av arbetets tidsram.
- På grund av arbetets tidsram, men även aktörernas begränsade möjligheter att ställa upp på intervjuer, har intervjuerna avgränsats till att vara cirka en timme långa. Att intervjuerna varade endast en timme innebär begränsningar i möjligheterna till fördjupningar i aktörernas arbete.
- Viss information som är relevant för att förstå kritiska infrastrukturers arbete med resiliens har på grund av sekretesskäl inte varit tillgänglig. Innehållet i rapporten har därför behövts avgränsas till den information som inte varit sekretessbelagd.
- Det finns begränsningar i hur mycket information som kan samlas in givet examensarbetets tidsramar. Eftersom resiliens är ett komplext ämne kan enbart mer övergripande bedömningar om arbetet med resiliens göras för både aktörer och de kritiska infrastrukturerna utifrån den information som samlas in.
- Arbetet undersöker endast hur kritiska infrastrukturer arbetar med resiliens och avser inte att mäta eller bedöma hur resilienta kritiska infrastrukturer är.

En stor del av litteraturen som använts i arbetet är skriven på engelska och vissa engelska termer har saknat en tydlig motsvarighet på svenska. I sådana lägen har termerna översatts med det som ansetts vara det mest lämpliga svenska ordet. Detta kan skapa vissa klyftor mellan originaltermen och den svenska översättningen som eventuellt påverkar hur läsaren uppfattar innehållet. Vid vissa tillfällen har därför originaltermen skrivits ut i parentes efter den svenska översättningen för att förhindra detta.

1.3 Frågeställningar

De frågor som denna rapport avser att besvara är:

- Vad är kritisk infrastruktur resiliens och vilka är de mest grundläggande förmågor som resiliens består av i denna kontext?
- Hur kan förmågor för resiliens undersökas inom olika kritiska infrastrukturer?
- Hur arbetar olika kritiska infrastrukturer med förmågor för resiliens och vilka förmågor fokuserar de på?

Kartläggningen och analysen som görs i denna rapport avser sedan vidare att undersöka frågorna:

- Finns det potentiellt utrymme till utveckling avseende enskilda kritiska infrastrukturers arbete med förmågor för resiliens?
- Finns det potentiellt möjlighet till överföring av erfarenheter mellan kritiska infrastrukturer avseende förmågor för resiliens?

2 Teoretisk bakgrund

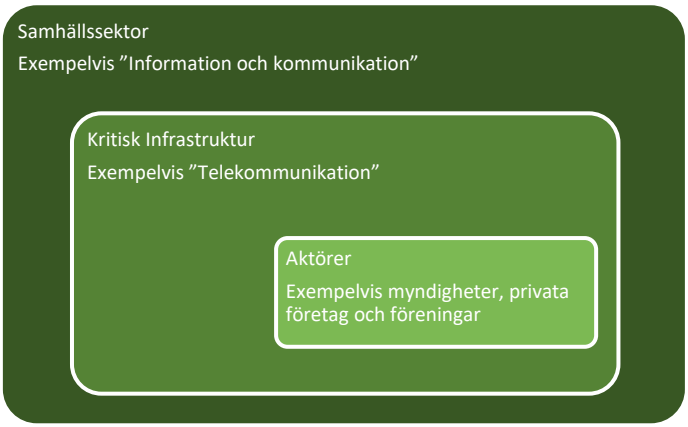
Detta avsnitt beskriver den teori som är centralt för arbetet. Första delen av avsnittet behandlar området kritiska infrastrukturer, andra delen behandlar konceptet risk och tredje delen beskriver konceptet resiliens. För konceptet resiliens görs en djupare genomgång eftersom resiliens utgör grunden till det ramverk för datainsamling och analys som beskrivs senare i rapporten. Den litteratur som har använts i teoriavsnittet har hittats genom litteratursökningar i digitala databaser, bland annat LUBsearch, Google Scholar, ScienceDirect och Researchgate. Litteratursökningen försökte göras så omfattande som möjligt, givet ramarna för examensarbetet, för att skapa en bred bild av respektive teoriområde.

2.1 Kritisk Infrastruktur

Kritisk infrastruktur kan definieras på flera olika sätt. Den definition för kritisk infrastruktur som kommer att användas i detta arbete är Myndigheten för samhällsskydd och beredskaps (MSB) definition för samhällsviktig verksamhet som kom år 2020d och ersatte den tidigare definitionen. Denna definition används eftersom den anses vara generell och snarlik andra definitioner av kritisk infrastruktur ur ett internationellt perspektiv (DHS, 2013; Fritzon, Ljungkvist, Boin, & Rhinard, 2007; Rød & Johansson, 2020; Australian Government, 2015). Dessutom är MSB den myndighet som har fått uppdrag av regeringen att utveckla en nationell strategi för skydd av kritiska infrastrukturer i Sverige (MSB, 2011, s. 2). MSB nuvarande definition på samhällsviktig verksamhet togs i bruk i oktober 2020. MSB definierar samhällsviktig verksamhet som:

Verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet (MSB, 2020d, s. 1).

I MSBs dokument används begreppet samhällsviktig verksamhet på liknande sätt som andra, internationella aktörer, använder begreppet kritisk infrastruktur (Eng. Critical Infrastructure) (DHS, 2013; Fritzon, Ljungkvist, Boin, & Rhinard, 2007; Rød & Johansson, 2020; Australian Government, 2015; MSB, 2013a; MSB, 2014). I detta arbete kommer därmed kritisk infrastruktur användas istället för begreppet ”samhällsviktig verksamhet”. Kritiska infrastrukturer verkar inom samhällssektorer (MSB, 2013a). En samhällssektor är ett område som berör en eller flera viktiga samhällsfunktioner (MSB, 2019). Inom samhällssektorerna verkar flera aktörer som tillsammans skapar kritiska infrastrukturer. De kritiska infrastrukturerna upprätthåller samhällsfunktioner (MSB, 2019). Sambanden mellan aktörer, kritisk infrastruktur och sektor visas i Figur 1.



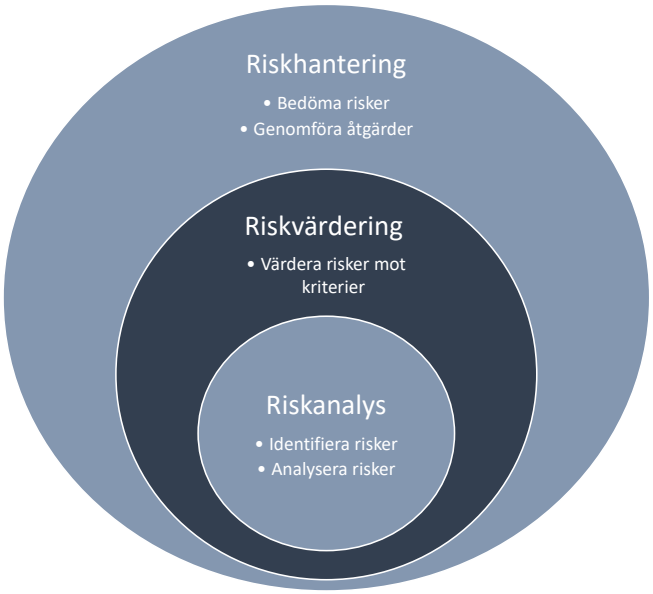
Figur 1. Sambandet mellan aktörer, kritisk infrastruktur och sektor.

2.2 Risk

Risk är ett koncept vars innebörd har varierat över tid, mellan discipliner och sociala- och kulturella sammanhang (Räddningsverket, 2003). Risk kan således betyda olika saker i olika sammanhang, och det finns flera etablerade definitioner för konceptet (Aven, 2007; Cambell, 2005; NE, 2020a). Society for Risk Analysis listar flera definitioner för risk där definitionerna innefattar bland annat sannolikheter för händelser, konsekvenser och osäkerheter (Aven, o.a., 2018). För detta arbete kommer följande definition, som presenterades i en artikel av Aven och Renn (2009), användas för att beskriva risk:

Risk refers to uncertainty about and severity of the events and consequences (or outcomes) of an activity with respect to something that humans value (Aven & Renn, 2009, s. 6).

Eftersom en störning i en kritisk infrastruktur kan utlösa en samhällskris är det viktigt för kritiska infrastrukturer att ha en god riskhantering (MSB, 2013a). Riskhanteringens tre olika delar beskrivs i riskhanteringsprocessen (Räddningsverket, 2003). Processen inleds med att identifiera risker följt av analys av riskerna. Därefter värderas riskerna mot satta kriterier. Sista steget i processen är att bedöma riskerna och genomföra åtgärder som reducerar riskerna (Räddningsverket, 2003). Riskhanteringsprocessen illustreras i Figur 2 nedan.



Figur 2. Illustration av riskhanteringsprocessen.

Inom riskhantering finns flertalet modeller och analysmetoder som används för att analysera och förebygga risker. Ett exempel på en sådan analysmetod är ”What-if”-analys där man identifierar hot och potentiella risker i en brainstorming process genom att ställa frågor som börjar med ”vad skulle hända om…?”. Ett annat exempel är felträdsanalys där möjliga händelsesekvenser som kan leda till negativa effekter analyseras (Center for chemical process safety, 1995). De flesta modeller som är utvecklade för att hantera risker anses förutsätta att man har kännedom om, eller åtminstone kan föreställa sig, oönskade scenarier som kan inträffa. Konceptet risk utgår från att hot är identifierbara och denna premiss begränsar riskhanteringsprocessens möjligheter att hantera oväntade händelser (Park, Seager, Convertino, & Linkov, 2013). Att endast arbeta med riskhantering kan alltså lämna en verksamhet oskyddad mot större oväntade störningar, så kallade svarta svanar (Eng. Black Swans). Park et al. (2013) menar att konceptet resiliens till skillnad från risk utgår från att verksamheter kommer drabbas av oväntade störningar. Risk och resiliens bör inte ses som två koncept som skapar motsättningar (Aven, 2019). Arbete med resiliens bör snarare ses som ett komplement till verksamhetens arbete med risk (Park et al., 2013).

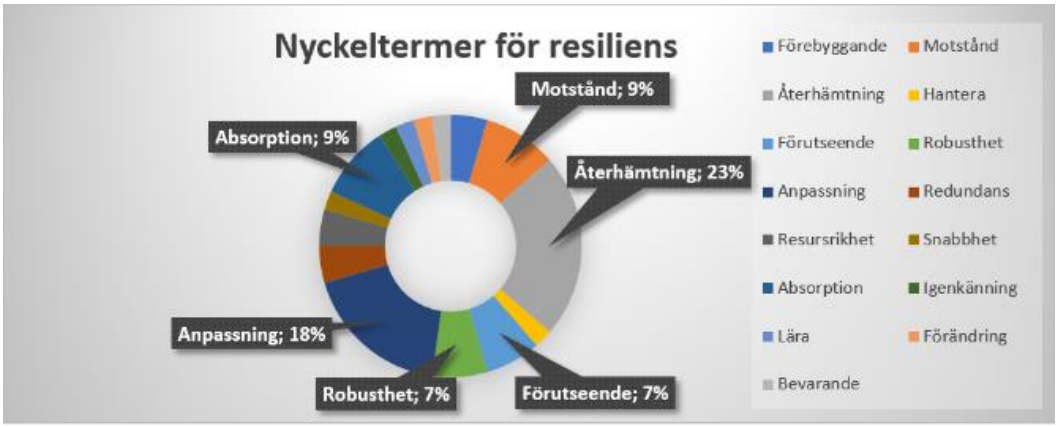
2.3 Resiliens

Konceptet resiliens har genom historien använts på flera olika sätt. Var konceptet resiliens har sin början är inte helt känt. Resiliens användes av romerska Marcus Fabius Quintilianus redan runt 100-talet som ”att undvika” (Alexander, 2013). Resiliens har senare kommit att användas inom mekaniken av bland annat av Rankine år 1867 för att beskriva ett materials egenskaper (MSB, 2013b). Runt 1950 användes resiliens inom psykiatrin för att beskriva psykiatriska problem hos barn (Alexander, 2013). Den moderna användningen av resiliens började med Holling 1973 som applicerade resiliens på komplexa system. Holling använde resiliens för att beskriva hur komplexa system, så som ekosystem, kan återhämtas (Holling, 1973). Holling applicerade på 1990-talet konceptet resiliens på sociotekniska system och ekonomiska system (Walker & Cooper, 2011). Idag används även resiliens inom kritiska infrastrukturer (OECD,

2019; Rød & Johansson, 2020). Definitionerna för resiliens som kan appliceras inom kritiska infrastrukturer är dock varierande och mångfaldiga (Rød & Johansson, 2020). Detta gör att resiliens som koncept är svårt att arbeta med. För att nå en tydlig definition på resiliens för detta arbete har ett flertal olika definitioner från litteratur sammanställts och jämförts. Sammanställningen gjordes i Excel där nyckeltermer från definitionerna plockades ut för att urskilja vilka nyckeltermer som är mest förekommande. Den sammanställda litteraturen har främst varit på engelska och har i arbetet därmed behövt översättas till svenska.

Sammanställningen av definitioner från olika källor för konceptet resiliens presenteras i Appendix A och nyckeltermerna presenteras i Figur 4. Det övergripande syftet med användningen av konceptet resiliens inom den analyserade litteraturen i Appendix A anses vara att beskriva en kritisk infrastrukturs förmåga att förebygga, motstå och hantera störningar för att minimera konsekvenserna för samhällsfunktionen. Hur arbetet med resiliens bör utformas och vad det är som påverkar en infrastrukturs resiliens skiljer sig åt i de olika definitionerna (e.g. Becker, 2014; Fritzon, Ljungkvist, Boin & Rhinard, 2007; DHS, 2013; Wood, 2015).

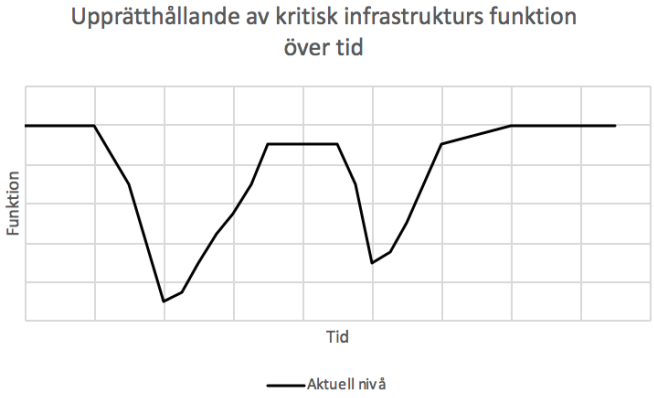
Nyckeltermer från de sammanställda resiliensdefinitionerna redovisas i Figur 3. I Figur 3 framgår det att de sex mest förekommande nyckeltermerna hos resiliensdefinitionerna i den sammanställda litteraturen är; återhämtning, anpassning, motstånd, absorption, förutseende och robusthet (utifrån en översättning av de engelska termerna av författarna). Dessa nyckeltermer verkar därmed beskriva de förmågor som bidrar till de kritiska infrastrukturernas resiliens. De tre termerna absorption, motstånd och robusthet anses innefatta liknande egenskaper (e.g. MSB, 2013a; NIAC, 2010; OECD, 2019) och har därför slagits ihop under termen robusthet i denna rapport.



Figur 3. Sammanställning av nyckeltermer som används för att beskriva konceptet resiliens.

Konceptet resiliens visualiseras ofta som en funktionsnivå över tid. En störning visas generellt som en ”dip” i prestationen för ett system som sedan över tid återgår till den önskade funktionsnivån (e.g. Francis & Bekera 2014; Ouyang & Wang, 2015; Bruneau et al., 2003). En störning anses alltså ske när den kritiska infrastrukturens funktion inte längre upprätthålls. Störningar kan vara både mindre avvikelser från funktionen (elavbrott som pågår en kortare tid) och större avvikelser från funktionen (elavbrott som pågår en längre tid). En störning inom kritiska infrastrukturer kan bero på externa händelser så som olyckor eller naturkatastrofer men även att en aktör inom den kritiska infrastrukturen inte lägre upprätthåller sin verksamhet. I Figur 4 presenteras hur en kritisk infrastrukturs upprätthållande av sin funktion över tid kan

påverkas vid en störning. Funktionsnivå visas på y-axeln och tid visas på x-axeln. Funktionen kan antingen mätas kvantitativt eller kvalitativt. En kvantitativ mätning av en funktion är exempelvis antal abonnenter som har tillgång till elförsörjning över ett år. En kvalitativ mätning av funktion är exempelvis att leveranssäkerheten ska vara bra, vilket baseras på flertal både mer kvantitativa och kvalitativa funktionsmått.



Figur 4. Illustration av hur den kritiska infrastrukturens funktion kan påverkas av störningar över tid.

Baserat på nyckeltermerna i Figur 3 definieras resiliens i detta arbete som en egenskap hos en kritisk infrastruktur att upprätthålla sin önskade funktion eller minimera funktionsbortfall vid störningar genom förmågan att:

1) vara förutseende,
2) vara robust,
3) ha en effektiv återhämtningsförmåga, samt
4) vara anpassningsbar.

I Tabell 1 ges en översikt av dessa fyra förmågor med korta beskrivningar och som sedan följs av mer utförligare beskrivningar. Resiliens ses i denna rapport som en ingående egenskap hos en kritisk infrastruktur. Detta innebär att resiliens inte är något som kan appliceras på en kritisk infrastruktur, utan att det är en inneboende egenskap som en kritisk infrastruktur kan uppvisa. Att resiliens är en egenskap inom kritiska infrastrukturer grundas i NIAC (2010) och OECD (2019) rapporter som beskriver att resiliens är en del av organisationens kultur. Även Becker (2014) och Park et al. (2013) beskriver att resiliens är en systemegenskap som framträder ur systemets aktiviteter.

Tabell 1. Förmågorna för resiliens och deras innebörd.

Förmåga	**Beskrivning**
Förutseende	En kritisk infrastrukturs förmåga att detektera, analysera och planera för framtida händelser och eventuella konsekvenser som kan negativt påverka funktionen.
Robusthet	En kritisk infrastrukturs förmåga att stå emot störningar och absorbera en eventuell chock för att minimera negativ påverkan på funktionen.
Återhämtning	En kritisk infrastrukturs förmåga att vid en större störning snabbt och effektivt återgå till ett tillstånd där funktionen återigen upprätthålls.
Anpassning	En kritisk infrastrukturs förmåga att förändras, utvecklas och dra lärdomar av tidigare händelser för att upprätthålla infrastrukturens funktion.

2.3.1 Förutseende

Förutseende för kritiska infrastrukturer innebär förmågan att förutse potentiella hot och konsekvenser som kan påverka den kritiska infrastrukturens upprätthållande av samhällsfunktionen (Becker, 2014). Enligt Becker (2014) är förmågan att förutse konsekvenser av händelser en förutsättning för att åtgärder som minskar eventuella negativa konsekvenser implementeras. Francis och Bekera skriver i sin artikel från 2014 att förutseende, förutom förmågan att identifiera hot och konsekvenser, även innefattar förmågan att förbereda för att motstå riskerna. Förutseende kommer i detta arbete att innebära den kritisk infrastrukturens förmåga att detektera framtida händelser och eventuella konsekvenser som kan skada funktionen. Vilka åtgärder som implementeras som en följd av identifieringen behandlas under anpassningsförmågan.

2.3.2 Robusthet

I analyserade rapporter och artiklar benämns robusthet på olika sätt. Förmågan robusthet benämns av MSB (2013a) som förmågan att motstå störningar, av NIAC (2010) som förmågan att absorbera chockar från störningar och OECD (2019) benämner robusthet som den kritiska infrastrukturens redundans. Hur robusthet behandlas i litteraturen varierar. Fritzon et al. (2007) skiljer på robusthet och resiliens men att delarna samverkar då robusthet inte kan skydda verksamheten helt. Det förekommer även litteratur där robusthet jämställs med resiliens (Wood, 2015). I detta arbete ses robusthet som en del av resiliens. Robusthet innebär att den kritiska infrastrukturen har förmågan att stå emot störningar och absorbera en eventuell chock, detta för att den kritiska infrastrukturen ska kunna fortsätta fungera även vid en störning. Att en kritisk infrastruktur är robust innebär att vid en eventuell händelse kommer robustheten minimera funktionsfallet hos den kritiska infrastrukturen, vilket beskrivs av Rød och Johansson (2020). Förmågan robusthet framträder under en störning men som bygger på de förberedelser som gjorts innan störningen (Francis & Bekera, 2014).

2.3.3 Återhämtning

Återhämtning är en förmåga som karaktäriseras av att ett system efter en störning snabbt återgår till det önskade tillståndet där systemets funktion upprätthålls (Rød & Johansson, 2020; NIAC, 2010), där det önskade tillståndet antingen innebär ett normaltillstånd eller ett nytt, förbättrat tillstånd (Francis & Bekera, 2014). Återhämtning kommer i detta arbete avse en kritisk infrastrukturs förmåga att vid en störning snabbt och effektivt återgå till ett tillstånd där samhällsfunktionen upprätthålls.

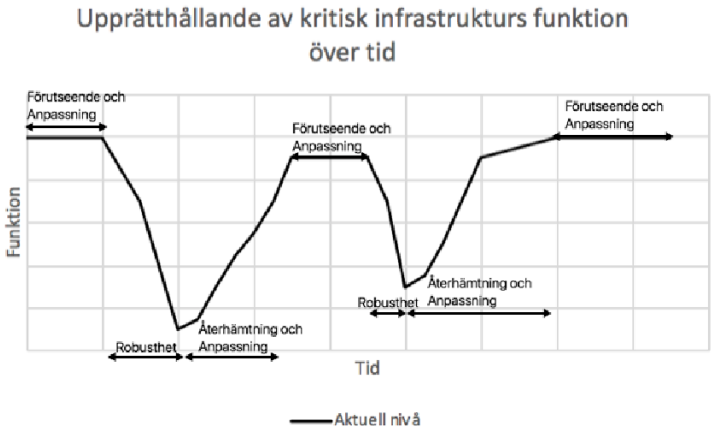
2.3.4 Anpassning

Anpassning används generellt för att beskriva kritisk infrastrukturs förmåga att utvecklas och förändras vid nya förhållanden (Francis & Bekera, 2014; DHS, 2013), dra lärdomar av tidigare störningar (OECD, 2019; DHS, 2013), samt implementera åtgärder för att motverka oönskade situationer, hot och faror (Rød & Johansson, 2020). Lärande från tidigare störningar är en grund för utveckling och åtgärdsimplementering inom kritisk infrastruktur (e.g. MSB, 2013b; NIAC, 2010; OECD, 2019). I detta arbete kommer anpassning innebära en kritisk infrastrukturs förmåga att förändras, utvecklas och dra lärdomar av tidigare händelser för att upprätthålla

infrastrukturens funktion. Anpassning sker både under och efter en störning (DHS, 2013). I detta arbete kommer anpassning främst anses vara en förmåga som visar sig efter att en kritisk infrastruktur har återhämtat sig från en störning.

2.3.5 Samverkan mellan de fyra förmågorna för resiliens

De fyra förmågorna för resiliens samverkar och används kontinuerligt inom kritiska infrastrukturer. För kritiska infrastrukturer sker oftast dagliga mindre störningar som påverkar deras funktion, och som därmed skulle kunna kopplas till konceptet resiliens. Fokus i denna rapport kommer dock vara att vara studera resiliens kopplat till mer storskaliga och oväntade händelser. Detta är i linje med flera vetenskapliga publikationer (Park, Seager, Convertino, & Linkov, 2013; Rød & Johansson, 2020). Vid större störningar kan respektive förmåga generellt kopplas till en viss period i den kritiska infrastrukturens funktion över tid. Förutseende är främst kopplat till tiden innan en störning, robusthet kopplat till tiden under störningen, återhämtning kopplat till tiden efter störningen och anpassning kopplat både till tiden under och efter störningen, vilket illustreras i Figur 5.



Figur 5. Illustration över hur de fyra förmågorna för resiliens samverkar och kan kopplas till ett mer långsiktigt tidsperspektiv där storskaliga störningar.

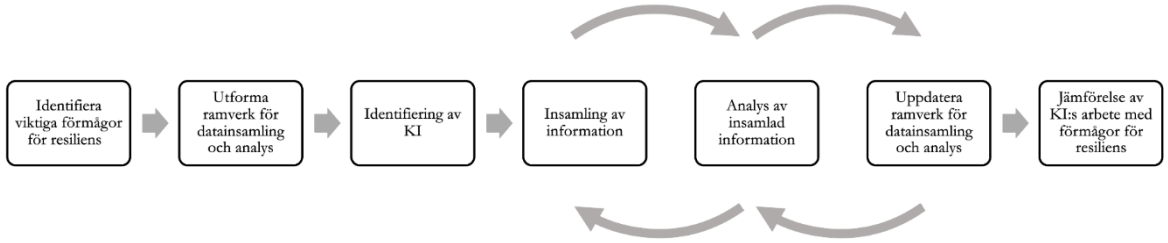
2.4 Kvalitativa metoder för att undersöka resiliens

Tidigare ramverk för konceptet resiliens, med fokus på kritiska infrastrukturer, har främst analyserat resiliens kvantitativt (Francis & Bekera, 2014; Ouyang & Wang, 2015; Johansson, Hassel, & Zio, 2013; Rød & Johansson, 2020; Axelsdóttir & Bjärenstam Jonason, 2018). Kvalitativa undersökningar förekommer endast i mindre utsträckning. Ett exempel på en kvalitativ undersökning som tidigare genomförts är en enkätundersökning av en verksamhets resiliens som gjordes av Shirali, Mohammadfam och Ebrahimipour (2013).

Kvantitativa frågeundersökningar kan ge mycket kunskap om attityder och beteenden, men har dock en begränsad användbarhet när fenomenet som undersöks är komplext och svåråtkomligt (Persson, 2016). Kvalitativa metoder är användbara när innebörden av ett koncept ska analyseras. Detta eftersom kvalitativa metoder ger möjlighet att få en djupare förståelse för fenomen jämfört med kvantitativa metoder som tenderar att främst mäta sådant som kan beskrivas med statistiska mått (Persson, 2016). Detta arbete undersöker vilka förmågor av konceptet resiliens som aktörer inom kritiska infrastrukturer adresserar. Resiliens anses i denna rapport vara en komplex egenskap hos kritiska infrastrukturer som kan mätas både kvalitativt och kvantitativt. För denna undersökning anses dock en kvalitativ metod vara lämplig för att kunna fånga innebörden av kritiska infrastrukturers arbete med konceptet resiliens.

3 Metod

I detta arbete undersöktes konceptet resiliens med hjälp av ett ramverk för datainsamling och analys som har tagits fram som en del av arbetet. Ordningen för de olika stegen i arbetsprocessen illustreras i Figur 6. De två stegen ”identifiera viktiga förmågor för resiliens” samt ”utforma ramverk för datainsamling och analys” adresseras i kapitel Resiliens respektive Ramverk.



Figur 6. De övergripande stegen i arbetsprocessen. KI är en förkortning för kritisk infrastruktur.

3.1 Identifiering av kritiska infrastrukturer

De kritiska infrastrukturerna som undersöks i denna rapport valdes utifrån de totalt 11 stycken sektorer som listas i MSBs handlingsplan (2013a). De kritiska infrastrukturerna som valdes var Telekommunikation, Energiförsörjning samt Räddningstjänst. De kritiska infrastrukturerna valdes för att skapa bredd i undersökningen, men avgränsades i antal för att skapa en rimlig omfattning. Vidare valdes de kritiska infrastrukturerna utifrån intresse och för att koppla till tidigare forskning inom området vid Lunds universitet. En annan faktor vid valet av kritiska infrastrukturer var tillgängligheten, exempelvis valdes sektor ”Hälso- och sjukvård samt omsorg” bort på grund av den höga belastning som sektorn upplever på grund av Covid-19 pandemin vid genomförandet av examensarbetet. Inom varje kritisk infrastruktur kontaktades relevanta aktörer som anses ha stor betydelse för den kritiska infrastrukturens upprätthållande av respektive samhällsfunktion. Den information som samlades in från aktörerna är inte heltäckande men anses användbar som underlag för att bedöma huruvida de kritiska infrastrukturerna uppvisar arbete med förmågorna för resiliens.

3.2 Metod för insamling av information

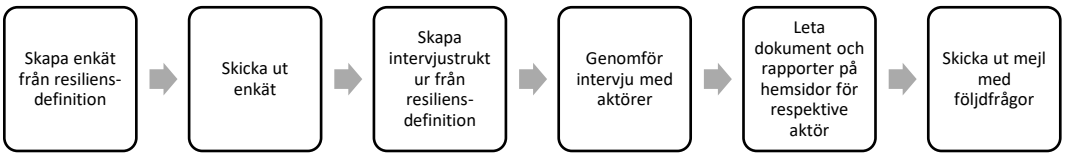
Enkäter och intervjuer användes för att samla in information för att undersöka hur aktörer inom kritiska infrastrukturer arbetar med konceptet resiliens. Den insamlade informationen kommer alltså från individer som arbetar inom de kritiska infrastrukturerna. I de fall där det efter informationsinsamlingen genom enkät och intervju funnits informationsluckor kring aktörernas arbete med förmågorna för resiliens har information dels sökts efter på respektive aktörs hemsida, dels följts upp via mejl med aktörerna.

3.2.1 Utformning av enkät och intervju

Vid enkät- och intervjuundersökningar har frågor delats in i kategorier för att studera hur verksamheter arbetar med de olika förmågorna för resiliens (van de Wiel, 2017; Shirali, Mohammadfam, & Ebrahimipour, 2013). Enkäten och intervjuformuläret delades in i kategorier baserat på de fyra förmågorna för resiliens från definitionen. Enkäten presenteras i

Appendix B. Enkäten utfördes online och bestod av Likertskalor följt av öppna frågor. Likertskalor innebär att respondenten får markera hur väl denne instämmer med frågan på en angiven skala (Persson, 2016). I enkäten användes en numerisk skala med ett jämt antal svarsalternativ (1–6). Enkäten användes dels för att få en grov indikation på aktörernas förhållningssätt till de olika förmågorna för resiliens, dels möjliggöra att få in svar från aktörer ifall aktörer inte skulle ha möjlighet att medverka vid intervjuer.

Enkäter och onlinebaserade intervjuer anses komplettera varandra eftersom de utmaningar som respektive metod har skiljer sig åt (van de Wiel, 2017). Vid användandet av båda metoderna förväntas felkällorna minimeras, exempelvis genom att missuppfattningar minskas vid användning av både enkäter och intervjuer (van de Wiel, 2017). Enkätsvaren kompletterades därför med en frivillig onlinebaserad intervju för de aktörer som hade möjlighet att delta. För att öka möjligheten för aktörerna att ställa upp på en intervju hölls intervjuerna relativt korta, cirka en timme långa. Intervjun utformades med semi-strukturerade frågor och hade som syfte att låta aktörerna utveckla sina enkätsvar och generera djupare förståelse för hur deras kritiska infrastruktur arbetar med förmågorna kopplade till resiliens. Semi-strukturerade intervjuer är intervjuer med delvis färdiga frågor med möjlighet att utforma följdfrågor under intervjuns gång (van de Wiel, 2017). Fördelen med att använda semi-strukturerade intervjuer i undersökningar är att intervjusvaren från olika expertisgrupper kan jämföras (van de Wiel, 2017), där expertisgrupper i denna undersökning avser aktörer inom de kritiska infrastrukturerna som undersöks. För att minska påverkan på respondenterna i enkäten och intervjuerna har ledande frågor, otydliga formuleringar och inbyggda förutsättningar försökts att undvikas i möjligast mån (Bell, 2010). Intervjuerna spelades in och sammanställdes skriftligen som en del av analysen. En sammanfattning av informationsinsamlingen presenteras i Figur 7 nedan.



Figur 7. Arbetsprocess för informationsinsamling från aktörerna.

3.3 Metod för analys av insamlad information

Det insamlande materialet sammanställdes med hjälp av kodning i Excel. Kodning är en metod för att hantera kvalitativ data som innebär att information från intervjuer grupperas i ”kluster” (Bell, 2010). Det insamlade materialet gicks igenom och kodades mot ramverkets faktorer. Kodningens kluster utgjordes alltså av ramverkets faktorer för de fyra förmågorna för resiliens. I de fall då ramverkets faktorer inte ansågs fungera bra som ”kluster” i kodningen av det insamlade materialet så uppdaterades ramverkets faktorer för att bättre representera de kritiska infrastrukturernas arbete med förmågorna för resiliens. Baserat på kodningen gjordes sedan en kvalitativ bedömning av till vilken grad varje aktör arbetade med ramverkets faktorer.

Bedömningen baserades på en sammanvägning av hur mycket av enkät-, intervju-, mejlsvaren och dokument som kunde kodas mot faktorn, samt hur mycket det som kodats mot faktorn ansågs bidra till respektive förmåga (förutseende, robusthet, återhämtning och anpassning). Följande parametrar togs i beaktning när sammanvägningen gjordes:

- Huruvida arbetet med faktorn fokuserar både internt (påverkan inom aktörens verksamhet) och externt (påverkan utanför aktörens verksamhet).
- Huruvida arbetet med faktorn fokuserar på flera områden inom den egna verksamheten.
- Huruvida arbete bidrar till flera områden inom den kritiska infrastrukturen.
- Huruvida arbetet med faktorn betonades som viktigt för verksamhetens resiliens. Exempelvis ifall arbetet har en tydlig koppling till aktören och den kritiska infrastrukturens funktion.

Baserat på ovanstående parametrar bedömdes aktörerna antingen arbeta med faktorerna i högre grad, i lägre grad eller inte alls. Om aktörens aktiviteter bedöms påverka flera områden inom verksamheten, påverkar både aktörens egen verksamhet samt andra verksamheter eller poängteras som viktigt av aktören för dess resiliens bedöms aktören arbeta med en faktor i högre grad. Då aktiviteterna kopplade till en faktor bedöms inrikta sig på begränsade områden, eller inte benämns som viktig av aktören för dess resiliens bedöms aktören arbeta med faktorn i lägre grad. I vissa fall fanns det för lite information för att bedöma till vilken grad aktören arbetade med faktorn och i de fallen gjordes ingen bedömning för aktören. Bedömnings-skalan introducerades för att kunna sammanställa arbetet med de fyra förmågorna för resiliens samt underlätta jämförelse av olika kritiska infrastrukturer. Skalan gör även undersökningen av arbetet med resiliens mindre konceptuellt vilket förväntas kunna öka den praktiska nyttan av ramverket genom att man lättare kan jämföra förmågor och se områden där arbetet med faktorerna kan utvecklas. Därmed används skalan inte för att bedöma nivån av resiliens för kritiska infrastrukturer, utan endast för att underlätta bedömningen av kritiska infrastrukturers arbete med förmågorna för resiliens. För varje aktör sammanställdes kodningen och bedömningarna. Aktörernas arbete med faktorerna färgkodades sedan i tabeller för att underlätta jämförelser mellan kritiska infrastrukturer. Som en del av analysen skickades sammanställningarna av det insamlade materialet till respektive aktör för granskning. Återkopplingen från aktörerna gjorde att eventuella missförstånd kunde redas ut och det gav även aktörerna en möjlighet att förtydliga eller addera information.

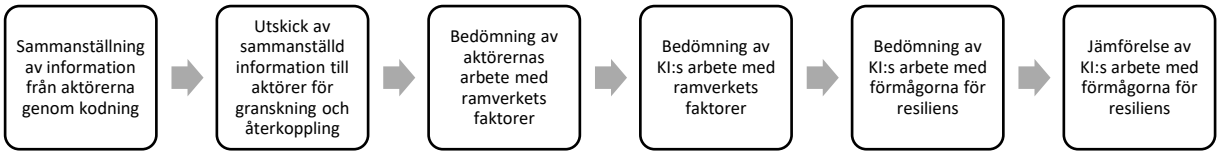
Efter att aktörernas arbeten med förmågorna för resiliens analyserats sammanvägdes samtliga aktörers arbeten inom respektive kritisk infrastruktur. Genom att sammanväga aktörernas arbete med faktorerna kunde hela den kritiska infrastrukturens arbete med faktorerna bedömas (i högre grad, i lägre grad, inte alls eller ingen bedömning). Bedömningen utgick ifrån hur aktörernas arbete ansågs bidra till den kritiska infrastrukturens arbete med respektive faktor. Baserat på de kritiska infrastrukturernas arbete med ramverkets faktorer gjordes sedan en kvalitativ bedömning av hur och till vilken grad de kritiska infrastrukturerna arbetar med respektive förmåga för resiliens. Bedömningarna utgick från de parametrar som listas nedan. Analysens bedömningar av arbetet med förmågorna jämfördes sedan med de bedömningar som aktörerna själva gjort i enkäten om deras arbete med respektive förmåga. Bedömningen av till vilken grad

de kritiska infrastrukturerna arbetar med förmågorna för resiliens utgick från:

- Huruvida en kritisk infrastruktur fokuserar på både organisatoriska och tekniska faktorer. Detta användes för att bedöma ifall en kritisk infrastruktur arbetade mer tekniskt eller organisatoriskt.
- Antal faktorer för respektive förmåga som en kritisk infrastruktur arbetade med i högre/lägre grad. Detta användes för att bedöma till vilken grad en kritisk infrastruktur arbetade med respektive förmåga.
- Ifall någon typ av metod eller system kan bedömas som omfattade eller generellt använd inom en kritisk infrastruktur. Detta förekom då antingen flertal aktörer arbetade med en metod eller ett system, eller då arbetet ansågs vara viktigt för en kritisk infrastrukturs arbete med en viss förmåga.

3.3.1 Metod för jämförelse av de kritiska infrastrukturerna

Efter att alla kritiska infrastrukturers arbete med förmågorna för resiliens fastställts jämfördes de kritiska infrastrukturerna med varandra. Jämförelsen utgick från hur väl de kritiska infrastrukturerna bedömdes arbeta med förmågorna för resiliens och vilka förmågor de fokuserar på. En sammanfattning av analysen av det insamlade materialet presenteras i Figur 8 nedan. För vissa av de undersökta kritiska infrastrukturer finns avbrottsdata som sammanställts i ett tidigare examensarbete av Axelsdóttir och Bjärenstam Jonason (2018). Initialt i arbetet var därmed även tanken att de kritiska infrastrukturernas arbete med resiliens skulle jämföras med avbrottsdata. Detta för att se om det finns en relation mellan aktörernas arbete med resiliens och kvantitativa empiriska beskrivningar av resiliensnivån för de kritiska infrastrukturerna. På grund av tidsbrist har detta dock inte kunnat genomföras.

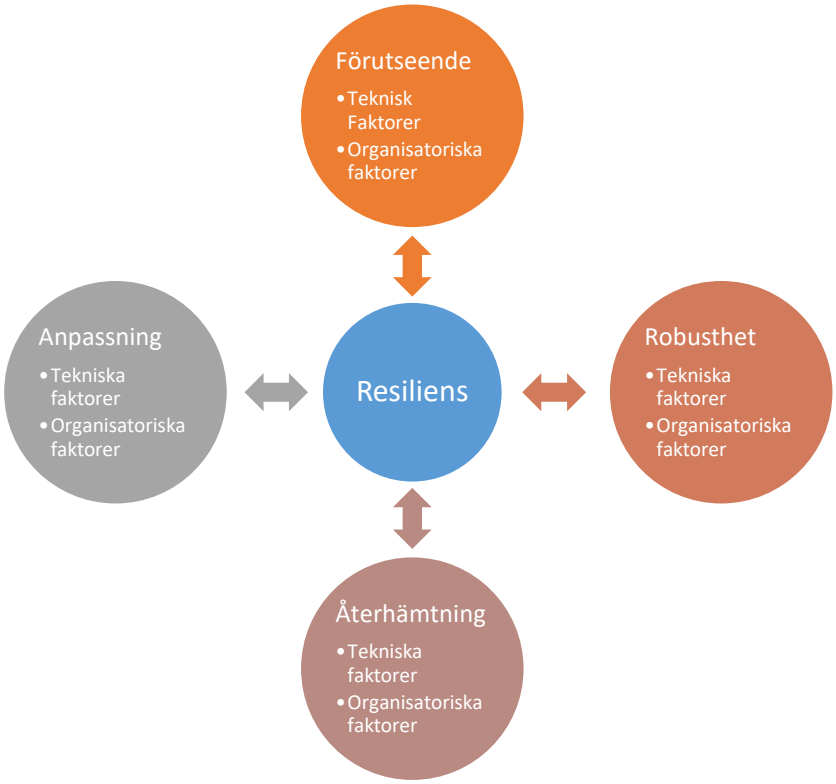


Figur 8. Arbetsprocess för analys av information från aktörerna och jämförelse. KI är en förkortning för kritiska infrastruktur.

4 Ramverk

I detta kapitel diskuteras i mer detalj hur de fyra förmågorna för resiliens, förutseende, robusthet, återhämtning och anpassning, beskrivs i olika publikationer. Baserat på beskrivningarna identifieras och sammanställs faktorer som beskriver hur kritiska infrastrukturer kan arbeta med konceptet resiliens. Beskrivning och argumentation för faktorernas bidrag till förmågorna för resiliens ges i kapitel 4.1–4.4. Sammanställningen av de bidragande faktorerna presenteras i tabellform i kapitel 4.5.

Kritiska infrastrukturer, så som Telekommunikation, Elförsörjning och Räddningstjänst, anses innefatta både mänskliga och tekniska komponenter som interagerar och samspelar för att upprätthålla infrastrukturens funktion. Detta i enlighet med ett socio-tekniskt perspektiv där en organisation utgörs av en teknisk och en social del (Fox, 1995). För att undersöka resiliens inom en kritisk infrastruktur bör därför både den organisatoriska och tekniska delen av infrastrukturen beaktas. Francis och Bekera (2014) beskriver chefernas engagemang samt kulturen hos personalen inom den kritiska infrastrukturen som exempel på organisatoriska delar, där kultur inom kritisk infrastruktur syftar på inställningen till inlärning, riskmedvetenhet, flexibilitet, etcetera. Tekniska delar är, enligt Fox (1995), de delar av systemet som omfattar bland annat material, maskiner och fysiska processer. De faktorer som identifieras för de fyra förmågorna för resiliens kommer följaktligen även delas in i organisatoriska och tekniska faktorer. Organisatoriska faktorer kommer innefatta faktorer som främst beror på de sociala relationerna inom den kritiska infrastrukturen, medan tekniska faktorer kommer innefatta faktorer av teknisk eller fysisk karaktär. Denna indelning syftar främst till att skapa ytterligare förståelse för hur de kritiska infrastrukturerna arbetar. Det görs ingen koppling mellan fördelningen mellan organisatoriskt och tekniskt arbete och ifall en kritisk infrastruktur är mer eller mindre resilient.



Figur 9. Konceptet resiliens och dess förmågor.

4.1 Förutseende

För att veta hur den kritiska infrastrukturen ska arbeta med resiliens behöver infrastrukturen definiera vad som är kritiskt i deras verksamhet (NIAC, 2010), vilket är ett organisatoriskt sätt att arbeta med resiliens. En kritisk infrastruktur behöver därmed sätta upp mål för sin verksamhet avseende sin funktion. Målen kan innebära att den kritiska infrastrukturens funktion inte får stoppas eller att tiden för avbrott i funktion ska minska (NIAC, 2010). När den kritiska infrastrukturen vet vad som är deras kritiska nivå kan infrastrukturen analysera vad som kan påverka den kritiska infrastrukturen negativt (NIAC, 2010). För att kunna analysera och detektera hur den kritiska infrastrukturen skulle påverkas av en eventuell händelse behövs någon form av informationsinsamling.

För att vara förutseende krävs det även att kritiska infrastrukturer kan detektera indikationer på avvikelser. Park et al. (2013) menar att förmågan att detektera indikationer på avvikelser i verksamheten och tidiga varningstecken är viktigt för en kritisk infrastrukturs resiliens. För att kunna detektera händelser som det finns stor osäkerhet kring eller som är svåra att uppfatta behöver kritiska infrastrukturer system för informationsinsamling, dessa system kan vara antingen organisatoriska eller tekniska. Systemen bör kontinuerligt förse kritiska infrastrukturer med information som möjliggör uppmärksammande av otydliga signaler och indikationer. En strategi som kan användas för att samla in information är användandet av rapporteringssystem. Rapporteringssystem samlar in information från personal om tidigare händelser (Akselsson, 2014). Ett tekniskt verktyg som kan användas för att samla in information är SCADA-system (Novotek Group, 2020). För identifiering av oönskade händelser behöver kritiska infrastrukturer organisatoriska eller tekniska strategier för att bearbeta den insamlade informationen (Rød & Johansson, 2020). Informationen kan användas för att implementera förebyggande åtgärder (Akselsson, 2014), vilket anses stärka övriga förmågor.

I både MSBs handlingsplan från 2013 och en DHS rapport från 2013 beskrivs förutseende, tillsammans med anpassningsförmåga, som en del av förebyggande åtgärder. Förebyggande åtgärder innebär att kunna identifiera risker och sårbarheter hos kritiska infrastrukturer för att sedan kunna använda informationen till att implementera åtgärder (MSB, 2013; DHS, 2013). Förebyggande åtgärder används för att förbereda kritiska infrastrukturer och öka förmågan för robusthet och återhämtningen vid en eventuell störning. Den del av de förbyggande åtgärderna som tillskrivs förmågan för förutseende består av detektion och analys av oönskade händelser, medan själva implementeringen av förebyggande åtgärder tillskrivs förmågan för anpassning.

Något som kan påverka förmågan förutseende är arbetskulturen inom kritiska infrastrukturer. För att medarbetare ska rapportera in händelser och olyckor behöver verksamheten uppmuntra rapportering. En säkerhetskultur som bejakar rapportering anses därför förstärka kritiska infrastrukturers informationsinsamling och därmed även deras förutseende förmåga (Akselsson, 2014).

4.2 Robusthet

Övningar inför framtida händelser är centralt för förmågan att hantera och motstå störningar (MSB, 2013a; Francis & Bekera, 2014). MSB (2013a) lyfter fram övningar som ett sätt att förbättra en verksamhets förmåga att motstå störningar. MSB (2013a) menar att övningarna kan lyfta fram de organisatoriska metoder som förbättrar organisationens förmåga till hantering av störningar. Även NIAC (2010) skriver att övning, planering och förebyggande åtgärder ökar en organisations robusthet. Övning och planering innebär att organisationen har strategier för hur en störning ska hanteras och övar på dessa för att minska konsekvenserna av störningen (NIAC, 2010). Övningar är något som kan kopplas till både robusthet och återhämtning och är därför en faktor som kan bidra till båda dessa förmågor. Övningar kopplat till robusthet, som till exempel utrymningsövningar, bidrar till att minska konsekvenserna under en störning och inte till återhämtning. Övningar kopplade till återhämtning behandlas i kapitel 4.3 Återhämtning. Ett samarbete mellan samhällsaktörer förbättrar den organisatorisk förmågan att hantera större störningar (MSB, 2018a). Ett etablerat samarbete mellan olika samhällsaktörer bidrar till ökad erfarenhet och förståelse för hur okända situationer ska hanteras. Eftersom det tar tid att etablera ett samarbete till andra aktörer behövs detta göras innan en störning inträffar (MSB, 2018a). En teknisk faktor på en åtgärd att öka kritiska infrastrukturers robusthet är att skapa en buffert i systemet. En buffert bidrar med kapacitet i systemet för att bibehålla funktionen, även om vissa delar har påverkats negativt av en händelse (Francis & Bekera, 2014; Becker, 2014). En annan teknisk faktor som ökar robusthet är att öka redundansen i kritiska infrastrukturer (NIAC, 2010). Konsekvenserna av en störning lindras om en kritisk infrastruktur har redundanta system (OECD, 2019). På det sättet kan funktionen upprätthållas även om ett del-system fallerar på grund av en störning. Skillnaden mellan buffert och redundans bedöms vara att buffert är att ha ett överskott av något som man är beroende av från externa aktörer. Redundans bedöms vara något som finns i den egna kritiska infrastrukturen för att minska påverkan av fel i system. Exempelvis kan buffert vara lager av drivmedel medan redundans kan vara att ha oberoende ledningar.

4.3 Återhämtning

Krishantering kräver resurser och vid en störning ska en kritisk infrastruktur därför kunna bedöma sitt behov och koordinera sina krishanteringsresurser därefter (MSB, 2018a). En god resurshantering med möjlighet att tillhandahålla organisatoriska och tekniska resurser vid behov är en förutsättning för en kritisk infrastrukturs återhämtningsförmåga (OECD, 2019; NIAC, 2010). Organisatoriska resurser kan exempelvis vara tillgång på kompetent personal, medan tekniska resurser kan vara utrustning och material. En fungerande resurshantering vid kriser kräver ledning för att tillgängliggöra både organisatoriska och tekniska resurser och säkerställa att dessa dirigeras efter behov samt koordination för att säkerställa att resurserna inte hämmar varandra utan används så effektivt som möjligt (Bergström, Uhr, & Frykmer, 2016; MSB, 2018a). Samarbete mellan intressenter har en positiv effekt på återhämtningsförmågan (DHS, 2013) medan misstro och oenighet kring resursfördelning vid störningar kan ha en negativ påverkan på återhämtningsförmågan (Francis & Bekera, 2014). En organisatorisk faktor som kan förbättra den långsiktiga återhämtningsförmågan hos en kritisk infrastruktur anses därför vara att etablera samarbete och förtroende mellan kritiska infrastrukturer och andra aktörer i samhället, så som ideella organisationer och statliga representanter.

Även utformade strategier med fokus på vad man ska göra efter att en störning inträffat förbättrar en kritisk infrastrukturs återhämtningsförmåga. Ett exempel på en sådan strategi är att ha en etablerad kontinuitetshantering (MSB, 2020b). Kontinuitetsplaner fungerar som vägledning för att återhämta en verksamhet efter en störning och omfattar bland annat olika rutiner för hur man återställer verksamheten efter en störning, hur man återgår till ordinarie arbetssätt och ansvarsfördelning (MSB, 2020a). I sin rapport från 2010 beskriver NIAC övningar som ett verktyg för att effektivisera återhämtningen vid störningar inom elsektorn, men menar att rapportens resultat är applicerbara på andra kritiska infrastrukturer (NIAC, 2010). I denna rapport skiljer sig övningar för återhämtning från övningar för robusthet. För återhämtning avses övningar som hjälper den kritiska infrastrukturen återbygga sin funktion efter att störningen har inträffat. Exempelvis kan gemensamma övningar genomföras där kontinuitetsplaner testas för att bygga förtroende mellan aktörer (Boin & McConnell, 2007).

4.4 Anpassning

I sin handlingsplan från (2013a) menar MSB att utveckling inom kritisk infrastruktur kräver att verksamheten har kapacitet att dra lärdomar från erfarenheter av tidigare händelser. För att kunna dra lärdomar behöver insamlad information och rapporteringar följas upp och utvärderas, genom både organisatoriska och tekniska system. Uppföljning och utvärdering efter störningar i lärande syfte som en del av verksamhetens anpassningsarbete förespråkas även i rapporter av NIAC (2010) och DHS (2013). Lärande av rapportering och uppföljning kan användas som underlag för beslut kring åtgärder inom kritiska infrastrukturer (Akselsson, 2014). Att en kritisk infrastruktur implementerar proaktiva åtgärder, både organisatoriska (exempelvis modifiering av procedurer och revidering av planer) och tekniska (exempelvis införande av ny teknologi och verktyg), för att bättre möta framtida störningar är en viktig del av anpassningsförmågan (OECD, 2019). Att ha ett utbyte av erfarenheter och lärdomar från tidigare störningar mellan aktörer inom kritisk infrastruktur är en organisatorisk faktor som kan bidra till att förebyggande åtgärder implementeras, vilket förbättrar anpassningsförmågan (MSB, 2013b; NIAC, 2010; DHS, 2013).

Något som bedöms kunna påverka anpassningsförmågan är den säkerhetskultur som finns i verksamheten. Säkerhetskulturen kan till exempel påverka hur väl informationen från rapporteringssystem implementeras, och därmed hur verksamheten anpassas. Säkerhetskulturen även kan påverka hur villig personalen är att anpassas till nya förändringar (Akselsson, 2014).

4.5 Sammanställning av ramverket för datainsamling och analys

I Tabell 2 presenteras de fyra förmågorna för resiliens och de organisatoriska och tekniska faktorerna för respektive förmåga som identifierats genom arbetet. Tabellen är en sammanfattning av resultaten från ovan för respektive förmåga samt utifrån den genomförda datainsamlingen och analysen. För både förmågan för förutseende och förmågan för anpassning har säkerhetskultur identifierats som en påverkande faktor. Säkerhetskultur är en del av organisationskulturen (Akselsson, 2014). Kultur inom en organisation anses vara en ingående egenskap och indikationer på hur säkerhetskulturen ser ut kan detekteras från alla arbetsmoment som organisationen genomför. Säkerhetskultur anses därför inte utgöra en egen faktor utan snarare kan ses som en delmängd i merparten av faktorerna som berör förmågorna för resiliens.

Tabell 2 utgör, tillsammans med resultaten ovan, arbetets ramverk för datainsamling och analys. Hur olika kritiska infrastrukturer arbetar med resiliens kan genom detta ramverk därmed bedömas och jämföras kvalitativt.

Tabell 2. Ramverkets faktorer som bidrar till ökad resiliens.

	Förutseende	**Litteratur**
Organisatoriska faktorer	• Den kritiska infrastrukturen har tydliga mål på vad som ska skyddas.	(NIAC, 2010)
	• Den kritiska infrastrukturen förses kontinuerligt med information genom organisatoriska system för informationsinsamling, exempelvis möten med andra aktörer.	(Park, et al., 2013; Axelsson,2014)
	• Den kritiska infrastrukturen har organisatoriska system för att analysera information.	(Rød & Johansson, 2020)
	• Den kritiska infrastrukturen har förmåga att uppmärksamma otydliga signaler och indikationer.	(Park et al.,2013)
Tekniska faktorer	• Den kritiska infrastrukturen förses kontinuerligt med information genom tekniska system för informationsinsamling, exempelvis SCADA-system.	(Park, et al., 2013; Axelsson,2014)
	• Den kritiska infrastrukturen har tekniska system för att analysera insamlad information.	(Rød & Johansson, 2020)
	Robusthet	
Organisatoriska faktorer	• Den kritiska infrastrukturen genomför övningar inför oönskade händelser.	(MSB, 2013a; NIAC, 2010)
	• Den kritiska infrastrukturen planerar inför oönskade händelser. Exempelvis strategier under störningen.	(NIAC, 2010)
	• Den kritiska infrastrukturen har ett samarbete med andra samhällsaktörer.	(MSB, 2018a)
Tekniska faktorer	• Det finns en buffert i den kritiska infrastrukturens kapacitet, exempelvis att ha barriärer eller extra lagerkapacitet.	(Francis & Bekera, 2014; Becker, 2014)
	• Det finns redundanta system eller en inbyggd redundans i systemen.	(NIAC, 2010; OECD, 2019)

Återhämtning		
Organisatoriska faktorer	• Det finns tillgång till organisatoriska resurser, exempelvis extra personal.	(NIAC, 2010; OECD, 2019)
	• Den kritiska infrastrukturen har en plan för ledning och koordination för resurshantering.	(MSB, 2018a; Bergström, Uhr, & Frykmer, 2016)
	• Den kritiska infrastrukturen har ett samarbete och förtroende med andra samhällsaktörer.	(DHS, 2013; Francis & Bekera, 2014)
	• Den kritiska infrastrukturen genomför övningar med fokus på återhämtning.	(NIAC, 2010)
	• Den kritiska infrastrukturen har utformade strategier med fokus på återhämtning, exempelvis kontinuitetsplaner.	(MSB, 2020b; MSB, 2020a)
Tekniska faktorer	• Det finns tillgång till tekniska resurser, exempelvis material eller tekniska system.	(NIAC, 2010; OECD, 2019)
Anpassning		
Organisatoriska faktorer	• Uppföljning och utvärdering görs kontinuerligt i lärande syfte med hjälp av organisatoriska system	(MSB, 2013a; NIAC, 2010; DHS, 2013; Akselsson, 2014)
	• Den kritiska infrastrukturen implementerar organisatoriska förebyggande/proaktiva åtgärder, exempelvis modifiering av planer och procedurer.	(OECD, 2019)
	• Det sker erfarenhetsutbyte mellan den kritiska infrastrukturen och andra aktörer.	(MSB, 2013b; NIAC, 2010; DHS, 2013)
Tekniska faktorer	• Uppföljning och utvärdering görs kontinuerligt i lärande syfte med hjälp av tekniska system.	(MSB, 2013a; NIAC, 2010; DHS, 2013; Akselsson, 2014)
	• Den kritiska infrastrukturen implementerar tekniska förebyggande/proaktiva åtgärder, exempelvis redundanshöjande åtgärder och införande av ny teknologi.	(OECD, 2019)

5 Kritiska infrastrukturers arbete med förmågor för resiliens

I detta kapitel ges en överblick av den information som samlats in från enkäter, intervjuer, uppföljningsmejl och dokumentsökning. Alla aktörer har inte velat medverka med namn på sin organisation. Av sekretesskäl har aktörerna därför benämnts som Aktör A - Aktör I. Samtliga aktörer som kontaktades har både svarat på enkäten och medverkat på en intervju. I Appendix C–Appendix E presenteras mer detaljerad information om hur varje aktör arbetar. Informationen i Appendix C–Appendix E utgör underlaget till bedömningarna kring hur aktörerna arbetar med förmågorna för resiliens, men på grund av rapportens ordbegränsningar har informationen lagts i Appendix. De kritiska infrastrukturerna och sektorerna som aktörerna är en del av anges i Tabell 3 nedan. Aktör B medverkade i enkät och intervju men valde senare att avbryta medverkan i examensarbetet och har därför exkluderats från analysen. Även en aktör inom Järnvägstransport medverkade i enkät och under intervju (Aktör I). På grund av tidsbrist och att det endast var en aktör som medverkade för Järnvägstransport har den insamlade informationen för den kritiska infrastrukturen inte analyserats.

Tabell 3. Översikt av medverkande aktörer, kritiska infrastrukturer och samhällssektorer.

Aktörer	**Kritisk Infrastruktur**	**Samhällssektor**	**Inkluderad i analys**
Aktör A	Räddningstjänst	Skydd & säkerhet	Ja
Aktör B	Räddningstjänst	Skydd & säkerhet	Nej
Aktör C	Räddningstjänst	Skydd & säkerhet	Ja
Aktör D	Elförsörjning	Energiförsörjning	Ja
Aktör E	Elförsörjning	Energiförsörjning	Ja
Aktör F	Elförsörjning	Energiförsörjning	Ja
Aktör G	Telekommunikation	Information & kommunikation	Ja
Aktör H	Telekommunikation	Information & kommunikation	Ja
Aktör I	Järnvägstransport	Transport	Nej

För varje kritisk infrastruktur presenteras först hur den kritiska infrastrukturen arbetar med ramverkets faktorer inom respektive förmåga för resiliens. För att tydliggöra vilken faktor som avses i punktlistorna har faktorerna skrivits ut kursivt. En visuell sammanfattning av hur de tre kritiska infrastrukturerna bedöms arbeta med ramverkets faktorer återfinns i Tabell 5, Tabell 6 och Tabell 7. Bedömningarna för arbetet med ramverkets faktorer har färgkodas enligt Tabell 4. För varje kritisk infrastruktur görs sedan bedömning av arbetet med de fyra förmågorna för resiliens (förutseende, robusthet, återhämtning, anpassning).

Tabell 4. Färgkodning för arbete med ramverkets faktorer.

	Arbetar med faktorn i högre grad.
	Arbetar med faktorn i lägre grad.
	Arbetar inte med faktorn.
	För lite information tillgänglig för att göra en bedömning.

5.1 Räddningstjänst

I 1 Kap. 2§ första stycket Lag (2003:778) om skydd mot olyckor står det att ”*Med räddningstjänst avses i lagen de räddningsinsatser som staten eller kommunerna skall ansvara för vid olyckor och överhängande fara för olyckor för att hindra och begränsa skador på människor, egendom eller miljön*”. Den kritiska infrastrukturen Räddningstjänst bedöms ha som funktion att vid olyckor och överhängande fara för olyckor hindra och begränsa skador på människor, egendom eller miljön.

Inom Räddningstjänst finns det olika typer av aktörer. Dessa inkluderar räddningstjänstförbund men även kommuner och myndigheter. För Räddningstjänst undersöktes tre olika aktörer, Aktör A, Aktör B och Aktör C. Aktör B valde efter undersökningen att avbryta sin medverkan och därför har Aktör B exkluderats från analysen. Anledningen till att Aktör B avbröt sin medverkan framgick inte helt. Försök till återkoppling med Aktör B har gjorts utan framgång. Aktör A och Aktör C är räddningstjänstförbund som är verksamma i olika delar av Sverige. Representanterna från aktörerna hade dessutom olika fokusområden. Aktörerna har antingen 1) fokus på den operativa delen av verksamheten eller 2) fokus på både den operativa och förebyggande delen av verksamheten. Störningar inom Räddningstjänst innefattar dels störningar inom aktörernas egna verksamheter, dels händelser som kan påverka hur väl den kritiska infrastrukturen Räddningstjänst levererar sin funktion. Aktiviteter rörande insatsförmåga bidrar därmed till att kunna upprätthålla funktionen. Nedan presenteras hur den kritiska infrastrukturen arbetar med ramverkets faktorer samt förmågorna för resiliens baserat på insamlad information från Aktör A och Aktör C. I detta kapitel presenteras enbart översiktligt hur aktörerna arbetar utifrån ramverkets faktorer. För mer detaljer kring insamlat material och sammanställningen av materialet hänvisas läsaren till Appendix C där aktörernas arbete och kopplingen till ramverkets faktorer presenteras mer ingående.

5.1.1 Räddningstjänsts arbete med ramverkets faktorer

Förutseende

Organisatoriska faktorer

- Sammanställningen visade att aktörerna inom Räddningstjänst har det övergripande målet att skydda samhället mot olyckor. Aktör C nämnde specifikt att de arbetar utifrån Lag (2003:778) om skydd mot olyckor, medan Aktör A beskrev att deras mål var att skydda samhället från olyckor. Aktörerna anses ha tydliga mål som de följer upp genom antingen nyckeltal eller genom utvärdering av sina aktiviteter. Den kritiska infrastrukturen bedöms arbeta med *tydliga mål* på vad som ska skyddas i högre grad.
- Sammanställningen visade att de organisatoriska metoderna för informationsinsamling inom Räddningstjänst främst sker via möten och forum. Aktörerna samlade in information med organisatoriska metoder från ett flertal andra aktörer, både internt inom den kritiska infrastrukturen och externt. Arbetet med *organisatoriska system för informationsinsamling* bedöms förekomma i högre grad inom den kritiska infrastrukturen.
- Sammanställningen visade att aktörerna arbetar med expertbedömningar som organisatorisk metod för att analysera information. För båda aktörerna framkom någon form av metod för hur expertbedömningarna går till. Aktör A diskuterar scenarier och Aktör C beskrev en framtagen metod för systematisk analysering. Arbetet med *organisatoriska system för analys* inom Räddningstjänst bedöms förekomma i högre grad.

- Sammanställningen av det insamlade materialet visar inte till vilken grad aktörer inom Räddningstjänst arbetar med att *uppmärksamma otydliga signaler och indikationer* som kan leda till störningar inom verksamheten eller påverkan på leveransen av funktionen. Däremot framkom det att finns en tendens hos aktörerna att fokusera sitt arbete på tidigare kända händelser i större utsträckning än framtida okända händelser. Det kan inte göras en bedömning om den kritiska infrastrukturens arbete med denna faktor.

Tekniska faktorer

- Sammanställningen visade att aktörerna använder sig av större tekniska system som finns inom den kritiska infrastrukturen, så som WIS, där flera aktörer medverkar för att dela och samla in information. Andra tekniska system som används inom Räddningstjänst är händelserapportering som ger information om den interna verksamheten. Arbetet med *organisatoriska system för informationsinsamling* bedöms förekomma i högre grad inom den kritiska infrastrukturen, eftersom systemen som används inom Räddningstjänst samlar in information både internt och externt.
- Sammanställningen påvisade ett varierande arbete med tekniska system för analys. För Aktör A framkom det att det finns ett tekniskt system för analys av information medan det för Aktör C inte fanns tillräckligt med information för att göra en bedömning. Variationen gör att det inte går att göra en bedömning för hur den kritisk infrastrukturen generellt arbetar med *tekniska system för analys.*

Robusthet

Organisatoriska faktorer

- Sammanställningen visade att aktörerna övade på sin operativa förmåga för att förbättra insatser och därmed funktionen. Båda aktörerna medverkar i någon form av samverkansövning. Aktör C berättade att de övar på det vardagliga arbetet men inte större övningar. Generellt i den kritiska infrastrukturen bedöms arbetet med *övningar kopplat till robusthet* ske i lägre grad.
- Sammanställningen visade att aktörerna inom den kritiska infrastrukturen har planer för oväntade händelser. Däremot fokuserar aktörerna på olika saker i sina planer för oväntade händelser. Det som kunde påvisas som någorlunda genomgående var att aktörerna har planer som berör personalen. Generellt inom Räddningstjänst visar samanställningen att det inte finns etablerade planer inom den kritiska för att hantera större oväntade händelser, eftersom detta enbart framkom hos ena aktören. Den kritiska infrastrukturen bedöms arbeta med *planer inför oväntade händelser* i lägre grad.
- Sammanställningen visade att aktörerna har ett stort samarbete med andra aktörer inom den kritiska infrastrukturen. Det framkom att aktörer inom den kritiska infrastrukturen kan bistå varandra med både utrustning och personal som behövs för att upprätthålla den kritiska infrastrukturens funktion. Den kritiska infrastrukturen bedöms arbeta med *samarbete till andra aktörer kopplat till robusthet* i högre grad.

Tekniska faktorer

- Sammanställningen visade att flera aktörer inom den kritiska infrastrukturen arbetar med bufferts för bland annat telekommunikation och el. Därför bedöms den kritiska infrastrukturen Räddningstjänst arbeta med *bufferts* i högre grad.

- Från sammanställningen framkom det endast redundans för Aktör A. För Aktör C finns det en kunskapslucka för denna faktor. Eftersom det enbart framkom få redundanta system bedöms Räddningstjänst arbeta med *redundanta system eller redundans i system* i lägre grad.

Återhämtning

Organisatoriska faktorer

- Sammanställningen visade att de organisatoriska resurser som finns inom den kritiska infrastrukturen varierar mellan aktörerna. Generellt bygger de organisatoriska resurserna på tillgång till personal. Eftersom det enbart framkom ett fåtal organisatoriska resurser för aktörerna bedöms den kritiska infrastrukturen arbeta med *organisatoriska resurser* i lägre grad.
- Det insamlade materialet visar att det finns vissa planer för ledning och koordination av resurshanteringen. De planer som framkom hade dels fokus på den interna resurshanteringen, dels på resurshanteringen mellan aktörer inom den kritiska infrastrukturen. Det verkar inte finnas genomgående, tydliga *planer för ledning och koordination av resurshantering* inom den kritiska infrastrukturen och därför bedöms Räddningstjänst endast arbeta med faktorn i lägre grad. Det är värt att anmärka att en ny paragraf i Lag (2003:778) om skydd mot olyckor kommer träda i kraft i januari 2021. Paragrafen ger MSB möjlighet att fördela tillgängliga resurser om det uppstår konkurrens om resurser vid omfattande kommunala räddningsinsatser. Eftersom detta träder i kraft efter rapportens genomförande så har detta inte tagits i beaktning vid bedömning av faktorn.
- Sammanställningen visar att det finns samverkansavtal mellan aktörer inom Räddningstjänst. Samverkansavtalen medför att aktörer hjälps åt med både tekniska och organisatoriska resurser för att återupprätta sina insatsmöjligheter både under och efter en händelse, vilket bidrar till att den kritiska infrastrukturen kan leverera sin funktion. Den kritiska infrastrukturen bedöms arbeta med *samarbete och förtroende med andra samhällsaktörer* i högre grad.
- Sammanställningen visade att aktörerna inom Räddningstjänst bedriver kontinuerligt arbete med övning för att förbättra den operativa verksamheten. Båda aktörerna arbetar även med samverkansövningar tillsammans med aktörer både inom och utanför den kritiska infrastrukturen. Hur övningarna genomförs varierar mellan aktörerna. Samverkansövningarna antas, efter aktörernas beskrivningar, generellt förekomma någon gång om året. Aktör C berättade dock att de inte anser att samverkansövningarna bidrar till deras egen återhämtning. Aktör A genomför dock övningar som bidrar till deras egen återhämtning (momentövningar). Eftersom det sker övningar som både berör aktörers återhämtning och den kritiska infrastrukturen återhämtning bedöms Räddningstjänst generellt arbeta med *övningar kopplat till återhämtning* i högre grad.
- Från sammanställningen framkom det inga tydliga planer eller strategier för återhämtning inom den kritiska infrastrukturen. Aktör C uppvisade ett större arbete med tydligare planer och strategier för hur funktionen ska upprätthållas. Däremot har Aktör A kontinuitetsplaner som de själva anser inte är så utvecklade. Eftersom endast Aktör C uppvisade ett arbete med faktor i högre grad kan detta inte anses generellt för den kritiska infrastrukturen. Utifrån aktörernas arbete bedöms Räddningstjänst därför arbeta med *planer och strategier för återhämtning* i lägre grad.

Tekniska faktorer

- Aktörerna som ingick i undersökningen bedriver operativt arbete. Tekniska resurser har en viktig roll i det operativa arbetet. Sammanställningen visar att båda aktörer har god tillgång till fordon och utrustning och den kritiska infrastrukturen bedöms arbeta med *tekniska resurser för återhämtning* i högre grad.

Anpassning

Organisatoriska system

- Sammanställningen visade att aktörerna arbetar med att följa upp och utvärdera insatser på olika sätt. Generellt för den kritisk infrastrukturen är att aktörerna har rapporteringssystem där insatser utvärderas i lärande syfte. Det framkom även att det sker utvärderingar som berör hela den kritiska infrastrukturen så som uppföljning av skogsbränderna 2018. Samtliga aktörer berättade att det även sker en uppföljning av implementerade åtgärder inom de egna verksamheterna. Den kritiska infrastrukturen bedöms arbeta med *uppföljning och utvärdering i lärande syfte* i högre grad.
- Från sammanställningen framkom det att aktörerna kontinuerligt implementerar organisatoriska åtgärder. En åtgärd som både Aktör A och Aktör C implementerar är att genomföra förändringar i rutiner. I övrigt implementerade aktörerna olika typer av organisatoriska åtgärder, och båda aktörerna gav flera exempel på sådana åtgärder (se Appendix C för mer ingående information). Aktör A anser att räddningstjänsten generellt är konservativ och svår att förändra, men eftersom detta inte stöds av information från Aktör C kan detta inte göras generellt för hela Räddningstjänsts arbete. Baserat på att båda aktörerna implementerar olika typer av organisatoriska åtgärder bedöms den kritiska infrastrukturen arbeta med *implementering av organisatoriska åtgärder* i högre grad.
- Sammanställningen visade att det inom Räddningstjänst sker erfarenhetsutbyte genom diskussioner. Diskussionerna inom erfarenhetsutbyte bygger på information från både organisatoriska och tekniska system så som möten och databaser från MSB. Även den digitala plattformen WIS anses bidra till erfarenhetsutbytet inom Räddningstjänst. Erfarenhetsutbyte sker både mellan aktörer inom och utanför den kritiska infrastrukturen. I den kritiska infrastrukturen bedöms det ske ett arbete med *erfarenhetsutbyte i lärande syfte* i högre grad.

Tekniska faktorer

- Från sammanställningen framkom det att aktörerna rapporterar in och utvärderar insatser de varit på genom tekniska system för att bättre kunna leverera sin funktion. Rapporteringssystem som används inom den kritiska infrastrukturen samlar in information och sammanställer denna genom exempelvis statistik. Insatsstatistik för Räddningstjänst finns att se på IDA (MSB, 2020e). Dock anses tekniska system för uppföljning och utvärdering inte användas inom Räddningstjänst för exempelvis utvärdering av åtgärder. Den kritiska infrastrukturen bedöms därför arbeta med *tekniska system för uppföljning och utvärdering* i lägre grad.
- Från sammanställningen framkom det att både Aktör A och Aktör C arbetar med implementering av tekniska åtgärder, exempelvis genom att ny utrustning köps in. Utrustning anses vara en viktig del av den kritiska infrastrukturens operativa verksamhet och därmed även för den kritiska infrastrukturens funktion. Den kritiska infrastrukturen bedöms därför arbeta med *tekniska åtgärder* i högre grad.

Sammanfattning av Räddningstjänst arbete med ramverkets faktorer

I Tabell 5 sammanfattas Räddningstjänsts arbete med ramverkets faktorer. Tabellen visar till vilken grad respektive aktör bedöms arbeta med faktorerna samt till vilken grad den kritiska infrastrukturen bedöms arbeta med faktorerna.

Tabell 5. Sammanfattning av Räddningstjänst arbete med ramverkets faktorer.

Förutseende			
Faktorer	Aktör A	Aktör C	Räddningstjänst
Har tydliga mål på vad som ska skyddas.			
Förses kontinuerligt med information genom organisatoriska system för informationsinsamling.			
Har organisatoriska system för att analysera information.			
Har förmåga att uppmärksamma otydliga signaler och indikationer.			
Förses kontinuerligt med information genom tekniska system för informationsinsamling.			
Har tekniska system för att analysera insamlad information.			
Robusthet			
Faktorer	Aktör A	Aktör C	Räddningstjänst
Genomför övningar inför oönskade händelser.			
Planerar inför oönskade händelser.			
Har ett samarbete med andra samhällsaktörer.			
Det finns en buffert i kapaciteten.			
Det finns redundanta system eller en inbyggd redundans i systemen.			
Återhämtning			
Faktorer	Aktör A	Aktör C	Räddningstjänst
Har tillgång till organisatoriska resurser.			
Har en plan för ledning och koordination för resurshantering.			
Har ett samarbete och förtroende med andra samhällsaktörer.			
Genomför övningar med fokus på återhämtning.			

Har utformade strategier med fokus på återhämtning.			
Har tillgång till tekniska resurser.			
Anpassning			
Faktorer	Aktör A	Aktör C	Räddningstjänst
Uppföljning och utvärdering görs kontinuerligt i lärande syfte med hjälp av organisatoriska system.			
Implementerar organisatoriska förebyggande/proaktiva åtgärder.			
Det sker erfarenhetsutbyte mellan den kritiska infrastrukturen och andra aktörer.			
Uppföljning och utvärdering görs kontinuerligt i lärande syfte med hjälp av tekniska system.			
Implementerar tekniska förebyggande/proaktiva åtgärder.			

5.1.2 Räddningstjänst arbete med förmågorna för resiliens

Förutseende

Det finns tydliga mål inom den kritiska infrastrukturen som aktörerna arbetar med för att upprätthålla funktionen inom Räddningstjänst. För att vara förutseende används både tekniska och organisatoriska system inom den kritiska infrastrukturen i högre grad. Det går inte att urskilja ifall den kritiska infrastrukturen arbetar mer med tekniska eller organisatoriska system för informationsinsamling. Det framkom dock att organisatoriska system används i högre grad än tekniska system för analys. Man kan alltså se skillnad i Räddningstjänst användning av organisatoriska och tekniska system på faktornivå. Dock kan man inte se en sådan skillnad på förmågenivå.

Sammanfattningsvis bedöms Räddningstjänst vara en kritisk infrastruktur som arbetar med förmåga för förutseende i relativ hög grad även om det finns vissa kunskapsluckor. Resultatet för den kritiska infrastrukturen överensstämmer relativt väl med aktörernas egna bedömningar för hur de arbetar med förutseende. Aktör A svarade i enkäten att de arbetar i lite lägre grad med förutseende (3/6) än vad som bedömdes i analysen. Under intervjun framkom det dock att Aktör A la sig lägre på skalan eftersom de tagit i beaktning att man alltid kan arbeta mer med förmågorna och att deras resurser är begränsade. Detta resonemang gjordes för alla Aktör A:s svar på enkätens skalfrågor. Aktör C svarade i enkäten relativt högt på skalfrågan om hur de arbetar med förmågan för förutseende (5/6).

Robusthet

Den kritiska infrastrukturen Räddningstjänst arbetar generellt med robusthet i lägre grad. Den delen av Räddningstjänsts arbete som främst bidrar till förmågan för robusthet är samarbetet med interna och externa aktörer. En annan del som bidrar till förmågan för robusthet är den

kritiska infrastrukturens arbete med bufferts. Aktörerna inom Räddningstjänst har uppvisat ett arbete med att minska beroende till andra kritiska infrastrukturer genom bufferts, exempelvis genom att införa reservkraftverk för att minska beroendet till elförsörjning. Det går inte att göra någon bedömning om huruvida den kritiska infrastrukturen mest arbetar organisatoriskt eller tekniskt med förmågan för robusthet.

Sammanfattningsvis bedöms Räddningstjänst vara en kritisk infrastruktur som arbetar med förmåga för robusthet i relativt låg grad eftersom endast två av faktorerna bidrog till robusthet i högre grad och resterande i lägre grad. Aktörernas egna bedömningar på deras arbete med förmågan för robusthet från enkäten varierade. Aktör A svarade att de arbetar i lite lägre grad med robusthet (3/6), dock med samma kommentar som för förutseende. Aktör C svarade relativt högt på skalfrågan (5/6). Den bedömning som gjorts för den kritiska infrastrukturen Räddningstjänst är att de arbetar mindre med förmågan för robusthet än vad aktörerna generellt själva anser att ge gör. Utifrån analysen bedöms robusthet vara den förmåga av de fyra förmågorna för resiliens som den kritiska infrastrukturen Räddningstjänst arbetar minst med.

Återhämtning

Räddningstjänst är en kritisk infrastruktur som i hög grad arbetar med den tekniska delen av återhämtning. Sammanställningen visade att det organisatoriska arbete som främst bidrar till förmågan för återhämtning är sådant arbete som aktörerna har interagerat i sin dagliga verksamhet. Exempelvis sker det inom Räddningstjänst ett kontinuerligt arbete med övningar kopplat till återhämtningsförmågan, och detta är en av de faktorer där Räddningstjänst uppvisar högst arbete. Däremot bedöms det att aktörer inom Räddningstjänst inte arbetar med de mer planerande momenten kopplade till återhämtning i form av resurshantering och strategier inför oönskade händelser i speciellt hög grad.

Sammanfattningsvis bedöms Räddningstjänst vara en kritisk infrastruktur som arbetar med förmågan för återhämtning i någorlunda hög grad men med vissa svagheter. Aktörernas egna bedömningar på deras arbete med förmågan för återhämtning från enkäten varierade. Aktör A svarade att de arbetar i lite lägre grad med återhämtning (3/6). Aktör C svarade högt på skalfrågan om hur de arbetar med återhämtning (6/6). Den bedömning som gjorts för Räddningstjänst är att arbetet med förmågan för återhämtning sker i lägre grad än vad Aktör C bedömer men är i linje med Aktör A:s bedömning.

Anpassning

Räddningstjänst är en kritisk infrastruktur som anses arbeta mycket med lärande genom organisatoriska system. Aktörer inom Räddningstjänst arbetar mycket med att följa upp och utvärdera tidigare händelser med organisatoriska system samt använda lärdomarna från detta för att implementera åtgärder. Däremot används tekniska system inte i lika hög grad som verktyg för uppföljning och utvärdering i lärande syfte inom den kritiska infrastrukturen. Erfarenhetsutbyte mellan aktörer bedöms bidra till lärandet och därmed även förmågan för anpassning inom Räddningstjänst i högre grad. Av sammanställningen framkom det att sociala kontaktnät generellt är det viktigaste verktyget inom den kritiska infrastrukturen för lärande. Aktörer uppvisar ett lärande både med hänsyn till sin egen operativa förmåga så väl som Räddningstjänst som kritiska infrastrukturs förmågor för resiliens. Sammanställningen visade att den kritiska infrastrukturen bedriver ett arbete med att implementera åtgärder baserat på det

lärande som sker. Organisatoriska och tekniska åtgärder implementeras i lika hög grad inom den kritiska infrastrukturen.

Sammanfattningsvis bedöms Räddningstjänst vara en kritisk infrastruktur som arbetar med förmågan för anpassning i högre grad. Aktörernas egna bedömningar på deras arbete med förmågan för anpassning från enkäten varierade. Aktör A svarade att de arbetar i lite lägre grad med anpassning (3/6) medan Aktör C svarade högt på skalfrågan (5/6). Den bedömning som gjorts för Räddningstjänst är att arbetet med förmågan för anpassning sker i högre grad än vad aktörerna själva bedömt sitt arbete med förmågan. Utifrån analysen bedöms anpassning vara den förmåga av de fyra förmågorna för resiliens som Räddningstjänst bedöms arbeta mest med.

5.2 Elförsörjning

För att samhället i Sverige ska fungera krävs försörjning av el till bostäder, näringsliv och offentlig service. Elförsörjning inkluderar både elproduktion och elnät för överföring av elektricitet till dessa slutkunder (SCB, 2020). Elproduktion är det som avser produktionen av elektricitet medan elnät avser infrastrukturen som möjliggör leveransen av el till samhället. I denna rapport har den kritiska infrastrukturen Elförsörjnings arbete med resiliens undersökt. Elförsörjningens funktion är alltså att leverera elektricitet till samhället.

Inom den kritiska infrastrukturen Elförsörjning har tre aktörer undersökts; Aktör D, Aktör E och Aktör F. Vid informationsinsamlingen framkom det att aktörerna kan arbeta med att antingen 1) övervaka den kritiska infrastrukturen för att skapa en fungerande marknad eller, 2) äga och driva elnät, eller en kombination av dessa två. Detta anses vara det som aktörerna bidrar med för att upprätthålla den kritiska infrastrukturens Elförsörjnings funktion. Nedan presenteras hur den kritiska infrastrukturen arbetar med ramverkets faktorer samt förmågorna för resiliens baserat på insamlad information från aktörerna. I detta kapitel presenteras enbart översiktligt hur aktörerna arbetar utifrån ramverkets faktorer. För mer detaljer kring insamlat material och sammanställningen av denna hänvisas läsaren till Appendix D där aktörernas arbete och kopplingen till ramverkets faktorer presenteras mer ingående.

5.2.1 Elförsörjnings arbete med ramverkets faktorer

Förutseende

Organisatoriska

- Inom den kritiska infrastrukturen har aktörerna mål på när den kritiska infrastrukturens funktion inte upprätthålls. Målen skiljer sig åt mellan aktörerna, men de mål som kan kopplas till den kritiska infrastrukturens funktion är att elförsörjningen inte ska ha ett uppehåll. Den el som levereras ska även ha en viss frekvens, spänningskvalitet och följa ett visst leveransmått. Målen mäts genom nyckeltal, kriterier och efterföljandet av lagar. Det bedöms därför finnas *tydliga mål* som den kritiska infrastrukturen arbetar med i högre grad.
- Från sammanställningen framkom det att flera aktörer arbetar med informationsinsamling genom både nationella och internationella kanaler där information delas och samlas in. Aktörerna uppvisade även ett arbete med att samla in information om elmarknaden. Den kritiska infrastrukturen bedöms arbeta med *organisatoriska system för informationsinsamling* i högre grad.

- Sammanställningen visade att analys av information inom Elförsörjning till stor del sker genom expertbedömningar. Fokuset hos aktörernas expertbedömningar varierar. De olika expertbedömningarna hos aktörerna fokuserar dels på elnätet, dels på omvärldens påverkan på elnätet så som väder, dels genom analys av statistik för att få fram tendenser. Aktörernas enskilda arbete med organisatoriskt analysarbete var fokuserat på en mindre del av den kritiska infrastrukturen och därför bedömdes aktörerna enskilt arbeta med faktorn i lägre grad. Dock anses kombinationen av system för analys som finns inom den kritiska infrastrukturen fokusera på flera delar och därför bedöms Elförsörjning som helhet arbeta med organisatoriska system för analys i högre grad.
- Sammanställningen visade att det inom den kritiska infrastrukturen Elförsörjning finns flera olika sätt att både samla in information och att analysera informationen. Olika parametrar så som information från SCADA-system, från driftrum och väderprognoser granskas genom både organisatoriska- och tekniska system. Kombinationen av system, som både kan hantera översiktlig information (exempelvis analys av statistik för att få fram tendenser) och specifika data (exempelvis SCADA-system), bedöms användas för att uppmärksamma olika typer av förändringar i systemet. Den kritiska infrastrukturen bedöms därför arbeta med att *uppmärksamma otydliga signaler och indikationer* i högre grad.

Tekniska Faktorer

- I sammanställningen framkom det att alla medverkande aktörer inom Elförsörjning samlar in information genom tekniska system. Informationsinsamlingen hos aktörerna sker på olika sätt och innefattar allt från större system som SCADA till digitala nätverksplattformar. Den kritiska infrastrukturen bedöms arbeta med *tekniska system för informationsinsamling* i högre grad.
- Inom den kritiska infrastrukturen finns SCADA- och GIS-system som kan analysera information kopplat till elnätdriften i högre grad. Eftersom nätdriften är en central del av upprätthållandet av Elförsörjnings funktion bedöms Elförsörjning arbeta med *tekniska system för analys* i högre grad.

Robusthet

Organisatoriska

- De övningar som framkom av sammanställningen hade ingen tydlig koppling till robusthet utan endast till återhämtning. Eftersom elavbrott generellt sker momentant förväntas inte övningar kunna bidra till att kunna motstå en sådan störning eller absorbera chocken av störningen. Det insamlade materialet anses dock inte vara tillräckligt för att göra en bedömning om huruvida aktörerna arbetar med *övningar kopplat till robusthet* och till vilken grad detta arbete görs.
- I sammanställningen framkom det att hela den kritiska infrastrukturen arbetar med N-1 kriteriet, vilket är en plan för att upprätthålla funktionen vid en störning som omfattar förlusten av den mest kritiska systemdelen. Det finns även planer kring känslig information inom den kritiska infrastrukturen så att informationen inte kommer ut vid en IT relaterad störning. Inom Elförsörjning finns det även planer för systemutveckling som anses bidra till robustheten inom Elförsörjning. Den kritiska infrastrukturen som helhet bedöms arbeta med *planer inför oönskade händelser* i högre grad.

- I sammanställningen framkom det att samarbetet som finns dels sker inom den kritiska infrastrukturen (samarbete mellan nätägare inom Elförsörjning kring underhåll), dels med aktörer utanför den kritiska infrastrukturen (möjlighet till elimport och avtal med industrier). Eftersom det sker flera slags samarbeten med olika aktörer, både internt och externt, bedöms Elförsörjning arbeta med s*amarbeten kopplat till robusthet* i högre grad.

Tekniska faktorer

- Från sammanställningen framkom det inga bufferts inom Elförsörjning. Det går därför inte att göra en bedömning hur den kritiska infrastrukturen arbetar med *bufferts.*
- Från sammanställningen framkom det att nätägare har flera redundanta system medan de övervakande och stödjande aktörerna inte arbetade med redundans i samma omfattning. Som helhet bedöms den kritiska infrastrukturen arbeta med *redundanta system eller en inbyggd redundans i systemen* i högre grad eftersom det finns hög grad av redundans i elnäten.

Återhämtning

Organisatoriska faktorer

- I sammanställningen framkom det att det finns organisatoriska resurser i form av kompetent personal som kan återställa systemen vid en störning. För återställning av den kritiska infrastrukturens Elförsörjning är kompetent personal en viktig komponent och därför bedöms den kritiska infrastrukturen arbeta med *organisatoriska resurser* i högre grad.
- I sammanställningen framkom det att det finns utarbetade planer för att koordinera kapacitet vid elbrist för effektivare användning av resurserna. Inom den kritiska infrastrukturen förekommer det även utbildningar som fokuserar på resurshantering vid en störning. För att effektivt kunna hantera resurserna finns det lager inom Elförsörjning som är placerade på flera ställen i Sverige, vilket anses vara en strategi för en effektiv resurshantering. Sammantaget bedöms arbetet med *ledning och koordination för resurshantering* inom den kritiska infrastrukturen förekomma i högre grad
- Sammanställningen visade att det finns ett flertal samarbeten inom den kritiska infrastrukturen kopplat till återhämtning. Till stor del bidrar samarbetet med andra aktörer till delandet av resurser, både med aktörer inom den kritiska infrastrukturen och med externa aktörer så som aktörer i Norden. Resursdelningen bidrar till en snabbare återställning av elnäten vid en störning. Elförsörjning bedöms arbeta med *samarbeten kopplat till återhämtning* i högre grad.
- Sammanställningen visade att det genomförs samverkansövningar kring driftstörningar inom den kritiska infrastrukturen där ett flertal aktörer medverkar. Övningarna fokuserar på hur aktörerna ska agera efter att en störning inträffat och anses därför bidra till förmågan för återhämtning inom Elförsörjning. De enskilda aktörerna inom Elförsörjning uppvisade även visst arbete med mindre övningar kopplat till robusthet så som övningar i reparationsberedskap. Den kritiska infrastrukturen bedöms arbeta med *övningar kopplat till återhämtning* i högre grad.
- I sammanställningen framkom det från flera aktörer att återställandet av elnäten efter en störning innebär ett stort arbete. Detta är något som hela den kritiska infrastrukturen bedöms arbeta med. För de aktörer som har en mer övervakande och stödjande roll framkom det att det finns vägledande dokument och krisledning för återhämtning. Eftersom arbete med

återställning sker både på ledningsnivå och på elnätsnivå bedöms arbetet med *strategier för återhämtning* inom Elförsörjning förekomma i högre grad.

Tekniska faktorer

- Sammanställningen visade att det finns resurser inom Elförsörjning i form av lager samt tillgång till reservmaterial och utrustning som kan användas vid återhämtning. En del av resurserna finns hos aktörerna inom Elförsörjning, men en del av resurserna finns endast tillgängliga via samarbeten med andra aktörer. Baserat på de tekniska resurser som finns inom Elförsörjning bedöms den kritiska infrastrukturen arbeta med *tekniska resurser* i högre grad.

Anpassning

Organisatoriska faktorer

- I sammanställningen framkom det att aktörerna inom Elförsörjning följer upp och utvärderar i lärande syfte. Beroende på aktörernas roller inom Elförsörjning har de olika fokus på sina utvärderingar. Aktören med övervakande roll fokuserade sina utvärderingar på hur den kritiska infrastrukturen hanterar en större störning (exempelvis stormen Gudrun). Nätägare utvärderar sin egen kapacitet utifrån tidigare störningar så som en storm. Inom den kritiska infrastrukturen sker det även utredningar inför en större åtgärdsimplementering för att utvärdera kostnaden och effekten av åtgärden. Sammanlagt sker det både utvärderingar av framtida åtgärder såväl som uppföljning av tidigare störningar på olika nivåer inom Elförsörjning. Den kritiska infrastrukturen bedöms arbeta med *utvärdering och uppföljning i lärande syfte* i högre grad.
- Sammanställningen visade att den kritiska infrastrukturen bedriver forskning för att bättre kunna anpassa mot störningar. Det förekommer även fler åtgärder men dessa är delvis sekretessbelagda och det finns därför en osäkerhet i bedömningen för denna faktor. Det går därför inte att bedöma till vilken grad den kritiska infrastrukturen arbetar med *organisatoriska åtgärder.*
- I sammanställningen framkom det att det finns en nationell samverkansgrupp som aktörer inom Elförsörjning ingår i och ett direktiv för erfarenhetsutbyte som berör Elförsörjning. Det finns även ett forum kallat samverkansområdet teknisk infrastruktur (SOTI) där aktörer inom teknisk infrastruktur, det vill säga både aktörer inom Elförsörjning och externa aktörer, utbyter erfarenheter (MSB, 2016). Detta forum lyftes dock inte av någon av de tre medverkande aktörerna utan har hittats genom dokumentsökning. Därför anses aktörerna inte arbeta med forumet i högre grad för erfarenhetsutbyte. Den kritiska infrastrukturen bedöms arbeta med *erfarenhetsutbyte i lärande syfte* i lägre grad.

Tekniska faktorer

- Sammanställningen visade att det finns SCADA- och GIS-system inom den kritiska infrastrukturen som utvärderar driftstatusen och ger kontinuerlig lägesbild för elnätet. Dessa system bedöms utgöra en viktig del för den kritiska infrastrukturens arbete med utvärdering av de fysiska delarna av Elförsörjningen (noder, kablar etcetera). Däremot framkom inga tekniska system som används för utvärdering och uppföljning av implementerade åtgärder utan enbart driftstatus. Den kritiska infrastrukturen bedöms därför arbeta med *utvärdering och uppföljning i lärande syfte med tekniska system* i lägre grad.

- Sammanställningen visade att det sker långsiktiga tekniska åtgärder i form av uppgradering av system i elnätet och kontinuerligt underhåll. Det kom även fram att det sker ett arbete med mer kortsiktiga åtgärder, exempelvis finns det ett digitalt verktyg som möjliggör att under kortare perioder öka utnyttjandegraden i elnätet. Eftersom det sker ett arbete med både kortsiktiga och långsiktiga tekniska åtgärder inom den kritiska infrastrukturen bedöms Elförsörjning arbeta med *tekniska åtgärder* i högre grad.

Sammanfattning av Elförsörjning arbete med ramverkets faktorer

I Tabell 6 sammanfattas Elförsörjnings arbete med ramverkets faktorer. Tabellen visar till vilken grad respektive aktör bedöms arbeta med faktorerna samt till vilken grad den kritiska infrastrukturen bedöms arbeta med faktorerna.

Tabell 6. Sammanfattning av Elförsörjning arbete med ramverkets faktorer.

Förutseende				
Faktorer	Aktör D	Aktör E	Aktör F	Elförsörjning
Har tydliga mål på vad som ska skyddas.				
Förses kontinuerligt med information genom organisatoriska system för informationsinsamling.				
Har organisatoriska system för att analysera information				
Har förmåga att uppmärksamma otydliga signaler och indikationer.				
Förses kontinuerligt med information genom tekniska system för informationsinsamling.				
Har tekniska system för att analysera insamlad information.				
Robusthet				
Faktorer	Aktör D	Aktör E	Aktör F	Elförsörjning
Genomför övningar inför oönskade händelser.				
Planerar inför oönskade händelser.				
Har ett samarbete med andra samhällsaktörer.				
Det finns en buffert i kapaciteten.				
Det finns redundanta system eller en inbyggd redundans i systemen.				
Återhämtning				
Faktorer	Aktör D	Aktör E	Aktör F	Elförsörjning

Har tillgång till organisatoriska resurser.				
Har en plan för ledning och koordination för resurshantering.				
Har ett samarbete och förtroende med andra samhällsaktörer.				
Genomför övningar med fokus på återhämtning.				
Har utformade strategier med fokus på återhämtning.				
Har tillgång till tekniska resurser.				
Anpassning				
Faktorer	Aktör D	Aktör E	Aktör F	Elförsörjning
Uppföljning och utvärdering görs kontinuerligt i lärande syfte med hjälp av organisatoriska system				
Implementerar organisatoriska förebyggande/proaktiva åtgärder.				
Det sker erfarenhetsutbyte mellan den kritiska infrastrukturen och andra aktörer.				
Uppföljning och utvärdering görs kontinuerligt i lärande syfte med hjälp av tekniska system.				
Implementerar tekniska förebyggande/proaktiva åtgärder.				

5.2.2 Elförsörjnings arbete med förmågorna för resiliens

Förutseende

Den kritiska infrastrukturen Elförsörjning arbetar i högre grad med informationsinsamling med både organisatoriska och tekniska system. Elförsörjning är en kritisk infrastruktur som arbetar med många olika tekniska system och systemen är ofta integrerade i själva elnätet. Sammanställningen visade att de medverkande aktörerna arbetar med förmågan för förutseende på olika sätt utifrån aktörernas olika roller inom den kritiska infrastrukturen. Bedömningen är att kombinationen av aktörernas arbeten skapar en stark förmåga för förutseende inom Elförsörjning som kritisk infrastruktur.

Sammanfattningsvis bedöms Elförsörjning vara en kritisk infrastruktur som arbetar med förmågan för förutseende i högre grad. Samtliga aktörer svarade högt på skalfrågan om till vilken grad de arbetade med förmågan för förutseende (5/6). Den bedömning som gjorts för Elförsörjning är alltså att arbetet med förmågan för förutseende sker i lika hög grad som vad alla aktörer själva bedömt sitt arbete med förmågan. Elförsörjning arbetar med förutseende och återhämtning mest av de fyra förmågorna för resiliens.

Robusthet
Sammanställningen visar att det finns vissa informationsluckor kring Elförsörjnings arbete med förmågan för robusthet. Enligt Aktör D sker en störning inom Elförsörjning mycket fort. Det snabba händelseförloppet vid typiska störningar inom Elförsörjning antas påverka hur aktörerna måste arbeta för att motstå och absorbera chocken av en störning. Övningar för ett sådant snabbt händelseförlopp är troligtvis inte effektivt för att höja förmågan för robusthet. Detta antas vara en bakomliggande orsak till informationsluckorna för faktorn *övningar kopplade till robusthet*. Det framkom att den kritiska infrastrukturen i högre grad arbetar med organisatoriska metoder i form av samarbeten och planer inför oönskade händelser. Även arbetet med redundanta system bedöms vara en viktig del för förmågan för robusthet inom Elförsörjningen. Redundans är troligtvis ett viktigt verktyg för att motstå och absorbera choken av en snabb störning. Det finns ingen tydlig skillnad i hur den kritiska infrastrukturen arbetar med organisatoriska respektive tekniska faktorer gällande robusthet.

Sammanfattningsvis bedöms Elförsörjning vara en kritisk infrastruktur som arbetar med förmågan för robusthet i någorlunda hög grad. I enkäten svarade Aktör D och F själva att de arbetar med robusthet i någorlunda hög grad (4/6) medan Aktör E svarade relativt högt på skalfrågan (5/6). Den bedömning som gjorts är att den kritiska infrastrukturen Elförsörjning arbetar mindre med förmågan för robusthet jämfört med Aktör E:s egen bedömning men i nivå med Aktör D och Aktör F:s egna bedömningar.

Återhämtning
Sammanställningen visade att det sker ett arbete med samtliga faktorer kopplat till återhämtning i högre grad. Den kritiska infrastrukturen arbetar med förmågan för återhämtning både organisatoriskt och tekniskt. För Elförsörjning framkom det flera arbeten som endast genomförs av en eller två aktörer men som bidrar till hela den kritiska infrastrukturens återhämtning.

Sammanfattningsvis är Elförsörjning en kritisk infrastruktur som arbetar med förmågan för återhämtning i högre grad. Resultaten från analysen överensstämmer väl med Aktör E:s egen bedömning på skalfrågan i enkäten om till vilken grad de arbetar med återhämtning (6/6). Både Aktör D och Aktör F svarade något lägre på skalfrågan (4/6). Detta innebär att aktörernas egna bedömningar är lägre jämfört med vad analysen visar att Elförsörjning som kritisk infrastruktur arbetar med förmågan för återhämtning. Utifrån analysen bedöms återhämtning tillsammans med förutseende vara de förmågor som Elförsörjning arbetar mest med av de fyra förmågorna för resiliens.

Anpassning
Även om det finns informationsluckor kring aktörernas arbete går det generellt att bedöma hur den kritiska infrastrukturen som helhet arbetar med förmågan för anpassning. Det går inte att bedöma om Elförsörjning arbetar mest med organisatoriska eller tekniska faktorer. Däremot visade sammanställningen att de åtgärder som implementeras inom Elförsörjning främst är tekniska. Sammanställningen visade att erfarenhetsutbyte är bland de områden där den kritiska infrastrukturen uppvisade minst arbete. Dock används metoder kopplade till utvärdering och uppföljning för lärande inom Elförsörjning i högre grad. Det sker alltså ett lärande inom den kritiska infrastrukturen, men främst baserat på egna utvärderingar snarare än baserat på erfarenheter från andra aktörer.

Sammanfattningsvis bedöms Elförsörjning vara en kritisk infrastruktur som arbetar med förmågan för anpassning i någorlunda låg grad. I enkäten svarade Aktör D och F själva att de arbetar med anpassning i någorlunda hög grad (4/6) medan Aktör E svarade relativt högt på skalfrågan (5/6). Den bedömning som gjorts är att den kritiska infrastrukturen Elförsörjning arbetar mindre med förmågan för anpassning jämfört med aktörernas egna bedömningar. Utifrån analysen bedöms anpassning vara den förmåga som den kritiska infrastrukturen Elförsörjning arbetar minst med av de fyra förmågorna för resiliens.

5.3 Telekommunikation

Telekommunikation är ett samlingsbegrepp för kommunikation som sker på avstånd med hjälp av tekniska hjälpmedel. Kommunikationen innefattar överföring av ljud, bild och data genom exempelvis telefoni, fiberoptik och internet (NE, 2020b; Telenor, 2020). Den övergripande funktionen för den kritiska infrastrukturen Telekommunikation är således att upprätthålla överföringen av ljud, bild och data.

För Telekommunikation undersöktes två aktörer och deras arbete med resiliens; Aktör G och Aktör H. Vid informationsinsamlingen framkom det att aktörerna inte äger eller driver några egna nät utan arbetar med att 1) övervaka den kritiska infrastrukturen för att skapa en fungerande marknad, samt 2) bidra till att leverera digital infrastruktur. Detta anses vara det som aktörerna bidrar med för att upprätthålla Telekommunikations funktion. Nedan presenteras hur den kritiska infrastrukturen arbetar med ramverkets faktorer samt förmågorna för resiliens baserat på insamlad information från aktörerna. I detta kapitel presenteras enbart översiktligt hur aktörerna arbetar utifrån ramverkets faktorer. För mer detaljer kring insamlat material och sammanställningen av denna hänvisas läsaren till Appendix E där aktörernas arbete och kopplingen till ramverkets faktorer presenteras mer ingående.

5.3.1 Telekommunikations arbete med ramverkets faktorer

Förutseende

Organisatoriska faktorer

- Sammanställningen av det insamlade materialet från aktörerna visade att båda aktörerna inom den kritiska infrastrukturen har tydliga mål på hur de ska arbeta för att upprätthålla funktionen. Målen som framkom av Aktör G och Aktör H som kan kopplas till den kritiska infrastrukturens funktion är att tillgodose det digitala behovet och göra det möjligt för alla att använda digitala tjänster. Målen berör även att skapa en fungerande marknad för att upprätthålla telekommunikationen i samhället. Telekommunikation bedöms arbeta med *tydliga mål* på vad som ska skyddas i högre grad.
- Sammanställningen av det insamlade materialet visade att det finns flera organisatoriska system för informationsinsamling inom den kritiska infrastrukturen, dels för att identifiera vad som sker inom den kritiska infrastrukturen, dels vad som sker i omvärlden. Arbetet med *organisatoriska system för informationsinsamling* bedöms därför förekomma i högre grad inom Telekommunikation.
- Sammanställningen av det insamlade materialet visade att aktörer inom Telekommunikation använder flera olika organisatoriska system för analys. Arbetet med *organisatoriska system för analys* inom den kritiska infrastrukturen bedöms förekomma i högre grad.

- Sammanställningen visade att organisatorisk analys av information från forum och tekniska system inom Telekommunikation bidrar till att kunna uppmärksamma otydliga signaler och indikationer. Den kritiska infrastrukturen bedöms arbeta med att *uppmärksamma otydliga signaler och indikationer* i telekommunikationsnätet i högre grad.

Tekniska faktorer

- Från sammanställningen framkom det att det används ett flertal större tekniska system, så som SCADA och GIS, för informationsinsamling för att övervaka nätverket samt samla in information om omvärlden. Arbetet med *tekniska system för informationsinsamling* inom den kritiska infrastrukturen bedöms förekomma i högre grad.
- I sammanställningen framkom det att nätägare använder system för information om telekommunikationsnätet medan aktörer med en mer övervakande roll använder system för att analysera omgivningen respektive marknadens påverkan på Telekommunikationens funktion. Eftersom systemen berör fler områden som kan påverka funktionen bedöms *tekniska system för analys* användas i högre grad inom Telekommunikation.

Robusthet

Organisatoriska faktorer

- I sammanställningen framkom det att det genomförs övningar inom Telekommunikation men att dessa övningar endast har en svag koppling till robusthet. Likt avbrott inom Elförsörjning sker avbrott inom Telekommunikation generellt snabbt. Övningar förväntas därför inte kunna bidra till att kunna motstå en sådan störning eller absorbera chocken av störningen. Inom den kritiska infrastrukturen bedöms därför *övningar kopplade till robusthet* endast förekomma i lägre grad.
- Sammanställningen av det insamlade materialet visade att det finns ett flertal planer inför oönskade händelser inom den kritiska infrastrukturen. Det finns väletablerade vägledningar som skapar en lägsta säkerhetsnivå inom den kritiska infrastrukturen. Även att Telekommunikation har uppvisat en motståndskraft mot den ökade nyttjandet av telekommunikationen inom Sverige under Covid-19 pandemin anses visa på att den kritiska infrastrukturen planerar inför oönskade händelser. Den kritiska infrastrukturen bedöms därför arbeta med *planer inför oönskade händelser* i högre grad.
- Det finns delar av aktörernas arbete med andra faktorer kopplat till robusthet som inte hade fungerat utan ett samarbete inom Telekommunikation. Exempelvis skulle inte vägledningarna kunna etablerats och få en positiv påverkan utan att aktörerna samarbetade. Det framkom även ett exempel på då samarbeten mellan aktörer inom Telekommunikation och externa aktörer bidrog till den kritiska infrastrukturens robusthet, se Appendix E, Aktör G för en mer ingående beskrivning. Dessa samarbeten var de exempel som framkom av sammanställningen av det insamlade materialet gällande *samarbete kopplat till robusthet*. Den kritiska infrastrukturen bedöms därför arbeta med faktorn i lägre grad.

Tekniska faktorer

- Sammanställningen visade att det finns bufferts inom den kritiska infrastrukturen i form av bränslereserver och reservkraftverk. Eftersom de bufferts som finns bedöms vara viktiga inom den kritiska infrastrukturen för beroenden till andra aktörer bedöms *buffert* vara en faktor som Telekommunikation arbetar med i högre grad.

- Sammanställningen visade att båda aktörerna som ingår i undersökningen uppgav att det finns flertal redundanta system inom Telekommunikation, främst i form av redundans i noder och fiberkablar. Det finns även transportabla mobilbasstationer som kan användas för att tillfälligt öka kapaciteten i telekommunikationsnätet. De redundanta systemen betonades som viktiga för upprätthållandet av Telekommunikations funktion. Arbetet med faktorn *redundanta system eller en inbyggd redundans i systemen* bedöms därför förekomma i högre grad inom den kritiska infrastrukturen.

Återhämtning

Organisatoriska faktorer

- I sammanställningen av det insamlade materialet framkom att det finns tillgång till organisatoriska resurser inom Telekommunikation så som samordningsstöd, kompetent personal och möjlighet för aktörer att låna varandras personal vid störningar. Även om Aktör G i sig endast arbetar med organisatoriska resurser i lägre grad så bedöms kombinationen av de *organisatoriska resurserna* som finns inom Telekommunikation, främst tillgången till personal, göra att den kritiska infrastrukturen arbetar med denna faktor i högre grad.
- Krisportalen anses vara det system från sammanställningen som främst bidrar till ledning och koordination av resurser inom Telekommunikation. Resterande planer kring resurshanteringen anses mest fokusera på aktörernas egen resurshantering snarare än fördelning av resurser inom den kritiska infrastrukturen Telekommunikation. Eftersom det finns en krisportal för att koordinera de resurser som finns inom den kritiska infrastrukturen bedöms Telekommunikation arbeta med *ledning och koordination av resurser* i högre grad.
- Från sammanställningen framkom det att det sker ett samarbete mellan aktörer både inom och utanför den kritiska infrastrukturen för att återhämta funktionen efter en störning. Samarbetet bidrar till att den kritiska infrastrukturens funktion återhämtas effektivare genom att både tekniska och organisatoriska resurser frigörs och att lägesbilder delas mellan aktörer. Den kritiska infrastrukturen bedöms arbeta med *samarbete för återhämtning* i högre grad.
- I sammanställningen framkom det att båda aktörerna inom den kritiska infrastrukturen arbetar med övningar som berör hanteringen efter störningar inom Telekommunikation. Övningarna sker på olika sätt och fokuserar på olika delar av återhämtningen. Den kritiska infrastrukturen bedöms arbeta med *övningar för återhämtning* i högre grad.
- I sammanställningen av det insamlade materialet framkom det att båda aktörerna som medverkat i undersökningen för Telekommunikation arbetar med kontinuitetsplaner för att effektivt kunna återhämta den kritiska infrastrukturen efter en störning. Planerna anses omfatta flera kritiska delar av den kritiska infrastrukturen samt beröra flera aktörer inom den kritiska infrastrukturen. Den kritiska infrastrukturen som helhet bedöms arbeta med *planer och strategier för återhämtning* i högre grad.

Tekniska faktorer

- De tekniska resurser som finns inom den kritiska infrastrukturen Telekommunikations som framkom i sammanställningen av det insamlade materialet är reservnoder, mobila reservkraftverk samt mobila basstationer. Dessa system anses vara viktiga för att återhämta

Telekommunikation och den kritiska infrastrukturen som helhet bedöms arbeta med *tekniska resurser* i högre grad.

Anpassning

Organisatoriska faktorer

- Sammanställningen av det insamlade materialet visade att det inom Telekommunikation görs utvärderingsrapporter och förs diskussioner efter större störningar. Det sker även en kontinuerlig uppföljning av hur aktörer inom Telekommunikation arbetar med anpassningsåtgärder. Sammanställningen anses visa att den kritiska infrastrukturen Telekommunikation arbetar med *utvärdering och uppföljning i lärande syfte* i högre grad.
- Båda aktörerna som medverkade i undersökningen för Telekommunikation gav tydliga exempel på organisatoriska förebyggande åtgärder som har implementerats inom den kritiska infrastrukturen för att öka Telekommunikationens resiliens. Åtgärderna var dels kopplade till aktörernas egen resiliens (uppdatering av krisdokument), dels till anpassning efter detekterade hot (sociala kampanjer för att motverka antagonistiska störningar). Utöver detta arbetade aktörerna med att få in lärdomar från tidigare störningar i den kritiska infrastrukturens arbete genom att kontinuerligt uppdatera de vägledande dokumenten. Sammanställningen visade att det *implementeras förebyggande organisatoriska åtgärder* inom Telekommunikationen i högre grad.
- Det mesta av erfarenhetsutbytet som sker inom den kritiska infrastrukturen sker via en nationell samverkansgrupp som både Aktör G och Aktör H ingår i. Sammanställningen visade att *erfarenhetsutbytet i lärande syfte* inom Telekommunikation sker mellan aktörer inom den kritiska infrastrukturen, och inte med externa aktörer. Därför bedöms den kritiska infrastrukturen endast arbeta med faktorn i lägre grad.

Tekniska faktorer

- Sammanställningen visade att det finns två tekniska system inom Telekommunikation som kan användas för *uppföljning och utvärdering i lärande syfte*; GIS och SCADA. Gällande GIS ansågs det inte finnas tillräcklig information för att bedöma till vilken grad systemet bidrar till Aktör G:s arbetet med faktorn. Däremot bedöms SCADA-systemet vara ett system som är mycket omfattande och som möjliggör att den kritiska infrastrukturen kan följa upp och utvärdera störningar i högre grad.
- Från sammanställningen framkom det, specifikt från Aktör H, att den kritiska infrastrukturen har genomfört flera större tekniska förändringar för att anpassas. Anpassningarna har varit fokuserade på hur Telekommunikationens tekniska infrastruktur kan stå emot väderrelaterade och antagonistiska störningar. Arbetet med *tekniska åtgärder* inom den kritiska infrastrukturen bedöms vara i högre grad.

Sammanfattning av Telekommunikations arbete med ramverkets faktorer

I Tabell 7 sammanfattas Telekommunikations arbete med ramverkets faktorer. Tabellen visar till vilken grad respektive aktör bedöms arbeta med faktorerna samt till vilken grad den kritiska infrastrukturen bedöms arbeta med faktorerna.

Tabell 7. Sammanfattning av Telekommunikation arbete med ramverkets faktorer.

Förutseende			
Faktorer	Aktör G	Aktör H	Telekommunikation
Har tydliga mål på vad som ska skyddas.			
Förses kontinuerligt med information genom organisatoriska system för informationsinsamling.			
Har organisatoriska system för att analysera information			
Har förmåga att uppmärksamma otydliga signaler och indikationer.			
Förses kontinuerligt med information genom tekniska system för informationsinsamling.			
Har tekniska system för att analysera insamlad information.			
Robusthet			
Faktorer	Aktör G	Aktör H	Telekommunikation
Genomför övningar inför oönskade händelser.			
Planerar inför oönskade händelser.			
Har ett samarbete med andra samhällsaktörer.			
Det finns en buffert i kapaciteten.			
Det finns redundanta system eller en inbyggd redundans i systemen.			
Återhämtning			
Faktorer	Aktör G	Aktör H	Telekommunikation
Har tillgång till organisatoriska resurser.			
Har en plan för ledning och koordination för resurshantering.			
Har ett samarbete och förtroende med andra samhällsaktörer.			
Genomför övningar med fokus på återhämtning.			

Har utformade strategier med fokus på återhämtning.			
Har tillgång till tekniska resurser.			
Anpassning			
Faktorer	Aktör G	Aktör H	Telekommunikation
Uppföljning och utvärdering görs kontinuerligt i lärande syfte med hjälp av organisatoriska system			
Implementerar organisatoriska förebyggande/proaktiva åtgärder,			
Det sker erfarenhetsutbyte mellan den kritiska infrastrukturen och andra aktörer.			
Uppföljning och utvärdering görs kontinuerligt i lärande syfte med hjälp av tekniska system.			
Implementerar tekniska förebyggande/proaktiva åtgärder			

5.3.2 Telekommunikations arbete med förmågorna för resiliens

Förutseende

Det finns tydliga mål inom den kritiska infrastrukturen som aktörerna arbetar mot för att upprätthålla funktionen. För att upprätthålla funktionen Telekommunikation används både organisatoriska och tekniska system och metoder vilket bidrar till förmågan att vara förutseende. Däremot finns det fler tekniska system än organisatoriska system för informationsinsamling vilket visar att den kritiska infrastrukturen har en tendens att fokusera mer på tekniska system även om båda typerna av systemens bedöms användas i högre grad. Både organisatoriska och tekniska system används i högre grad för att analysera den insamlade informationen. Det framkom inte ifall de organisatoriska eller de tekniska analyssystemen används mest.

Sammanfattningsvis är Telekommunikation en kritisk infrastruktur som arbetar med förmåga för förutseende i högre grad. Resultaten från analysen överensstämmer relativt väl med aktörernas egna bedömningar på hur de arbetar med förutseende med hänsyn till aktörernas enkätsvar. Både Aktör G och Aktör H la sig högt på skalfrågan i enkäten om deras arbetade med förutseende (6/6 respektive 5/6). Analysen visar att den kritiska infrastrukturen arbetar med förutseende i relativt hög grad, vilket alltså är något lägre än aktörernas egna bedömningar. Utifrån analysen bedöms förutseende tillsammans med återhämtning vara de förmågorna som den kritiska infrastrukturen telekommunikation arbetar mest med av de fyra förmågorna för resiliens.

Robusthet

Inom Telekommunikation bedöms aktörerna arbeta med alla faktorer som bidrar till förmågan för robusthet i antingen lägre eller högre grad. Det som framkom från sammanställningen av aktörernas arbete är att den kritiska infrastrukturen i högre grad arbetar med de tekniska faktorerna, det vill säga buffert i kapaciteten och redundanta system, vilket bidrar till förmågan för robustheten. Inom Telekommunikation anses aktörerna inte arbeta lika mycket med organisatoriska faktorer för att öka robustheten i den kritiska infrastrukturen. Från sammanställningen framkom det att aktörer inom Telekommunikation har planerat och byggt ett telekommunikationsnätverk som klarar av ökningar i nyttjandegraden utan att drabbas av störningar. Under Covid-19 pandemin har, enligt aktörerna, flera länder inom Europa drabbats av störningar inom telekommunikationen på grund av den ökade användningen medan Telekommunikation i Sverige har absorberat chocken och inte drabbats av störningar. För Aktör H finns det vissa luckor där informationen inte varit tillräcklig för att göra en bedömning. Luckorna skapar en osäkerhet i bedömningen av aktörens arbete med vissa faktorer kopplade till robusthet, men med den tillgängliga informationen har det ändå varit möjligt att göra en bedömning för hur arbetet generellt ser ut inom den kritiska infrastrukturen.

Sammanfattningsvis är Telekommunikation en kritisk infrastruktur som arbetar med förmåga för robusthet i relativt hög grad. Resultaten från analysen överensstämmer relativt väl med Aktör G:s egen bedömning för hur de arbetar med robusthet eftersom Aktör G la sig högt på skalfrågan i enkäten om deras arbetade med robusthet (6/6). Aktör H la sig också relativt högt på skalfrågan i enkäten (5/6). Utifrån analysen bedöms robusthet vara den förmåga som den kritiska infrastrukturen Telekommunikation bedöms arbeta minst med av de fyra förmågorna för resiliens.

Återhämtning

Inom den kritiska infrastrukturen arbetar aktörerna både med organisatoriska och tekniska faktorer som bidrar till förmågan för återhämtning. Även om den kritiska infrastrukturens arbete med både organisatoriska och tekniska faktorer bidrar till förmågan för robusthet i högre grad går det att utskilja att det finns fler tekniska resurser än organisatoriska resurser för återhämtning. Sammanställningen pekar på att Aktör G generellt arbetar mindre med faktorerna för återhämtning jämfört med Aktör H. Sammanställningen visade även att Aktör H i högre grad utgick från den kritiska infrastrukturens arbete under intervjun jämfört med Aktör G som främst utgick från sitt eget arbete.

Den kritiska infrastrukturen arbetar med samtliga av ramverkets faktorer som bidrar till förmågan för återhämtning i högre grad. Telekommunikations arbete med återhämtning bedöms som högre än vad aktörerna som ingick i undersökningen själva har angett på enkäten. Detta eftersom Aktör G la sig relativt högt på skalfrågan i enkäten om deras arbete med återhämtning (5/6) medan Aktör H la sig något lägre på skalfrågan i enkäten om deras arbetade med återhämtning (4/6). Utifrån analysen bedöms återhämtning tillsammans med förutseende vara de förmågorna som den kritiska infrastrukturen telekommunikation arbetar mest med av de fyra förmågorna för resiliens.

Anpassning

Sammanställningen visade att det sker ett arbete med både organisatoriska och tekniska faktorer som bidrar till anpassning inom Telekommunikation. Däremot är den kritiska infrastrukturen inte lika bra på att anpassas efter lärdomar om störningar som drabbat aktörer utanför Telekommunikation, detta eftersom det inte sker något erfarenhetsutbyte med aktörer som är verksamma utanför den kritiska infrastrukturen. För de tekniska faktorerna saknades det tillräcklig information för antingen Aktör G eller Aktör H för att göra en bedömning av aktörernas arbete med faktorn. Luckorna skapar viss osäkerhet i bedömningen av Aktör G: arbete med uppföljning och utvärdering samt Aktör H:s arbete med implementerande av tekniska åtgärder. Analys av den kombinerade tillgängliga informationen har ändå gjort det möjligt att göra en bedömning för hur arbetet generellt ser ut inom Telekommunikation.

Sammanfattningsvis bedöms Telekommunikation vara en kritisk infrastruktur som i hög grad arbetar med förmågan för anpassning. Bedömningen av analysen stämmer relativt väl med den bedömning som aktörerna inom den kritiska infrastrukturen själva gjorde i enkäten. Aktör G la sig relativt högt på skalfrågan i enkäten om deras arbetade med återhämtning (5/6). Aktör H la sig något lägre på skalfrågan i enkäten om deras arbetade med återhämtning (4/6).

6 Jämförelse av de kritiska infrastrukturerna

I detta kapitel jämförs resultaten av analysen för de tre kritiska infrastrukturerna. Först ges en visuell sammanfattning av de kritiska infrastrukturernas arbete med ramverkets faktorer, sedan diskuteras och jämförs de kritiska infrastrukturernas arbete med förmågorna för resiliens mer ingående.

6.1 Jämförelse av de kritiska infrastrukturerna arbete med ramverkets faktorer

Nedan presenteras resultatet av de kritiska infrastrukturernas arbete med ramverkets faktorer som framkom från föregående kapitel. I Tabell 8 jämförs visuellt de kritiska infrastrukturernas arbete med respektive faktor för förmågorna för resiliens.

Tabell 8. Jämförelse av de kritiska infrastrukturernas arbete med ramverkets faktorer.

Förutseende			
Faktorer	Räddningstjänst	Elförsörjning	Telekommunikation
Har tydliga mål på vad som ska skyddas.			
Förses kontinuerligt med information genom organisatoriska system för informationsinsamling.			
Har organisatoriska system för att analysera information			
Har förmåga att uppmärksamma otydliga signaler och indikationer.			
Förses kontinuerligt med information genom tekniska system för informationsinsamling.			
Har tekniska system för att analysera insamlad information.			
Robusthet			
Faktorer	Räddningstjänst	Elförsörjning	Telekommunikation
Genomför övningar inför oönskade händelser.			
Planerar inför oönskade händelser.			
Har ett samarbete med andra samhällsaktörer.			
Det finns en buffert i kapaciteten.			

Det finns redundanta system eller en inbyggd redundans i systemen.			
Återhämtning			
Faktorer	Räddningstjänst	Elförsörjning	Telekommunikation
Har tillgång till organisatoriska resurser.			
Har en plan för ledning och koordination för resurshantering.			
Har ett samarbete och förtroende med andra samhällsaktörer.			
Genomför övningar med fokus på återhämtning.			
Har utformade strategier med fokus på återhämtning.			
Har tillgång till tekniska resurser.			
Anpassning			
Faktorer	Räddningstjänst	Elförsörjning	Telekommunikation
Uppföljning och utvärdering görs kontinuerligt i lärande syfte med hjälp av organisatoriska system			
Implementerar organisatoriska förebyggande/proaktiva åtgärder.			
Det sker erfarenhetsutbyte med andra aktörer.			
Uppföljning och utvärdering görs kontinuerligt i lärande syfte med hjälp av tekniska system.			
Implementerar tekniska förebyggande/proaktiva åtgärder.			

6.2 Jämförelse av de kritiska infrastrukturernas arbete med förmågorna för resiliens

Förutseende

Vid analys av de kritiska infrastrukturernas arbete med förmågan för förutseende framkom det att Räddningstjänst, Elförsörjning och Telekommunikation alla arbetar med förutseende i antingen relativt hög grad eller högre grad. En skillnad som framkom i de kritiska infrastrukturernas arbete var att både Elförsörjning och Telekommunikation bedömdes ha en förmåga att uppmärksamma otydliga signaler och indikationer, medan det för Räddningstjänst inte gick att bedöma till vilken grad de arbetar med detta. Det fanns även en mindre skillnad i arbetet med tekniska faktorer mellan de kritiska infrastrukturerna där Elförsörjning och Telekommunikation bedömdes vara de kritiska infrastrukturerna som arbetar mest med att analysera genom tekniska system. Det går däremot inte bestämma huruvida det finns en skillnad mellan organisatoriskt och tekniskt arbete på förmågenivå för de olika kritiska infrastrukturerna utan enbart på faktornivå. Telekommunikation och Elförsörjning bedömdes uppvisa mer arbete med förmågan för förutseende jämfört med Räddningstjänst. Det förekom ingen signifikant skillnad mellan hur aktörerna för respektive kritisk infrastruktur själva ansåg att de arbetade med förmågan för förutseende och det analysen visade.

Robusthet

Robusthet är den förmåga som både Räddningstjänst och Telekommunikation bedömdes arbeta med i lägst grad. Elförsörjning och Telekommunikation bedömdes arbeta med redundans i högre grad än Räddningstjänst. Detta kan bero på att det inom Elförsörjning och Telekommunikation finns fysiska nätverk där redundans i hög grad används för att skapa robusthet. Att Räddningstjänst bedöms vara den kritiska infrastruktur som arbetar med *planer inför oönskade händelser* i lägst grad kan bero på att det inte finns väletablerade strategier i samma utsträckning som för de andra kritiska infrastrukturerna, exempelvis N-1 kriteriet som finns inom Elförsörjning. Det som samtliga kritiska infrastrukturer arbetade mindre med var övningar kopplat till robusthet. Detta skulle kunna bero på att en påverkan på de kritiska infrastrukturernas funktioner ofta sker snabbt och att det därför blir svårare att öva på att absorbera chocken och minska de direkta konsekvenserna. Detta anses speciellt gälla för de mer tekniska infrastrukturerna där omfattande avbrott i funktionen kan ske på mindre än en sekund. Ett exempel på en sådan störning är ett avbrott i el- eller telekommunikationsnät då en elkraftsledning eller en optokabel av någon anledning slutar att fungera. Generellt var Räddningstjänst den kritiska infrastruktur som bedömdes arbeta minst med förmågan för robusthet medan Elförsörjning och Telekommunikation bedömdes arbeta i samma grad med förmågan. Bedömningen för Räddningstjänsts arbete med förmågan för robusthet var lägre än aktörernas egen bedömning. För Elförsörjning och Telekommunikation var bedömningen på samma nivå som aktörernas egna bedömningar.

Återhämtning

Återhämtning är den förmåga för resiliens som både Elförsörjning och Telekommunikation ansågs arbeta mest med av de fyra förmågorna. Även räddningstjänst arbetar med återhämtning i relativt hög grad. Analysen tyder således på att återhämtning är en förmåga för resiliens som samtliga kritiska infrastrukturer fokuserar sitt arbete på. Att Räddningstjänst endast i lägre grad arbetar med specifika strategier kopplade till återhämtning kan bero på att de medverkande

aktörerna bedriver operativ verksamhet. Detta gör att återställning för deras egen verksamhet efter insatser och större störningar är integrerat med deras vardagliga rutiner, vilket skulle förklara att analysen inte kunde påvisa att den kritiska infrastrukturen arbetar med detta i högre grad. Det framkom en viss skillnad i hur aktörerna inom de kritiska infrastrukturerna själva bedömer hur de arbetar jämfört med vad analysen visade. Analysen kunde påvisa att både Elförsörjning och Telekommunikation arbetar med förmågan för återhämtning i högre grad än vad aktörerna själva angett i enkäten. Däremot påvisar analysen ett arbete med förmågan för återhämtningen inom Räddningstjänst som ligger på ungefär samma nivå som aktörerna själva angett i enkäten.

Anpassning

Anpassning är en förmåga som både Räddningstjänst och Telekommunikation arbetar med i relativt hög grad, detta är dessutom den förmåga som Räddningstjänst arbetar mest med. Elförsörjning arbetar inte lika mycket med denna förmåga, och bedöms vara den förmåga som Elförsörjning arbetar minst med. Det finns en viss skillnad i hur de kritiska infrastrukturerna arbetar med anpassning. Räddningstjänst arbetar mer organisatoriskt med anpassning och är även den kritiska infrastruktur som arbetar mest med erfarenhetsutbyte i lärande syfte. För Elförsörjning kunde det inte avgöras ifall de arbetar mer tekniskt eller organisatoriskt. Telekommunikation arbetar mer tekniskt med anpassning. Det finns även en skillnad i hur aktörerna inom de kritiska infrastrukturerna själva bedömer hur de arbetar jämfört med vad analysen visar. Vid jämförelse med analysen framkom det att aktörer inom Räddningstjänst i enkäten underskattade sitt arbete med förmågan för anpassning medan aktörer inom Elförsörjning överskattade sitt arbete med förmågan. Telekommunikation bedömdes arbeta ungefär lika mycket med anpassning som aktörerna inom den kritiska infrastrukturen själva angett i enkäten.

Övergripande skillnader i arbete med resiliens mellan de kritiska infrastrukturerna

Resultatet visade att det fanns skillnader i vilka förmågor för resiliens som de kritiska infrastrukturerna fokuserade på sitt arbete på. En sammanfattning av vilka förmågor som de kritiska infrastrukturerna bedömdes arbeta med i högst respektive lägst grad presenteras i Tabell 9.

Tabell 9. Presentation av de förmågor för resiliens som de kritiska infrastrukturerna arbetar mest respektive minst med.

Kritisk infrastruktur	Förmåga för resiliens, högst arbete	Förmåga för resiliens, lägst arbete
Räddningstjänst	Anpassning	Robusthet
Elförsörjning	Förutseende och Återhämtning	Anpassning
Telekommunikation	Förutseende och Återhämtning	Robusthet

Generellt så arbetade Elförsörjning och Telekommunikation på liknande sätt för alla förmågorna för resiliens medan det i resultatet framkom att Räddningstjänst arbete skiljde sig från de andra två kritiska infrastrukturerna. Räddningstjänst bedömdes fokusera sitt arbete mest på förutseende och anpassning. Elförsörjning och Telekommunikation fokuserade sitt arbete

mest på förutseende och återhämtning. Dessutom bedömdes Elförsörjning och Telekommunikation tendera att arbeta mer med tekniska system jämfört med Räddningstjänst. Exempelvis har Elförsörjning och Telekommunikation fysiska nätverk, till skillnad från Räddningstjänst, där tekniska system spelar en viktig roll. Det som är gemensamt för alla kritiska infrastrukturerna är att de arbetade lite mindre med förmågan för robusthet och lite mer med förmågan för förutseende. Generellt svarade aktörerna för de kritiska infrastrukturerna i enkäterna att de skulle vilja arbeta mer med förmågorna för resiliens än vad de gör i dagsläget. I intervjun med respektive aktör framkom det att denna skillnad främst berodde på att aktörerna ansåg att deras arbete alltid kan bli bättre. Baserat på både detta och analysens resultat bedöms det finnas möjligheter till utveckling i arbetet med förmågorna för resiliens.

Inom varje kritisk infrastruktur framkom det likheter och skillnader mellan hur aktörerna arbetar med faktorerna. Exempelvis framkom det att de undersökta kritiska infrastrukturerna generellt arbetar mindre med robusthet, vilket visar på möjlighet till utveckling inom detta område. I de fall där aktörerna har liknande roller inom den kritiska infrastrukturen bedömdes det även finnas möjlighet till erfarenhetsutbyte mellan aktörerna. En av skillnaderna på aktörsnivå som framkom av analysen var hur Aktör A och Aktör C arbetar med robusthetsfaktorn *planer inför oönskade händelser.* Aktör C arbetar med att ta fram planer för insatser som har identifierats specifikt för deras område. För Aktör A framkom inget som kunde kopplas till att arbete med att ta fram planer för specifika insatser inom deras område. Här anses det finnas potential för erfarenhetsöverföring mellan aktörerna inom Räddningstjänst.

Kartläggningen påvisade både skillnader och likheter i hur Räddningstjänst, Eldistribution och Telekommunikation arbetar med förmågorna för resiliens och det anses därför finnas möjligheter till erfarenhetsutbyte mellan de kritiska infrastrukturerna. Erfarenhetsutbyten skulle exempelvis kunna göras gällande utformning av övningar, utformning av planer och strategier, eller metoder för att samla in och analysera information. Dock antas det finnas vissa begränsningar i hur mycket de kritiska infrastrukturerna kan lära sig av varandras arbete. Detta till följd av de olika typer av störningarna som drabbar de kritiska infrastrukturerna och de skillnader som finns mellan de funktioner som de kritiska infrastrukturerna upprätthåller. De störningar som påverkar Elförsörjning och Telekommunikation bedöms vara momentana medan störningar inom Räddningstjänst bedöms ske över en längre tid. De olika störningsförloppen bedöms vara en av de bidragande orsakerna till att de kritiska infrastrukturerna fokuserar på olika förmågor för resiliens och på olika faktorer inom respektive förmåga.

7 Diskussion

Analysen omfattade tre olika kritiska infrastrukturer; Räddningstjänst, Elförsörjning och Telekommunikation. För varje kritisk infrastruktur medverkade två till tre aktörer. I undersökningen medverkande även en aktör från den kritiska infrastrukturen Järnvägstransport, kallad Aktör I. Aktör I svarade på enkäten och intervjuades men på grund av att det endast var en aktör som representerade hela den kritiska infrastrukturen Järnvägstransport i kombination med tidsbrist gjordes bedömningen att inte ta med Järnvägstransport som kritisk infrastruktur i analysen. Från informationsinsamlingen av Aktör I förekom det vissa informationsluckor vilket gör att ytterligare information hade behövts för att kunna göra en bedömning av deras arbete med förmågorna för resiliens. Baserat på den information som var tillgänglig gick det inte att urskilja om Aktör I:s arbete fokuserade mer eller mindre på någon förmåga för resiliens.

I analysen framkom det att de kritiska infrastrukturerna Räddningstjänst, Elförsörjning och Telekommunikation fokuserade på olika förmågor för resiliens. Även om analysen påvisade att aktörerna arbetar mer eller mindre med vissa förmågor för resiliens är det viktigt att poängtera att denna metod inte mäter hur resilienta de kritiska infrastrukturerna är. Hur utveckling av arbete med en viss förmåga påverkan en kritisk infrastrukturs resiliens kan alltså inte besvaras genom detta arbete. Huruvida alla fyra förmågor för resiliens är lika viktiga för en viss kritisk infrastrukturs resiliens går alltså utanför detta arbetes ramar, men ses som ett intressant område för vidare forskning, se kapitel 8. Styrkan med metoden och analysen är att den visar hur kritiska infrastrukturer arbetar med de olika förmågorna för resiliens.

7.1 Reliabilitet, Validitet och Generalitet

Informationsinsamlingen gjordes genom enkäter, intervjuer, dokumentsökning samt mejlkontakt. I informationsinsamlingen förekom det en del osäkerheter som skulle kunna påverka resultatet. En sådan osäkerhet är att enkäten inte hann testas på testpersoner, mer än reflektioner från examensarbetets handledare, innan den skickades ut till aktörerna på grund av tidsbrist. En enkät rekommenderas att testas innan den skickas ut (Bell, 2010). Bristen av testning av enkäten innan utskick bedöms dock inte minska enkätens användningsbarhet för informationsinsamlingen. Bedömningen baseras på att enkäten utformades för att vara kort och endast ge indikationer på aktörers arbete med de olika förmågorna för resiliens, samt för att skapa ett underlag för intervjuerna. Genom intervjuerna visade det sig också att aktörerna hade förstått enkätfrågorna och kunnat ge erforderliga svar. Däremot uppkom vissa missförstånd kring begrepp så som ”resiliens” och ”störningar” men dessa kunde för det mesta redas ut under intervjun eller under efterföljande kontakt.

Informationsinsamlingen begränsades av intervjutiden som endast var cirka en timme lång. Eftersom resiliens är ett komplext koncept, och mycket av aktörernas arbete kan kopplas till begreppet, anses en intervju på cirka en timme inte vara tillräcklig för att ge en helhetsbild av en aktörs arbete med förmågorna för resiliens. Informationen från intervjuerna anses därför endast utgöra fragment av aktörernas arbete med resiliens vilket skapar en viss osäkerhet. Detta kan ha påverkat de skillnader som har framkommit i arbetet med resiliens dels mellan aktörer, dels mellan kritiska infrastrukturer. För att minska denna osäkerhet användes dokumentsökning och följdfrågor via mejl som metoder för att komplettera informationen från intervjuerna. Det anses troligt att längre intervjuer, alternativt uppföljande fördjupande intervjuer, med respektive

aktör hade gett större inblick i aktörernas arbete med ramverkets faktorer och därmed ett bredare underlag för analysen. Dessutom bygger undersökningen på intervjuer med en till två representanter per aktör. Det är möjligt att det insamlade materialet hade blivit mer täckande ifall fler representanter för respektive aktör medverkat i intervjuerna. I framtida användning av ramverket för undersökning av kritiska infrastrukturers arbete med förmågorna för resiliens uppmuntras därför att antingen hålla längre intervjuer under informationsinsamlingen, eller intervjua fler representanter för varje aktör. Eftersom undersökningen som genomförts är kvalitativ och resultaten baseras på bedömningar snarare än mätvärden så är det möjligt att andra personer hade gjort andra bedömningar än de i rapporten. För att stärka kvalitén i den kvalitativa bedömningen har varje faktor och förmåga för resiliens diskuterats ingående. För att den kvalitativa bedömningen ska kunna genomföras av andra personer har de parametrar som styrt bedömningarna av aktörernas arbete med ramverkets faktorer listats i metoden.

Vissa av de medverkande aktörerna ville inte ha med organisationens namn i rapporten. Med hänsyn till detta anonymiserades alla aktörernas namn genom att benämna aktörerna som Aktör A - Aktör H. Eftersom aktörerna velat vara anonyma har de dokument som hittats för respektive aktör inte kunnat refereras till i rapporten. I Appendix C-Appendix E anges antal och typ av dokument som använts för varje aktör samt hur dessa har hittats. För att minska osäkerheterna kring validiteten av informationen som samlades in har varje sammanställning granskats av respektive aktör. Varje aktör har därmed, utöver att godkänna innehållet, fått komma med kommentarer om eventuella missförstånd och fått möjlighet att utveckla svaren kring sitt arbete.

Ramverket för datainsamling och analys har kunnat appliceras på alla tre undersökta kritiska infrastrukturer trots de skillnader som finns angående funktion, verksamhet och störningar. Ramverket för datainsamling och analys bedöms därmed vara relativt generellt applicerbart och bör kunna användas för undersökning av förmågorna för resiliens inom flera kritiska infrastrukturer. Vid skapandet av Ramverket för datainsamling och analys har till stor del internationell litteratur använts. Ramverket för informationsinsamling och analys är således inte specifikt utformat för Sverige utan snarare utformat från ett internationellt perspektiv. Något som kan variera i internationella kontexter är till vilken grad information kan samlas in enligt rapportens metod. Ramverket för informationsinsamling och analys är inte anpassat för att det kan finnas sekretessbelagd information som skapar informationsluckor. Både lagar och normer kring sekretess kan därför påverka informationsinsamlingen och därmed även ramverkets applicerbarhet i internationella kontexter.

Vid insamling av information framkom det att aktörernas arbete ofta kunde kopplas till flera av ramverkets faktorer eftersom faktorerna ofta överlappar varandra. En förbättringsåtgärd som identifierats för att särskilja faktorerna ytterligare är att dela in fler faktorer i organisatoriska och tekniska faktorer. Faktorn ”*Har förmåga att uppmärksamma otydliga signaler och indikationer*” kunde med nuvarande formulering exempelvis innefatta både en teknisk del och en organisatorisk del. Arbetet med faktorn var dessutom ofta en kombination av hur en aktör bedömts arbeta med system för informationsinsamling och system för analys. En annan förbättringsåtgärd i ramverkets utformning är att förtydliga vad som är internt och externt arbete. Detta hade kunnat göras genom att dela upp faktorer så som ”*samarbete med andra samhällsaktörer”* i en intern del (samarbete med andra aktörer inom den kritiska infrastrukturen) och en extern del (samarbete med aktörer utanför den kritiska infrastrukturen).

I denna rapport ansågs samtliga faktorer bidra i lika hög grad till förmågorna för resiliens. Det är möjligt att det finns en hierarki mellan faktorerna, det vill säga att vissa faktorer i större utsträckning bidrar till förmågorna för resiliens än andra. Ett ytterligare förbättringsförslag för ramverket är därför att ta hänsyn till hur mycket varje faktorer anses bidra till förmågan. Vid framtida användning av ramverket rekommenderas implementeringen av dessa förbättringsåtgärder.

7.2 Diskussion av Resultaten

Detaljerad information om aktörernas aktiviteter och hur dessa kopplas till ramverkets faktorer presenteras i Appendix C-Appendix E. Informationen som presenteras i rapporten är en förkortad version av informationen i Appendix C-Appendix E. Anledningen till att inte all information från informationsinsamlingen presenteras i rapporten är de ordbegränsningar som finns för rapporten. Resultatet av undersökningen visade hur de tre kritiska infrastrukturerna Räddningstjänst, Elförsörjning och Telekommunikation arbetar med förmågorna för resiliens och vilka förmågor som de kritiska infrastrukturerna arbetar mest respektive minst med. Räddningstjänst arbetar mest med anpassning och minst med robusthet. Elförsörjning arbetar mest med förutseende samt återhämtning och minst med anpassning. Telekommunikation arbetar mest med förutseende samt återhämtning och minst med robusthet. Resultatet visade även att det fanns skillnader i hur de kritiska infrastrukturerna fördelade sitt arbete mellan organisatoriska och tekniska faktorer. Skillnaden kan dock endast ses på faktornivå, och alltså inte för förmågor. Elförsörjning och Telekommunikation arbetar lika mycket med organisatoriska som tekniska faktorer för samtliga förmågor för resiliens, men bedömdes fokusera stora delar av sitt arbete på tekniska metoder. Genom dessa resultat går det att öka förståelsen för hur kritiska infrastrukturer arbetar med resiliens i verkligheten. Resultaten bedöms kunna användas för att detektera styrkor och svagheter i kritiska infrastrukturers arbete med resiliens och därigenom utveckla arbetet med förmågorna för resiliens. Ramverket bedöms ge viktiga indikationer på hur kritiska infrastrukturer arbetar med resiliens, även fast det finns förbättringspotential (se kapitel 7.1 Reliabilitet, Validitet och Generalitet).

För vissa förmågor hade aktörerna inom de kritiska infrastrukturerna värderat sitt arbete antingen högre eller lägre än det som analysens resultat påvisat. Detta kan bero på att konceptet resiliens inte har en vedertagen definition (e.g. MSB, 2013a; Rød & Johansson, 2020; OECD, 2019; DHS, 2013) och därför kan uppfattningen om innebörden av förmågorna för resiliens variera hos aktörerna. Exempelvis var en del av det som aktörer inom Telekommunikation själva ansåg bidra till förmågan för robusthet något som i rapportens analys bedömdes bidra till förmågan för anpassning. Variationen i kritiska infrastrukturers arbete med förmågorna för resiliens anses delvis bero på skillnaden i deras funktion, verksamhet och vilka slags störningar som de arbetar med. Det är även möjligt att aktörer bedriver arbete som, enligt rapportens definition, bidrar till resiliens men som aktörerna själva inte kopplar till resiliens utan endast ser som en del av deras verksamhet. Detta kan liknas vid att resiliens ses som en ingående egenskap som framträder ur de aktiviteter som bedrivs (Becker, 2014; Park, Seager, Convertino, & Linkov, 2013). Aktör C gav exempelvis feedback på utskicket av sammanställningen att de själva anser att arbete kring insatser endast är en del av deras verksamhet och därmed inte bör kopplas till förmågorna för resiliens. Räddningstjänst funktion, ”att vid olyckor och överhängande fara för olyckor hindra och begränsa skador på människor,

egendom eller miljön”, innebär att arbete kopplat till insatsförmågan hos Aktör C bidrar till att aktören kan leverera funktionen, och därmed bidrar till den kritiska infrastrukturens resiliens.

Tidigare publikationer som hittats inom området syftar främst till att mäta resiliens inom kritiska infrastrukturer (Francis & Bekera, 2014; Axelsdóttir & Bjärenstam Jonason, 2018; Ouyang & Wang, 2015). Detta arbete undersöker enbart hur kritiska infrastrukturer arbetar med konceptet resiliens genom ett kvalitativt ramverk för datainsamling och analys. Arbetet ger konkreta förslag på hur kritiska infrastrukturer kan arbeta med resiliens genom ramverkets faktorer. Något som liknar den kartläggning och analys som har gjorts i detta arbete har inte hittats i tidigare litteraturer och anses därför vara unikt. Detta försvårar jämförelse av rapportens resultat med tidigare studier. Den rapport som anses vara mest jämförbar är NIAC (2010), som kartlägger bland annat hur elförsörjningen i USA arbetar med resiliens. Däremot finns det fortfarande skillnader i hur kartläggningen i NIAC och i denna rapport genomförts vilket gör att resultaten inte enkelt kan jämföras. De likheter som ändå går att utskilja mellan rapporterna är att förmågorna för resiliens har beskrivits genom kritiska infrastrukturers aktiviteter. Vidare är det en överstämmelse i resultatet kring att det finns utvecklingsmöjligheter angående informationsutbytet mellan Elförsörjningen och andra samhällsaktörer.

8 Förslag på vidare arbete

I kapitel 4 Ramverk så identifierades säkerhetskultur som en viktig faktor som kan påverka kritiska infrastrukturers arbete med resiliens. Att undersöka hur säkerhetskulturen ser ut inom kritiska infrastrukturer skulle troligtvis ge en större inblick i kritiska infrastrukturers arbete med resiliens. Säkerhetskulturens betydelse för kritiska infrastrukturers arbete med resiliens är utanför ramen för detta arbete men anses vara ett område med potential för vidare arbete.

Under arbetets gång har det inte hittats något etablerat ramverk som används för att jämföra kritiska infrastrukturer på nationell nivå. Ett sådant ramverk skulle kunna bidra till att skapa en bättre förståelse för hur kritiska infrastrukturer i olika länder arbetar med resiliens och skapa möjligheter att dra lärdomar av varandras arbete. Detta arbete har endast undersökt och jämfört tre kritiska infrastrukturers arbete med resiliens i Sverige. Genom att fortsätta arbetet skulle det framtagna Ramverket för datainsamling och analys potentiellt kunna användas för att jämföra hur kritiska infrastrukturer arbetar med förmågor för resiliens både inom Sverige såväl som på internationell nivå.

Vid analys av insamlad information från aktörerna inom Räddningstjänst, Elförsörjning och Telekommunikation framkom det att de kritiska infrastrukturerna arbetar med beroenden som finns mellan dem och andra kritiska infrastrukturer. Detta framkom exempelvis genom att det finns reservkraftverk inom de kritiska infrastrukturerna Räddningstjänst och Telekommunikation för att undvika störningar orsakade av bortfall av elektricitet. Beroenden mellan kritiska infrastrukturer och hur dessa påverkar säkerheten inom kritiska infrastrukturer är något som lyfts fram i bland annat EPCIP (European Comission, 2019; Council Directive 2008/114/EC, 2008). Beroende mellan kritiska infrastrukturer ligger utanför ramarna för detta arbete men det framkom ändå under undersökningen att detta är något som påverkade de kritiska infrastrukturernas arbete med förmågorna för resiliens. Förslag på vidare arbete är därför att undersöka hur beroenden mellan kritiska infrastrukturer ser ut och hur detta påverkar hur kritiska infrastrukturer arbetar med förmågorna för resiliens.

Ramverket för datainsamling och analys är framtaget för att undersöka hur kritiska infrastrukturer arbetar med förmågorna för resiliens. Arbetet kan därför ses som ett komplement till undersökningar med fokus på att mäta resiliens inom kritiska infrastrukturer, så som de empiriska resilienskurvor som togs fram i ett tidigare examensarbete av Axelsdóttir och Bjärenstam Jonason (2018). I denna rapport var den initiala tanken att resilienskurvorna för de kritiska infrastrukturerna baserat på empiriska avbrottsdata skulle jämföras med rapportens resultat. Detta var dock något som tyvärr hamnade utanför ramarna för arbetet på grund av tidsbrist. Förslag på vidare arbete är således att kartlägga flera kritiska infrastrukturer och analysera ifall det finns en koppling mellan arbetet med förmågorna för resiliens och hur de kritiska infrastrukturernas empiriska resilienskruvor ser ut. Det hade även varit intressant att undersöka om vissa förmågor är viktigare för en kritisk infrastrukturs resiliens som helhet. Eftersom detta arbete inte undersöker egenskapen resiliens hos kritiska infrastrukturer, utan endast hur kritiska infrastrukturer arbetar med de fyra förmågorna för resiliens, anses detta vara ett intressant område för vidare arbete.

9 Slutsatser

Nedan besvaras rapportens frågeställningar utifrån arbetets resultat och diskussion.

Vad är kritisk infrastruktur resiliens och vilka är de mest grundläggande förmågor som resiliens består av i denna kontext?

Resiliens är en egenskap hos en kritisk infrastruktur att upprätthålla sin önskade funktion eller minimera funktionsbortfall vid störningar genom förmågan att vara förutseende, vara robust, ha en effektiv återhämtning och vara anpassningsbar. Förutseende avser att detektera, analysera och planera för framtida händelser och eventuella konsekvenser som kan negativt påverka funktionen. Robusthet avser att stå emot störningar och absorbera en eventuell chock för att minimera negativ påverkan på funktionen. Återhämtning avser att vid en större störning snabbt och effektivt återgå till ett tillstånd där funktionen återigen upprätthålls. Anpassning avser att förändras, utvecklas och dra lärdomar av tidigare händelser för att upprätthålla infrastrukturens funktion.

Hur kan förmågor för resiliens undersökas inom olika kritiska infrastrukturer?

För varje förmåga för resiliens har ett flertal faktorer identifierats i rapportens ramverk för datainsamling och analys. Genom att samla in information med hjälp av enkät, intervju, mejl och dokument kan en kritisk infrastrukturs arbete med förmågorna för resiliens kartläggas genom ramverkets faktorer. Kartläggningen beskriver hur respektive kritisk infrastruktur arbetar med respektive förmåga för resiliens.

Hur arbetar olika kritiska infrastrukturer med förmågor för resiliens och vilka förmågor fokuserar de på?

De kritiska infrastrukturerna arbetar mer eller mindre med alla fyra förmågor för resiliens. Hur de kritiska infrastrukturerna arbetar med förmågorna för resiliens varierar. Arbetet kan vara antingen fokuserat på de organisatoriska faktorerna eller de tekniska faktorerna inom varje förmåga för resiliens. Räddningstjänst arbetar mest med förmågan för anpassning. Elförsörjning och Telekommunikation arbetar mycket tekniskt och båda de kritiska infrastrukturerna arbetar mest med förmågan för förutseende och förmågan för återhämtning.

Finns det potentiellt utrymme till utveckling avseende enskilda kritiska infrastrukturers arbete med förmågor för resiliens?

Det går att se områden där enskilda kritiska infrastrukturer kan utveckla sitt arbete med förmågorna för resiliens. Exempelvis visade analysen att det finns utrymme för samtliga analyserade kritiska infrastrukturer att utveckla sitt arbete med förmågan för robusthet. Denna rapport mäter dock inte hur resilient en kritisk infrastruktur är utan visar enbart hur kritiska infrastrukturer arbetar med förmågorna för resiliens. Därför går det inte att bedöma hur en förändring i arbetet med förmågorna för resiliens hos kritiska infrastrukturer förändrar deras resiliens som helhet.

Finns det potentiellt möjlighet till överföring av erfarenheter mellan kritiska infrastrukturer avseende förmågor för resiliens?

Det utvecklade ramverket för datainsamling och analys gör det möjligt att jämföra hur olika kritiska infrastrukturers arbetar med förmågorna för resiliens vilket skapar en möjlighet för de kritiska infrastrukturerna, och aktörerna inom de kritiska infrastrukturerna, att lära sig av varandra. Det anses främst finnas möjligheter till att kritiska infrastrukturer lär sig av varandra gällande de metoder och system som de olika kritiska infrastrukturerna arbetar med. Erfarenhetsutbyte mellan kritiska infrastrukturer bedöms dock försvåras av skillnaderna i hur de kritiska infrastrukturernas funktion påverkas av störningar. Erfarenhetsutbytet anses ha potential att bidra till att kritiska infrastrukturer utvecklar sitt arbete med förmågorna för resiliens.

10 Litteraturförteckning

Akselsson, R. (2014). *Människa, teknik, organisation och riskhantering.* Lund: KFS i Lund AB.

Alexander, D. (2013). *Resilience and disaster risk reduction: an etymological journey.* London, UK: Institute of Risk and Disaster Reduction, University College London.

Australian Government. (2015). *Critical Infrastructure Resilience strategy: Plan.* Canberra: Australian Government.

Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability Engineering and System Safety 92(6)*, 745-754.

Aven, T. (2019). The Call for a Shift from Risk to Resilience: What Does it Mean. *Risk Analysis, 39(6)*, ss. 1196-1203.

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research, Vol.12, No.1*, 1-11.

Aven, T., Ben-Haim, Y., Boje Andersen, H., Cox, T., López Droguett, E., Greenberg, M., . . . Zio, E. (2018). *Society for Risk Analysis Glossary.* Society for Risk Analysis.

Axelsdóttir, E., & Bjärenstam Jonason, R. (2018). *Critical Infrastructure Resilience - Comparing Swedish infrastructures based on interruption data.* Lund: LTH, Lunds Universitet.

Becker, P. (2014). *Sustainability Science: Managing Risk and Resilience for Sustainable Development.* Amsterdam and Oxford: Elsevier.

Bell, J. (2010). *Doing Your Research Project: A Guide for First Time Researchers in Education, Health and Social Science.* Maidenhead, Berkshire, UK: Open University Press.

Bergström, J., Uhr, C., & Frykmer, T. (2016). A Complexity Framework for Studying Disaster Response Management. *Journal of Contingencies & Crisis Management. Sep2016, Vol. 24 Issue 3*, p124-135.

Boin, A., & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies & Crisis Management. Mar2007, Vol. 15 Issue 1*, 50-59.

Brodie, M., Weltzien, E., Altman, D., Blendon, R. J., & Benson, J. M. (2006). Experiences of Hurricane Katrina Evacuees in Houston Shelters: Implications for Future Planning. *American Journal of Public Health, Vol. 96 Issue 8*, 1402-1408.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., Thomas, O. D., Andrei, R. M., . . . von Winterfeldti, D. (2003). *A framework to quantitatively assess and enhance the seismic resilience of communities.* Eathquake spectra, 19(4), 733-752.

Cambell, S. (2005). Determining overall risk. *Journal of Risk Research, Vol. 8 Issue 7/8*, 569-581.

Center for chemical process safety. (1995). *Guidlines for Hazard Evaluations Procedures-Second Edition with Worked Examples, 2nd ed.* New York: American Institute of Chemical Engineers.

Commision of the European Communities. (2006). *Communication from the Commission: on a European Programme for Critical Infrastructure Protection* . Bryssel: Commision of the European Communities.

Council Directive 2008/114/EC. (2008). *On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* http://data.europa.eu/eli/dir/2008/114/oj: Council of the European Union.

DHS. (2013). *NIPP 2013 - Partnering for Critical Infrastructure Security and Resilience.* USA: Department of Homeland Security.

Esri Sverige. (den 19 november 2020). *esri Sverige*. Hämtat från Vad är GIS?: https://www.esri.se/sv-se/what-is-gis/overview [Hämtad 20 december 2020]

European Comission. (2019). *Commission Working Staff Document: Evaluation of Council Directive 2008/114 on the Identification and Designation of European Critical*

Infrastructures and the Assessment of the Need to Improve Their Protection. Bryssel: European Comission.
Fox, W. M. (1995). Sociotechnical System Principles and Guidlines: Past and Present. *Journal of applied behavioral science, Vol. 31, No 1,* 91-105.
Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety, 121,* 90-103.
Fritzon, Å., Ljungkvist, K., Boin, A., & Rhinard, M. (2007). Protecting Europe's Critical Infrastructures: Problems and Prospects. *Journal of Contingencies & Crisis Management, Vol. 15 Issue 1,* p30-41.
History.com Editors. (2019). *Hurricane Katrina*. Hämtat från History.com: https://www.history.com/topics/natural-disasters-and-environment/hurricane-katrina#section_5 [Hämtad 02 november 2020]
Holling, C. (1973). *Resilience and stability of ecological systems.* Vancouver, Canada: Institute of Resource Ecology, University of British Columbia.
Johansson, J., Hassel, H., & Zio, E. (2013). *Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems.* Reliability Engineering and System Safety, 120, 27-38.
Lessin, T., & Deal, C. (Regissörer). (2008). *Trouble the water* [Film].
Little, R. G. (2003). Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems . *36th Annual Hawaii International Conference on System Sciences* (ss. 1-9). Los Alamitos, CA, USA: IEEE.
MSB. (2011). *Skydd av samhällsviktig verksamhet - MSB:s redovisning av en samlad nationell strategi för skydd av samhällsviktig verksamhet.* Myndigheten för samhälsskydd och beredskap.
MSB. (2013a). *Handlingsplan för skydd av samhällsviktig verksamhet.* Myndigheten för samhällsskydd och beredskap.
MSB. (2013b). *Resiliens, Begreppets olika betydelser och användningsområden.* Myndigheten för samhällsskydd och beredskap.
MSB. (2014). *Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure.* Karlstad: Myndigheten för samhällsskydd och beredskap.
MSB. (2016). *Faktablad: Samverkansområdet Teknisk Infrastruktur (SOTI).* Karlstad: MSB Publ.nr: MSB751.
MSB. (2018a). *Gemensamma grunder för samverkan och ledning vid samhällsstörningar.* Myndigheten för samhällsskydd och beredskap.
MSB. (2018b). *Om krisen eller kriget kommer.* Karlstad: Mydigheten för samhällsskydd och beredskap.
MSB. (2019). *Vägledning för identifiering av samhällsviktig verksamhet.* Karlstad: Myndigheten för samhälsskydd och beredskap.
MSB. (2020a). *Fördjupning om kontinuitetsplan.* Myndigheten för samhällsskydd och beredskap, Publ.nr MSB1507.
MSB. (2020b). *Kontinuitetshantering*. Hämtat från Myndigheten för samhällsskydd och beredskap: https://www.msb.se/kontinuitetshantering [Hämtat 22 september 2020]
MSB. (2020c). *NIS-direktivet*. Hämtat från Myndigheten för samhällsskydd och beredskap: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/ [Hämtad 06 december 2020]
MSB. (2020d). *Uppdaterad information samhällsviktig verksamhet.* Karlstad: Myndigheten för samhällsskydig verksamhet. Hämtat från Myndigheten för samhällsskydd och beredskap.
MSB. (2020e). *Övergripande statistik*. Hämtat från Myndigheten för samhälsskydd och beredskap: https://ida.msb.se/ida2#page=2b3dc9ff-12fe-4c4d-a8f1-863a95d215a6 [Hämtad 12 december 2020]

NE. (2020a). *Risk*. Hämtat från Nationalencyklopedin: https://www.ne.se/uppslagsverk/encyklopedi/enkel/risk [Hämtad 20 december 2020]
NE. (2020b). *Telekommunikation*. Hämtat från Uppslagsverket: https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/telekommunikation [Hämtad 20 december 2020]
NIAC. (2010). *A Framework for Establishing Critical Infrastructure Resilience Goals.* USA: National Infrastructure Advisory Council.
Novotek Group. (2020). *Framtidens HMI/SCADA redan idag*. Hämtat från NOVOTEK: https://www.novotek.com/sv/l-sningar/hmi-scada/ [Hämtad 07 oktober 2020]
OECD. (2019). *Good Governance for Critical Infrastructure Resilience.* OECD Reviews of Risk Management Policies, OECD Publishing, Paris. https://doi.org/10.1787/02f0e5a0-en.
Ouyang, M., & Wang, Z. (2015). *Resilience assessment of independent infrastructure systems: With a focus on joint restoration modeling and analysis.* Reliability Engineering and System Safety, 141, 74-82.
Park, J., Seager, T. P., Convertino, M., & Linkov, I. (2013). *Integrating Risk and Resilience Approaches to Catastrophe Managent in Engineering System.* Risk Analysis, 3(3).
Persson, A. (2016). *Frågor och svar om frågekonstruktion i enkät- och intervjuundersökningar.* Stockholm: Statistiska centralbyrån.
Quyang, M., Duenas-Osorio, L., & Min, X. (2012). A three-stage resilience analysis frameworkfor urban infrastructure systems. *Structural Safety, 36*, ss. 23-31.
Räddningsverket. (2003). *Handbok för riskanalys.* Räddningsverket.
Rød, B., & Johansson, J. (2020). *Critical infrastructures - How resilient are they?* Not yet published. Manuscript to be submitted for possible publication in an international journal.
SCB. (2020). *Elektricitet i Sverige*. Hämtat från Statistiska centralbyrån: https://www.scb.se/hitta-statistik/sverige-i-siffror/miljo/elektricitet-i-sverige/ [Hämtad 05 december 2020]
SFS 2003:778. (u.d.). *Lag om skydd mot olyckor.* Justitiedepartementet. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2003778-om-skydd-mot-olyckor_sfs-2003-778 [Hämtad 04 december 2020].
Shirali, G., Mohammadfam, I., & Ebrahimipour, V. (2013). *A new method for quantitative assessment of resilienec engineering by PCA and NT approach: A case study in a preocess industry.* Reliability Engineering and System Safety, 119, 88-94.
Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *The Electricity Journal Volume 30, Issue 3*, 30-35.
Telenor. (2020). *Telekom*. Hämtat från Telenor: https://www.telenor.se/foretag/ordlista/telekom/ [Hämtad 20 december 2020]
UNDRR. (2020). *Resilience*. Hämtat från UNDRR: https://www.undrr.org/terminology/resilience [Hämtad 09 september 2020]
van de Wiel, M. (2017). *Emaining expertise using interviews and verbal protocols.* Frontline Learning Research, 5(3), 112 - 140.
Walker , J., & Cooper, M. (2011). *Genealogies of resilience: From systems ecology to the political economy of crisis adaptation.* Security Dialogue, 42(2), 143-160.
Wood, D. (2015). *Four concepts for resilience and the implications for the future of resilience engineering* . Reliability Engineering and System Safety, doi:http://dx.doi.org/10.1016/j.ress.2015.03.018i.

Appendix A- Sammanställning av definitioner för resiliens

Definition	Nyckeltermer (orginal)	Referenser
”*Förmåga i samhället att förebygga, motstå, hantera och återhämta sig.*”	• Förebyggande • Motstå • Återhämtning	(MSB, 2013a, s. 5)
“*…the following four aspects to describe resilience could be discerned: anticipation, robustness, recovery, and adaptation*”	• Förutseende (anticipation) • Robusthet (robustness) • Återhämtning (recovery) • Anpassning (adaptation)	(Rød & Johansson, 2020, s. 3)
“*Resilience can be defined as the capacity of critical infrastructure to absorb a disturbance, recover from disruptions and adapt to changing conditions, while still retaining essentially the same function as prior to the disruptive shock*”	• Robusthet (robustness) • Redundans (redundancy) • Resursrikhet (resourcefulness) • Anpassning (adaptability)	(OECD, 2019, s. 36)
“*Resilience here refers to the capability to ‘bounce back’ after a break- down.*”	• Återhämtning (bounce-back)	(Fritzon, Ljungkvist, Boin, & Rhinard, 2007, s. 40)
“*For purposes of this discussion, community seismic resilience is defined as the ability of social units (e.g., organizations, communities) to mitigate hazards, contain the effects of disasters when they occur, and carry out recovery activities in ways that minimize social disruption and mitigate the effects of future earthquakes.*”	• Robusthet (robustness) • Redundans (redundancy) • Resursrikhet (resourcefulness) • Snabbhet (rapidity)	(Bruneau, o.a., 2003, s. 735)
“*The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions...[it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.*”	• Förebygga (prepare) • Anpassning (adapt) • Återhämtning (recover) • Motstå (withstand)	(DHS, 2013, s. 7)
“*The capability of a strained body to recover its size and shape after deformation; an ability to recover from or adjust easily to misfortune or change*”	• Återhämtning (recover) • Anpassning (adapt)	(Little, 2003, s. 6)
“*…resilience is an endowed or enriched property of a system that is capable of effectively combating (absorbing,*	• Förutseende och absorption (anticipate/absorb)	(Francis & Bekera, 2014, ss. 91-92)

adapting to or rapidly recovery from) disruptive events. The resilience approach emphasizes an assessment of the system's ability to (i) anticipate and absorb potential disruptions; (ii) develop adaptive means to accommodate changes within or around the system; and (iii) establish response behaviors aimed at either building the capacity to withstand the disruption or recover as quickly as possible after an impact."	• Anpassning (adapting) • Återhämtning (rapidly recovery/respons behaviors)	
"*Resilience is an emergent property determined by the ability of the human–environment system to anticipate, recognize, adapt to and learn from variations, changes, disturbances, disruptions and disasters that may cause harm to what human beings value. Resilience is in other words a means to reach the ends of safety and sustainability*"	• Förutseende (anticipate) • Igenkänning (recognize) • Anpassning (adapt) • Lärande (learn)	(Becker, 2014, s. 146)
"*Ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.*"	• Förutseende (ability to anticipate) • Absorption (ability to absorb) • Anpassning (ability to adapt) • Återhämtning (ability to recover)	(NIAC, 2010, s. 15)
"*…resilience as the joint ability of infrastructure systems to resist (prevent and withstand) any possible hazards absorb the initial damage, and recover to normal operation.*"	• Motstå (ability to resist) • Absorption (ability to absorb) • Återhämtning (ability to recover)	(Quyang, Duenas-Osorio, & Min, 2012, s. 23)
"*The ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management.*"	• Motstå (resist) • Absorption (absorb) • Hantera (accommodate) • Anpassning (adapt) • Förändring (transform) • Återhämtning (recover) • Bevarande (preservation)	(UNDRR, 2020)

Appendix B- Enkätformulär

Resiliens inom Kritisk Infrastruktur Examensarbete LTH, Lunds Universitet

Den här enkäten är en del av informationsinsamlingen till vårt examensarbete där vi undersöker vi hur kritiska infrastrukturer i Sverige arbetar med resiliens. Examensarbetet skrivs på avdelningen för riskhantering och samhällssäkerhet och är en del av forskningen som bedrivs inom centrumbildningen CenCIP vid Lunds Universitet (www.cencip.lu.se).

All information kommer sammanställas och publiceras i examensarbetets rapport. Information från enkäterna som publiceras i rapporten kommer dock inte att kunna härledas till enskilda individer. Informationen kommer ej heller att hanteras av externa personer. Ni kan vid vilken tidpunkt som helst välja att avsluta medverkan i enkätundersökningen. Vid eventuella frågor tveka inte att kontakta oss på bas14sa1@lu.se eller bra15fkl@lu.se. Detta gäller även ifall ni vill avbryta medverkan eller återkalla ett svar då enkäten redan är inskickad. Vid intresse och möjlighet kommer enkäten att följas upp med en kortare intervju (cirka 1 timme).

Enkäten tar ca 10 minuter, de öppna frågorna besvaras i mån av tid.

Tack för din medverkan!

Med vänlig hälsning
Stina Andersson och Felicia Klint
* Required

1. Namn på er organisation *

2. Godkänner ni att er organisations namn anges i examensarbetets rapport?

   Mark only one oval.

   - ◯ Ja
   - ◯ Nej (endast samhällssektorn kommer anges)

3. Ditt/era primära ansvarsområde(n) inom organisationen (exempelvis säkerhet, HR, utbildning) *

Övergripande frågor

4. Vad avser er organisation med termen resiliens?

5. Vad är det som er verksamhet levererar till samhället, dvs. er huvudsakliga funktion, och hur mäter ni hur väl ni uppfyller denna funktion?

Vår definition på resiliens

I vårt arbete avser resiliens i stort en kritisk infrastrukturs förmåga att upprätthålla sin önskade funktion eller minimera funktionsbortfall vid störningar genom fyra förmågor:

1) Förutseende: förmågan att detektera, analysera och planera för framtida händelser och eventuella konsekvenser som kan negativt påverka funktionen.
2) Robusthet: förmågan att stå emot störningar och absorbera en eventuell chock för att minimera negativ påverkan på funktionen.
3) Återhämtning: förmågan att vid en större störning snabbt och effektivt återgå till ett tillstånd där funktionen återigen upprätthålls.
4) Anpassning: förmågan att förändras, utvecklas och dra lärdomar av tidigare händelser för att upprätthålla infrastrukturens funktion.

Följande frågor behandlar hur er organisation arbetar med dessa fyra förmågor.

Förutseende

Förmågan att detektera framtida händelser och eventuella konsekvenser som kan skada samhällsfunktionen.

6. Till vilken grad arbetar er organisation med att vara förutseende? *

Mark only one oval.

	1	2	3	4	5	6	
Inte alls	◯	◯	◯	◯	◯	◯	Väldigt mycket

7. Till vilken grad skulle er organisation vilja arbeta med att vara förutseende? *

Mark only one oval.

	1	2	3	4	5	6	
Inte alls	◯	◯	◯	◯	◯	◯	Väldigt mycket

8. Hur arbetar er organisation för att vara förutseende, t.ex. vilka metoder/verktyg använder ni eller vilka processer har ni på plats?

Robusthet

Förmågan att stå emot störningar och absorbera en eventuell chock.

9. Till vilken grad arbetar er organisation med att vara robust? *

Mark only one oval.

	1	2	3	4	5	6	
Inte alls	◯	◯	◯	◯	◯	◯	Väldigt mycket

10. Till vilken grad skulle er organisation vilja arbeta med robusthet? *

Mark only one oval.

	1	2	3	4	5	6	
Inte alls	◯	◯	◯	◯	◯	◯	Väldigt mycket

11. Hur arbetar er organisation för att vara robust, t.ex. vilka metoder/verktyg använder ni eller vilka processer har ni på plats?

Återhämtning

Förmågan att vid en större störning snabbt och effektivt återgå till ett tillstånd där samhällsfunktionen upprätthålls.

12. Till vilken grad arbetar er organisation med att ha en effektiv återhämtning efter en större störning? *

Mark only one oval.

	1	2	3	4	5	6	
Inte alls	◯	◯	◯	◯	◯	◯	Väldigt mycket

13. Till vilken grad skulle er organisation vilja arbeta med att ha en effektiv återhämtning efter en större störning? *

Mark only one oval.

	1	2	3	4	5	6	
Inte alls	◯	◯	◯	◯	◯	◯	Väldigt mycket

14. Hur arbetar er organisation för att kunna ha en effektiv återhämtning, t.ex. vilka metoder/verktyg använder ni eller vilka processer har ni på plats?

Anpassning

Förmågan att förändras, utvecklas och dra lärdomar av tidigare händelser för att upprätthålla infrastrukturens samhällsfunktion.

15. Till vilken grad arbetar er organisation med anpassningsförmåga? *

Mark only one oval.

	1	2	3	4	5	6	
Inte alls	◯	◯	◯	◯	◯	◯	Väldigt mycket

16. Till vilken grad skulle er organisation vilja arbeta med anpassningsförmåga? *

Mark only one oval.

	1	2	3	4	5	6	
Inte alls	◯	◯	◯	◯	◯	◯	Väldigt mycket

17. Hur arbetar er organisation med er anpassningsförmåga, t.ex. vilka metoder/verktyg använder ni eller vilka processer har ni på plats?

5 kortare frågor

18.

Check all that apply.

	Ja	Till större grad	Till mindre grad	Nej	Vet ej
Har ni tillräckliga system för informationsinsamling, t.ex. SCADA-system?	☐	☐	☐	☐	☐
Har ni etablerade planer för ledning och koordination vid en störning?	☐	☐	☐	☐	☐
Har ni kontinuitetsplaner?	☐	☐	☐	☐	☐
Har ni ett samarbete med andra aktörer inom området?	☐	☐	☐	☐	☐
Har ni ett erfarenhetsutbyte med andra aktörer inom området?	☐	☐	☐	☐	☐

Appendix C – Sammanställning av insamlat material för Räddningstjänst

De aktörer som undersöktes för den kritiska infrastrukturen Räddningstjänst var tre räddningstjänstförbund som arbetar inom olika geografiska områden i Sverige. En av aktörerna, Aktör B, har senare valt att hoppa av och denna aktörs sammanställning finns därför inte med i Appendix C. Representanten från Aktör A arbetade främst operativt medan representanterna från Aktör C arbetade både operativt och förebyggande, vilket kan påverka vilken information som kom fram under intervjun. För Aktör A har Gemensamma grunder av MSB (2018a) kompletterat informationsinsamlingen. Aktör A mejlade även ett verksamhetsdokument, men på grund av tidsbrist har detta inte analyserats. För Aktör C har tre verksamhetsdokument som Aktör C själva skickade ut kompletterat informationsinsamlingen. Nedan presenteras hur Aktör A och Aktör C arbetar med ramverkets faktorer inom respektive förmåga för resiliens. För att tydliggöra vilken faktor som avses i punktlistorna har faktorerna skrivits ut kursivt.

Aktör A

Förutseende

Organisatoriska faktorer

- Aktör A berättade under intervjun att deras övergripande mål att skydda samhället mot olyckor. Målet mäts genom nyckeltal så som responstid och antal olyckor. Nyckeltalen jämförs med andra aktörer inom sektorn Skydd och säkerhet för att veta hur väl målet uppfylls. Aktör A anses arbeta med *tydliga mål* som bidrar till upprätthållandet av den kritiska infrastrukturens funktionen i högre grad.
- Under intervjun förklarade Aktör A att de samlar in information från omgivningen genom exempelvis möten med andra aktörer (MSB, polisen, kommuner etcetera) samt genom kommunikation med räddningscentraler. Aktör A antas samla in information från flera olika områden inom den kritiska infrastrukturen. Aktör A bedöms därför arbeta med *organisatoriska system för insamling av information* i högre grad.
- Analys av insamlad information görs främst genom expertbedömningar. Detta framkom under intervjun där Aktör A berättade att de utbildar personal för att analysera och göra bedömningar utifrån den insamlade information. Aktör A beskrev att de går igenom händelser som kan förekomma och diskuterar hur de ska hantera denna. Eftersom Aktör A har kompetent personal som analyserar och diskuterar potentiella händelser bedöms Aktör A arbeta med *organisatoriska analysmetoder* i högre grad.
- Under intervjun bedömdes Aktör A fokusera mycket på att arbeta med risker som baserats på tidigare händelser snarare än på oväntade störningar. Detta tyder på att Aktör A inte arbetar i högre grad med att uppmärksamma otydliga signaler och indikationer för att detektera potentiella störningar. Däremot är den insamlade informationen är inte tillräcklig för att bedöma Aktör A:s förmåga att *uppmärksamma otydliga signaler och indikationer*.

Tekniska faktorer

- De tekniska system för informationsinsamling som Aktör A berättade om under intervjun är bland annat plattformen Webbaserad Informationsinsamlings System (WIS). WIS är, enligt Aktör A, en online-baserad samverkansplattform där aktörer inom den kritiska

infrastrukturen kan dela information om risker och händelseutvecklingar. Aktör A samlar även in information genom ett verksamhetsprogram, vilket Aktör A berättade om under intervjun. Verksamhetsprogrammet samlar in information om avvikelser, felanmälningar, förbättringsförslag, produktionsuppföljning, tillbud samt arbetsmiljörelaterade händelser. Eftersom Aktör A samlar in information både internt och externt bedöms Aktör A arbeta med *tekniska system för informationsinsamling* i högre grad.

- Aktören angav under intervjun att de saknar tekniska system för analys. Däremot framkom det vid mejlkontakt med Aktör A att de använder Daedalos för händelserapportering vilket även hat en analysfunktion. Aktör A bedöms därför arbeta med *tekniska system för analys* i lägre grad.

Robusthet

Organisatoriska faktorer

- Exempel på övningar kopplat till robusthet som framkom under intervjun med Aktör A är livräddningsövningar och utbildning på utrustning. Enligt Aktör A:s hemsida deltar de dessutom i samverkansövningar med andra aktörer inom sektionen Skydd och säkerhet så som räddningstjänster, polis och ambulans. Övningarna antas bidra till robustheten genom att Aktör A kan leverera sin funktion till samhället på ett mer effektivt sätt. Den tillgängliga informationen om Aktör A:s arbete med övningar kopplade till robusthet anses dock inte visa att Aktör A arbetar med faktor i högre grad. Aktör A bedöms därför arbeta med *övningar kopplat till robusthet* i lägre grad.
- De planer som Aktör A angav under intervjun som de arbetar med inför oväntade händelser var personalplanering och användande av brandvärn. Dessutom berättade Aktör A under intervjun att de arbetar med interoperabilitet vilket bedöms vara en strategi för att lättare dela resurser mellan stationer och även till andra aktörer för att förbättra funktionen. Det framkom inga planer och strategier under informationsinsamlingen som omfattar hur Aktör A ska hantera större oväntade störningar, vilket gör att Aktör A bedöms arbeta med sådana planer i mindre utsträckning. Aktör A arbetar därför med *planer för oväntade händelser* bidrar därför i lägre grad.
- Aktör A samarbetar med andra aktörer inom den kritiska infrastrukturen. Exempel som Aktör A gav under intervjun är att aktörer kan låna ut utrustning till varandra och hjälpas åt vid insatser. Samarbetet bidrar till att andra aktörer inom den kritiska infrastrukturen kan hjälpa till att bättre leverera sin funktion till samhället. Exempelvis kan aktörerna snabbare påbörja en insats ifall de har kortare framkörningstid till det drabbade området. Aktör A bedöms arbeta med *samarbete kopplat till robusthet* i högre grad.

Tekniska faktorer

- En typ av buffert som framkom under intervjun är att aktören har ett lager av drivmedel till fordonen och mindre dricksvattenreserv. Det framkom även bufferts för kommunikation, elförsörjning och internet. Systemen används för att undvika kritiska beroenden från andra kritiska infrastrukturer. Sammanlagt bedöms Aktör A arbetar med flera *bufferts* och arbetar därmed med faktorn i högre grad.
- Det framkom ett exempel kopplade till redundanta system som Aktör A använder för att upprätthålla sin funktion. Detta var att Aktör A har en överkapacitet i utryckningsfordon.

Detta var den enda som framkom som kan kopplas till redundanta system. Aktör A bedöms därför arbeta med *redundanta system eller en inbyggd redundans i systemen* i lägre grad.

Återhämtning

Organisatoriska faktorer

- Aktör A:s organisatoriska resurser består delvis av privatpersoner som aktören har utbildat för att skapa ett brandvärn, detta förklarade Aktör A under intervjun. Brandvärnet kan hjälpa till med enklare uppgifter så som att dra slang vid skogsbränder och eftersläckningsarbete så att ordinarie personal görs tillgänglig för andra insatser. Aktören har även tillgång till en IT-konsult som kan hjälpa till vid en teknisk störning. Dessa resurser anses enbart beröra mindre områden för upprätthållande av funktionen och Aktör A bedöms därför arbeta med *organisatoriska resurser* i lägre grad.
- I svaret från enkäten framkom det att det finns någon slags plan för ledning och koordination, detta är dock inget som framkom under intervjun. Aktören har alltså någon typ av *plan för ledning och koordination* men det går inte att fastställa dess omfattning eller till vilken grad Aktör A arbetar med detta.
- Det samarbete som finns med andra aktörer inom den kritiska infrastrukturen som bidrar till återhämtningsförmågan sker genom samverkansavtal. Samverkansavtal är, enligt Aktör A, att räddningstjänster hjälps åt med både organisatoriska och tekniska resurser. Samarbetet bedöms bidra till att Aktör A kan återhämtas snabbare genom att det finns extra resurser att tillgå. Aktör A bedöms därför arbeta med *samarbete kopplat till robusthet i* högre grad.
- Aktör A arbetar på flera sätt med övningar kopplat till återhämtning, detta gäller för både störningar inom verksamheten och störningar för leveransen av funktionen. Aktören förklarade under intervjun att de gör momentövningar som övar individer på bland annat analyser, lägesbilder samt att ta fram beslutsunderlag. På deras hemsida står det även att det sker flera samverkansövningar med exempelvis polisen och andra räddningstjänster samt utbildning av brandvärn. Övningarna förväntas bidra genom att snabbare kunna återgå till upprätthållande av leverans av funktionen. Aktör A arbetar därför med *samarbete kopplat till återhämtning i* högre grad.
- För att bidra till återhämtningsförmågan finns strategier och kontinuitetsplaner. Aktör A berättade dock att kontinuitetsplanerna inte är välutvecklade och därför anses Aktör A arbeta med *strategier för återhämtning* i lägre grad.

Tekniska faktorer

- Aktör A är en räddningstjänst som bland annat bedriver operativ verksamhet som har flera tekniska resurser som gör att de snabbare kan återställa sig både under och efter en insats för att återigen kunna leverera funktionen. Några av de tekniska resurser som Aktör A har för att kunna återställa leveransen av funktionen till samhället som framkom under intervjun som utryckningsfordon, den utrustning som finns på fordonen och kommunikationsutrustning som Rakel. Aktör A bedöms ha flera olika tekniska resurser för återhämtning, både av samhället och sin egen verksamhet, och bedöms arbeta med *tekniska resurser* i högre grad.

Anpassning

Organisatoriska faktorer

- Under intervjun berättade Aktör A att de gör insatsutvärderingar och försöker bygga in lärdomar från dessa i sina rutiner och arbetssätt. Det är främst linjechefer som ansvarar över att se till att de nya rutinerna följs. För rapportering har Aktör A bland annat ett verksamhetsprogram där personal kan rapportera arbetsmiljörelaterade händelser, brister och förbättringsförslag. Aktören följer även upp händelserapportering genom att återkoppla för varje rapporterat ärende. Exempel på utvärderingar som gjorts var efter skogsbränderna 2014 och 2018 där det togs gemensamma guidelines, både på regional och nationell nivå för att förbättra räddningstjänsternas arbete med bekämpning av skogsbränder. Aktören bedöms arbeta med *uppföljning och utvärdering i lärande syfte med organisatoriska system* i högre grad.
- I intervjun berättade Aktör A att de anpassar sig till nya situationer exempelvis genom att utbilda sin personal i antagonistiska hot efter att detta har identifierats som en ökande trend. Även att de försöker bygga in lärdomar i deras rutiner anses vara en förebyggande organisatorisk åtgärd. Aktör A berättade dock under intervjun att verksamheten är konservativ och att det ibland är svårt att implementera nya rutiner. Detta skulle enligt aktören kunna försvåra en hantering av en oväntad störning eller händelse. Baserat på kombinationen av att Aktör A har implementerat några åtgärder och att de själva anser att de har svårt att genomföra förändringar bedöms Aktör A arbeta med *implementering av organisatoriska åtgärder* i lägre grad.
- Det erfarenhetsutbyte som Aktör A har med andra aktörer, både inom och utanför den kritiska infrastrukturen, sker genom WIS och samverkansövningar. Aktör A bedöms arbeta med erfarenhetsutbyte med andra aktörer i högre grad.

Tekniska faktorer

- Det finns ett händelserapporteringssystem, kallad Daedalos, för att samla in information om insatser. Via rapporteringssystemet sammanställs bland annat insatsstatiskt. Insatsstatistik för Räddningstjänst finns att se på IDA (MSB, 2020e). Händelserapportering fokuserar endast på händelser som har skett och det framkom inget under intervjun som visar hur Aktör A arbetar med *uppföljning och utvärdering med tekniska system* gällande implementerade åtgärder. Därför bedöms Aktör A endast arbeta med faktorn i lägre grad.
- De tekniska åtgärder som framkom under intervjun som tidigare har implementerats är kopplade till införskaffandet av ny utrustning till följd av lärdomar från utvärderingarna. Exempelvis berättade Aktör A att de kunde använda avvikelserapporter för att identifiera om batteridrivna verktyg behöver längre batteritid för att klara en hel insats. Aktör A bedöms arbeta med *förebyggande tekniska åtgärder* i högre grad.

Aktör B

Aktör B valde att avbryta sin medverkan i examensarbetet. Sammanställningen för Aktör B har därför strukits från rapporten.

Aktör C

Förutseende

Organisatoriska faktorer

- Under intervjun berättade Aktör C att de har målen att minska antalet olyckor, deras konsekvenser samt verka för ökad trygghet. Målen följ upp i Aktör C:s delårsrapporter där de kollar på deras aktiviteter kopplade till målen. Det finns även vissa nyckeltal som används för att mäta hur väl de arbetar mot målen. Aktör C anses arbeta med *tydliga mål* som bidrar till upprätthållandet av den kritiska infrastrukturens funktionen i högre grad.
- Aktör C berättade under intervjun att de har en stabsfunktion som har ett kontaktnät där de kontinuerligt får in information från andra aktörer inom den kritiska infrastrukturen. Aktör C berättade även att de medverkar i forum med flera andra externa aktörer där de hämtar information om samhällstrender och utvecklingar. Forumen finns både på lokal- och regionalnivå. Aktör C har en räddningscentral som har en modell som används för att samla in information. Utifrån modellen samlar räddningscentralen ihop fakta om bland annat väder, vind, hotsituationer och vattennivåer. Aktör C betonade under intervjun att den största delen av deras informationsinsamling sker via kontakter. Aktör C har flera organisatoriska metoder för att samla in information och Aktör C bedöms därför arbeta med *organisatoriska system för insamling av information* i högre grad.
- Den modell som Aktör C:s räddningscentral använder för att samla in information används, enligt Aktör C, även för att analysera informationen om hur verksamheten påverkas för att dra slutsatser. En annan organisatorisk analysmetod som Aktör C berättade om under intervjun var riskstudier. Riskstudierna innebär att Aktör C använder information om samhällsförändringar för att bland annat analysera de risker som finns i medlemskommunerna. Utöver det ovanstående arbetar Aktör C med kontinuitetshantering vilket innebär att Aktör C identifierar kritiska delar inom verksamheten som behövs för att upprätthålla funktionen samt analyserar hur dessa ska skyddas oavsett vad som händer. Aktör C har flera organisatoriska system för att analyser insamlad information av varierande karaktär och Aktör C bedöms arbeta med *organisatoriska analysmetoder* i högre grad.
- Den information som framkom under intervjun anses visa att Aktör C fokuserar på att arbeta systematiskt med dels kända risker, dels faktorer som påverkar insatsförmågan, dels oväntade störningar. Däremot är den insamlade informationen inte tillräckligt detaljerad för att bedöma till vilken grad Aktör C arbetar med att *uppmärksamma otydliga signaler och indikationer*.

Tekniska faktorer

- Tekniska system för informationsinsamling som Aktör C berättade att de använder var databaser som tillhandahålls av MSB. Den information som Aktör C nämnde att de får in från MSB:s databaser var information om tidigare insatser inom den kritiska infrastrukturen. Ett annat tekniska system som används för informationsinsamling beskrivs i Aktör C:s handlingsprogram från 2020. Handlingsprogrammet beskriver att de har ett internt händelserapporteringssystem och att systemet används för att identifiera olyckor som är vanligt förekommande inom den kritiska infrastrukturen. Eftersom Aktör C använder tekniska system för att samla in både intern och extern information bedöms Aktör C arbeta med *tekniska system för insamling av information* i högre grad.

- Under intervjun framkom det inget tekniskt system som används för att analysera information. När analysmetoder diskuterades under intervjun var det endast organisatoriska metoder som beskrevs. Det framkom inte ifall Aktör C arbetar med tekniska analysmetoder men eftersom det inte kom upp under intervjun bedöms Aktör C inte arbeta med denna faktor i högre grad. Utifrån given information går det inte att bedöma huruvida Aktör C arbetar med *tekniska system för analys* i lägre grad eller inte alls.

Robusthet

Organisatoriska faktorer

- Aktör C anser själva att de inte arbetar med större övningar kopplat till robusthet i större utsträckning eftersom de inte anser att sådana större övningar bidrar till deras resiliens. Dock framkom det att de kontinuerligt övningar på ”vardagliga” moment så som rökdykning, simning, livräddning och trafikolyckor. Dessa övningar bedöms bidra till aktörens förmåga att leverera sin funktion genom att skador på människa, egendom och miljö begränsas. Eftersom Aktör C själva uttryckte att de inte arbetar med större *övningar kopplat till robusthet* i någon större utsträckning bedöms Aktör C endast arbeta med faktor i lägre grad.
- Under intervjun förklarade Aktör C att hela deras verksamhet går ut på att ha planer och vara beredda på vad som än händer för att de ska kunna upprätthålla funktionen. En plan som Aktör C berättade om var att de planerar för att det alltid ska finnas personer på plats. Ifall det sker en störning kan personal snabbt omfördelas för att hjälpa till på de kritiska områdena som identifierats inom verksamheten. Planen bedöms göra att Aktör C kan använda sin personal och kompetenser effektivt under störningar. En annan plan Aktör C berättade om är att de har larmplaner vilket, enligt Aktör C:s handlingsprogram från 2020, är planer för att underlätta utalarmering vid insatser. I Aktör C:s handlingsprogram från 2020 beskrivs det dessutom att det finns flera planer för specifika händelser och att dessa planer behandlar hur insatser ska genomföras. Eftersom Aktör C har flera planer som berör insatser men även för att upprätthålla verksamheten oavsett vad som inträffar, så bedöms Aktör C arbeta med *planer för oväntade händelser* i högre grad.
- Aktör C berättade under intervjun att de kan låna personal och utrustning av andra räddningstjänster ifall det skulle behövas för att klara av en insats. Detta förbättrar insatsförmågan inom den kritiska infrastrukturen vilket förbättrar leveransen av funktionen. I Aktör C:s handlingsprogram från 2020 framkommer det att Aktör C har samverkansavtal med flera aktörer som på olika sätt förbättrar insatsförmågan inom den kritiska infrastrukturen. Eftersom tillgång till personal och utrustning anses vara en viktig del för att upprätthålla funktionen inom den kritiska infrastrukturens funktion bedöms Aktör C arbeta med *samarbete kopplat till robusthet* i högre grad.

Tekniska faktorer

- Den buffert som Aktör C berättade om under intervjun var att de har reservtankar kopplade till reservkraftverken. Aktör C nämnde även att de infört bufferts för de system som avses vara kritiska för deras funktion. Exempelvis har de dubbla matningar i telekommunikation. På vissa stationer finns det även kraftverk som går på automatiskt vid elavbrott. De exempel som gavs anses vara kopplade till beroenden till andra kritiska infrastrukturer och blir

därmed en buffert för Aktör C. *Bufferts* är en faktor som Aktör C bedöms arbeta med i högre grad.

- Under intervjun framkom det inte vilka redundanta system som finns hos Aktör C inom deras egen verksamhet. Det går därför inte att bedöma till vilken grad Aktör C arbetar med *redundanta system eller en inbyggd redundans i systemen.*

Återhämtning

Organisatoriska faktorer

- För att återhämta personalen efter en insats har Aktör C stödgrupper för insatspersonal. Aktör C berättade även att de har resurser i form av experter på ett företagshälsovårdsperspektiv. Återhämtning för personal är viktigt eftersom frisk personal är viktigt för den kritiska infrastrukturens möjlighet att upprätthålla funktionen. Under intervjun nämnde Aktör C att de har resurser i form av ”allt från utrustning till personal”. Detta anse vara något som tyder på att det kan finnas fler organisatoriska resurser inom aktörens verksamhet. Under intervjun fanns det dock inte tid att gå in djupare på detta och det kan därför inte göras en bedömning till vilken grad Aktör C arbetar med *organisatoriska resurser för återhämtning*.
- Under intervjun förklarade Aktör C att de hoppas på att resurser delas mellan aktörer vid en händelse men att de inte finns etablerade planer för detta utan att *’’var och en tittar på detta för sig själv’’*. Det som Aktör C berättade under intervju tolkas som att resurser endast kan fördelas genom samarbete mellan aktörer inom den kritiska infrastrukturen. Samarbete kan bidra till återhämtning, men anses inte vara en *plan för ledning och koordination av resurshantering* som bidrar till leveransen av funktionen. Aktör C bedöms därför endast arbeta med faktorn i lägre grad.
- Under intervjun med Aktör C berättade aktören att de samverkar på bemanningsnivå, kan låna både tekniska och organisatoriska resurser av varandra samt att ett annat förbund kan gå in och täcka ett område när Aktör C återställer sig efter en insats. Ett annat exempel som Aktör C gav på samverkan mellan aktörer var när de hjälpte till med bemanning och utrustning till ett annat förbund inom den kritiska infrastrukturen efter att det förbundet påverkats av en större intern störning. Aktör C bedöms arbeta med *samarbete och förtroende till andra aktöre*r i högre grad.
- Under intervjun berättade Aktör C att de övar på sin operativa förmåga, detta bedöms bidra till att de bättre kan leverera sin funktion. Detta bedöms innebära att de övar på återhämtning så att den kritiska infrastrukturens funktion upprätthålls. En annan sak som framkom under intervjun är att de har samverkansövningar med andra aktörer i form av tabletop-diskussioner där de går igenom hur insatser ska hanteras. Under intervjun berättade dock Aktör C att de inte har samverkansövningar med avseende på återhämtning för Aktör C:s egen verksamhet. Detta eftersom de anser att aktiviteter relaterade till deras egen återhämtning efter en insats ingår i deras vanliga arbetsuppgifter och därför inte behöver speciella övningar för att fungera. Däremot anses Aktör B ändå genomföra *övningar kopplade till återhämtning*. På grund av detta bedöms Aktör C endast arbeta med faktor i lägre grad.
- Aktör C berättade under intervjun att de arbetar med kontinuitetsplaner. I kontinuitetsplanerna beskrivs deras "plan B" där det står beskrivet vad ska göras för att komma tillbaka till normalläget efter en störning. Syftet med planen är att hela tiden komma

tillbaka till ett nytt normalt. Aktör C berättade även att de har reservrutiner som beskriver hur man genomför saker rent praktiskt för att upprätthålla funktionen vid bortfall av en specifik nyckelfunktion. Aktör C anses ha planer och strategier som bidrar till återhämtning av funktionen på flera olika sätt och därför bedöms därför arbeta med *strategier med fokus på återhämtning* i högre grad.

Tekniska faktorer

- Aktör C är en räddningstjänst som bedriver operativ verksamhet och som har flera tekniska resurser som gör att de kan leverera sin funktion, framförallt i form av utrustning. Några av de tekniska resurser som Aktör C har för att mer effektivt leverera sin funktion framkom i deras internkontroll och är exempelvis utrustning, fordon och förplägnad. Att mer effektivt leverera funktionen bedöms bidra till att Aktör C snabbare kan komma tillbaka till normal verksamhet och åka ut på nya insatser. Under intervjun berättade Aktör C att de även har manuella reservkraftverk. Aktör C bedöms ha flera olika tekniska resurser för återhämtning och bedöms arbeta med detta i högre grad.

Anpassning

Organisatoriska faktorer

- Under intervjun berättade Aktör C att de följer upp och utvärderar insatser på två olika sätt. Ena sättet som Aktör C berättade om var olycksutredningar som har ett förebyggande fokus. Olycksutredningarna utvärderar varför en olycka inträffade, vad som orsakade olyckan och vad de kan lära sig av den. En olycksutredning anses innebära att den kritiska infrastrukturen lär sig upprätthållit sin funktion ”att vid olyckor och överhängande fara för olyckor hindra och begränsa skador på människor, egendom eller miljön” bättre. Det andra sättet som Aktör C utvärderar på är genom insatsutvärderingar som har ett operativt fokus. I insatsutvärderingarna går Aktör C igenom deras egen operativa förmåga, ifall de använde rätt metodik eller taktik vid hantering av olyckan och vad de kan lära sig av den. Enligt Aktör C sker utvärderingarna kvalitativt. Aktör C berättade att de utbildar personal som genomför olycksutredningar och insatsutvärderingar Utöver detta sker det även uppföljning av implementerade åtgärder där personal följer upp åtgärdernas effekter både delår och helår. Eftersom Aktör C utvärderar med förebyggande fokus, genom operativt fokus och även på implementerade åtgärder bedöms Aktör C arbeta med uppföljning och utvärdering i lärande syfte i högre grad.
- En förebyggande organisatorisk åtgärd som framkom under intervjun är att Aktör C har gjort sina kontinuitetsplaner hemliga och håller dessa inlåsta. Detta bidrar till att förebygga antagonistiska störningar. Andra organisatoriska åtgärder som nämndes under intervjun var att Aktör C ändrar metodik, uppdaterar rutiner och förändrar sitt budskap i det förebyggande arbetet. Aktör C beskrev att de implementerar åtgärder både baserat på sina egna och på andras utvärderingar. Eftersom de uppgav flera olika typer av organisatoriska åtgärder runder intervjun samt att de även *implementerar organisatoriska åtgärder* utifrån andras utvärderingar bedöms Aktör C arbeta med faktorn i högre grad.
- Aktör C berättade under intervjun att de ingår i en grupp som går igenom samtal efter svåra händelser och därigenom har ett erfarenhetsutbyte med andra samtalsledare inom den kritiska infrastrukturen. Aktör C tillade i mejl att detta erfarenhetsutbyte är litet. Ett annat erfarenhetsutbyte som Aktör C berättade om var att de kollar på andras

olycksundersökningar och utvärderingar för att få ett större perspektiv. Detta utbyte sker genom databaser som tillhandahålls av MSB. Eftersom det sker ett erfarenhetsutbyte dels genom diskussioner, dels att det finns databaser för att dela information om händelser inom den kritiska infrastrukturen anses Aktör C arbeta med *erfarenhetsutbyte med andra aktörer* i högre grad.

Tekniska faktorer

- Vid utvärdering görs vissa beräkningar när det gäller brandspridning, rökspridning och liknande med program. Exempel på program som används för utvärdering är Excel. Från mejlkontakt framkom även att Aktör C använder ett rapporteringssystem för att registrera de olyckor Aktör C hanterat. Rapportering inkluderar, enligt Aktör C, trolig orsak till olyckan, aktiviteter under insatsen samt lärdomar från insatsen. Insatsstatistik för Räddningstjänst finns att se på IDA (MSB, 2020e). Händelserapportering fokuserar endast på händelser som har skett och det framkom inget under informationsinsamlingen som visar hur Aktör C arbetar med *uppföljning och utvärdering med tekniska system* gällande implementerade åtgärder. Därför bedöms Aktör C endast arbeta med faktorn i lägre grad.
- De tekniska åtgärder som framkom under intervjun som Aktör C har implementerat består av att de arbetar med IT säkerhet samt att de köper in ny utrustning och utryckningsfordon. Dessa tekniska åtgärder anses vara omfattande med tydliga kopplingar till upprätthållandet av funktionen. Aktör C bedöms därför arbeta med att *implementera tekniska åtgärder* i högre grad.

Appendix D – Sammanställning av insamlat material för Elförsörjning

För den kritiska infrastrukturen Elförsörjning har tre aktörer undersökts. Aktörerna representerar olika områden inom den kritiska infrastrukturen. Aktörerna kan antingen ha mer övervakande roller inom Elförsörjning eller äga och driva elnät. Det arbete som Aktör D, Aktör E och Aktör F genomför bidrar därför till Elförsörjning på olika sätt. Aktörerna har ibland bidragit med information om hur andra aktörer inom Elförsörjning arbetar. I bedömningarna har därför dels aktörernas egna arbeten tagit hänsyn till men till viss grad har även andra aktörers arbeten inom den kritiska infrastrukturen bedömts utifrån den information som framkommit. För Aktör D har två dokument, en rapport och ett krisberedskapsdokument, kompletterat informationsinsamlingen. Även information från Aktör D:s hemsida har använts som komplement. För Aktör E har dokument och information från aktörens hemsida kompletterat intervju och enkät. För Aktör F har det sökts i dokument men inga dokument har använts i informationsinsamlingen. Mer information har förfrågats från Aktör F men aktören har ej svarat på dessa frågor. Nedan presenteras hur Aktör D, Aktör E och Aktör F arbetar med ramverkets faktorer inom respektive förmåga för resiliens. För att tydliggöra vilken faktor som avses i punktlistorna har faktorerna skrivits ut kursivt.

Aktör D

Förutseende

Organisatoriska faktorer

- Under intervjun framkom det att det finns tydliga lagar och regler som Aktör D arbetar mot. Det finns även vissa nyckeltal som används för att bedöma hur väl funktionen upprätthålls. Att Aktör D har tydliga mål på när funktionen inte upprätthålls gör att Aktör D bedöms arbeta med *tydliga mål* i högre grad.
- Aktör D samlar in information genom möten med andra aktörer, både nationellt och internationellt. Aktör D kan även få information genom att begära ut risk och sårbarhetsanalyser från andra aktörer inom den kritiska infrastrukturen. Aktör D har även en marknadsanalysgrupp som övervakar elmarknadens rörelser. Balans i elmarknaden lyftes fram av aktörerna som en viktig sak för att motverka störningar inom Elförsörjning och därför bidrar informationsinsamling om detta till förutseende. Kombinationen av dessa *organisatoriska system för informationsinsamling* gör at Aktör D bedöms arbeta med faktor i högre grad.
- Insamlad information antas främst analyseras genom expertbedömningar. Detta bygger dels på att Aktör D har publicerat dokument där de presenterar statistik inom Elförsörjning och analyserar tendenser och trender i Sverige och omvärlden. Från mejlkontakt skrev Aktör E att det inom den kritiska infrastrukturen förekommer analyser på statistik på elavbrott samt risk och sårbarhetsanalyser. Detta är en del av det tillsynsarbetet som sker inom den kritiska infrastrukturen. Arbetet med *organisatoriska system för analys* inom den kritiska infrastrukturen bedöms förekomma i lägre grad utifrån denna information.
- Under intervjun framkom det inte om den information som Aktör D samlar in används för att identifiera otydliga signaler. Hur Aktör D arbetar med att möjligheter att *uppmärksamma otydliga signaler och indikationer* kan därför inte bedömas.

Tekniska faktorer

- Under intervjun berättade Aktör D att de har prenumerationstjänster på Montel och nyhetsbrev, vilket anses vara en typ av tekniska system för informationsinsamling kring elmarknaden och omvärldsbilden. Det framkom även från mejlkontakt med Aktör D att de har tillgång till en digital plattform där det finns aktuella lägesbilder för elnätverkens status. Sammanlagt har Aktör D *tekniska system för informationsinsamling* riktade dels mot marknaden, dels mot omvärldsläget och dels mot statusen i elnätet. Aktör D bedöms därför arbeta med faktorn i högre grad.
- Enligt Aktör D arbetar de inte med tekniska analysmetoder i så stor utsträckning. Informationen om hur Aktör D arbetar med *tekniska analysmetoder* anses inte vara tillräcklig för att göra en bedömning om deras arbete med faktorn.

Robusthet

Organisatoriska faktorer

- De övningar som Aktör D berättade om under intervjun hade ingen tydlig koppling till robusthet utan till återhämtning. Eftersom det inte tydligt framkom att Aktör D inte har övningar som skapar robusthet inom Elförsörjning har en bedömning av Aktör D:s arbete med *övningar som bidrar till förmågan för robusthet* inte gjorts.
- En strategi som aktören berättade om under intervjun för att undvika att funktionen inte längre kan upprätthållas var att de personalplanerade för att undvika personalbrist. En annan typ av strategi som används är N-1 kriteriet vilket innebär att den kritiska infrastrukturens funktion upprätthålls även om ett system fallerar. Aktör D arbetar även med att skydda viktig information genom sekretess, exempelvis genom att förhindra att känslig information läggs ut på digitala plattformar som kan utsättas för cyberattacker. Dessa åtgärder anses tillsammans visa att Aktör D arbetar med *planer inför oönskade händelser* i högre grad.
- Aktör D berättade att det är viktigt att det råder en balans mellan den el som produceras och den el som förbrukas för att Elförsörjning ska fungera. Från mejlkontakt med Aktör D framkom det att aktörer inom Elförsörjning samverkar med varandra på olika sätt för att säkerställa att det råder balans inom Elförsörjning. Det framkom dock inga specifika exempel på hur samverkan tar sig form. Eftersom Aktör D betonade samverkans vikt för upprätthållanden av Elförsörjnings funktion anses detta vara något Aktör D arbetar med *samarbete kopplat till robusthet* i högre grad.

Tekniska faktorer

- Informationen om Aktör D:s arbete med *bufferts* anses inte vara tillräcklig för att göra en bedömning om aktörens arbete med faktorn.
- Informationen om Aktör D:s arbete med *redundanta system eller en inbyggd redundans i systemen* anses inte vara tillräcklig för att göra en bedömning om aktörens arbete med faktorn.

Återhämtning

Organisatoriska faktorer

- Aktör D berättade under intervjun att de lägger resurser på att verksamheten inte ska vara beroende av en viss person för vissa uppgifter ska kunna genomföras. För att förhindra detta ser Aktör D till att andra i personalstyrkan har kompetens för att ta över ifall en viss person försvinner. Aktör D har även tillgång till en IT-konsult som kan hjälpa vid en teknisk störning. Dessa *organisatoriska resurser* anses vara mindre omfattande Aktör D bedöms därför arbeta med faktorn i lägre grad.
- Under intervjun framkom det att Aktör D har satta regler för krishantering. Enligt Aktör D finns det planer inom Elförsörjning för att se till att elen fördelas effektivt i samhället vid elbrist. Om det blir en elbrist på grund av en störning kan Aktör D:s framarbetade planer således bidra till återhämtningsförmågan inom Elförsörjning genom att koordinera och se till att elen används effektiv. Aktör D har även en tjänsteman i beredskap, vilket är en funktion som bidrar till koordinering av både den interna och externa resurshanteringen vid en kris och därmed till återhämtningsförmågan inom Elförsörjning. I ett uppföljningsmejl beskrev Aktör D att de även ingår i ett system där aktörer inom Elförsörjning hjälper varandra med personal och material vid störningar via en digital plattform. Dessa strategier anses täcka både intern resurshantering för Aktör D och resurshantering inom den kritiska infrastrukturen Elförsörjning. Aktör D bedöms därför arbeta med *ledning och koordination av resurser* i högre grad.
- När Aktör D tillfrågades om deras möjligheter att ge stöd till andra aktörer inom Elförsörjning så svarade Aktör D i ett mejl att de ger kunskapsstöd till bland annat kommuner och länsstyrelser. Detta anses vara en typ av samarbete som bidrar till återhämtningen inom den kritiska infrastrukturen. Även den resursdelning som sker inom Elförsörjning där aktörer hjälper varandra med personal och material tyder på att det finns ett samarbete och förtroende inom Elförsörjning. Det framkom även under en uppföljningsintervju med Aktör D att de vid en större störning har ett tätt samarbete med nätägare i Sverige samt internationella aktörer med vilka de för samtal för att hantera störningen. Eftersom det finns etablerade krissamarbeten med både nationella och internationella aktörer bedöms Aktör D arbeta med *samarbete med andra samhällsaktörer kopplat till återhämtning* i högre grad.
- I ett dokument om krisberedskap på Aktör D:s hemsida framkom det att det planeras minst en branschövning per år. Branschövningen utgår från ett scenario där en störning har skett, vilket tolkas som att övningen fokuserar på återhämtning. Eftersom detta var den enda *övningen kopplat till återhämtning* som framkom under intervjun, och övningen endast förväntas ske en gång per år, bedöms Aktör D endast arbeta med faktorn i lägre grad.
- Aktör D angav i enkäten att de har kontinuitetsplaner, men utvecklade inte hur dessa används i deras arbete under intervjun. Det anses inte finnas tillräckligt med information för att göra en bedömning om Aktör D:s arbete med *strategier med fokus på återhämtning*.

Tekniska faktorer

- Under intervjun framkom det inte om Aktör D arbetar med några tekniska resurser som kan användas för att återhämta den kritiska infrastrukturen efter störning. Det anses inte finnas tillräcklig information för att göra en bedömning om till vilken grad Aktör D arbetar med *tekniska resurser*.

Anpassning

Organisatoriska faktorer

- Aktör D följer upp och utvärderar hur andra aktörer inom Elförsörjning arbetar med anpassning. I Aktör D:s publikationer kan man se att aktören utvärderar tidigare störningar i ett lärande syfte. Exempelvis har Aktör D publicerat en rapport där erfarenheter från stormen Gudrun används för att ta fram förbättringsförslag för Elförsörjning. Detta gör att Aktör D bedöms arbeta med *uppföljning och utvärdering i lärande syfte* i högre grad.
- Under intervjun uppgav Aktör D att de arbetar med att implementera förebyggande organisatoriska åtgärder. Aktör D gav dock inga exempel på sådana åtgärder, delvis på grund av sekretesskäl. På Aktör D:s hemsida finns det dock information om att Aktör D arbetar med att få andra aktörer i samhället att anpassa sig så att konsekvenserna av ett elavbrott blir mindre. På Aktör D:s hemsida finns även information om att de investerar i forskning inom Elförsörjning som bidrar till den kritiska infrastrukturens resiliens, exempelvis forskning om elanvändning i relation till klimatförändringar. Från mejlkontakt med Aktör D framkom det att de erbjuda kunskapsstöd. Kunskapsstöden är strategier som går ut på att informera aktörer inom den kritiska infrastrukturen hur de kan använda reservkraftverk för att få tillgång till el även vid ett stort elavbrott. Aktör D arbetar alltså med flera olika *förebyggande organisatoriska åtgärder*, och bedöms därför arbeta med faktor i högre grad.
- Aktör D berättade under intervjun att det sker ett erfarenhetsutbyte via NIS-direktivet och att utbytet handlar om störningar som drabbat andra aktörer. Enligt MSB (2020c) innebär NIS-direktivet att flera sektorer rapporterar in händelser och att det sedan är MSB som hanterar informationen. Aktör D bedöms därför endast arbeta med *erfarenhetsutbyte i lärande syfte* i lägre grad.

Tekniska faktorer

- Under intervjun framkom inte om Aktör D arbetar med några tekniska system som kan användas för uppföljning och utvärdering i lärande syfte. Det anses därför inte finnas tillräcklig med information för att göra en bedömning huruvida Aktör D använder *tekniska system för uppföljning och utvärdering.*
- Aktör D angav att det finns tekniska åtgärder som har implementerats, men kunde inte ge några exempel. Det finns därför inte tillräckligt med information om Aktör D arbetar med *tekniska åtgärder för* att göra en bedömning.

Aktör E

Förutseende

Organisatoriska faktorer

- Aktören E berättade i sin intervju att de har tydliga gränser och mått på när deras leverering av funktionen inte längre anses upprätthållas. Aktör E nämnde dessutom att de följer ellagen och elberedskapslagen eftersom de är en del av samhällssektorn energiförsörjning. Aktör E bedöms arbeta med *tydliga mål* i högre grad.
- I intervjun berättade Aktör E att de arbetar med öppen informationsinsamling för omvärldsbevakning. Den öppna informationsinsamlingen sker, enligt Aktör E, utan några stödsystem och bedöms därför vara en organisatorisk metod för att samla in information.

Det nämndes även att det finns ett samarbete med andra aktörer inom Norden där aktörerna utbyter data för att hålla systemet i balans, samt för datahanteringen i elmarknaden. De system för informationsinsamling som framkom under intervjun bedöms samla in information från flera olika områden som kan påverka Aktör E:s arbete i den kritiska infrastrukturen. Aktör E bedöms arbeta med *organisatoriska system för informationsinsamling* i högre grad.

- Aktör E uppgav under intervjun att de har specialister och experter som räknar på vad som behövs göras i systemet rent fysiskt, exempelvis vid utbyggnader eller hur förändringarna påverkar elnätet. Aktör E analyserar även väderprognoser för att förutse väderrelaterade störningar i Elförsörjning. Aktör E gör även risk- och sårbarhetsanalyser samt långsiktiga marknadsanalyser, som båda anses vara verktyg för att analysera insamlad information. Aktör E:s arbete med organisatoriska analyssystem bedöms vara i högre grad.
- I intervjun berättade Aktör E att det finns sensorer i systemet som övervakar i realtid som mäter i både sekunder och millisekunder, men även att det finns system som automatiskt slår av driften vid vissa signaler. Dessutom övervakar Aktör E hur förändringar i omvärlden påverkar elnätet. Systemen anses kunna detektera små förändringar samt externa och Aktör E antas därför arbeta med att *uppmärksamma otydliga signaler och indikationer* på störningar i högre grad.

Tekniska faktorer

- Sensorerna som övervakar systemet i realtid bedöms vara ett tekniskt system som används för informationsinsamling. Sensorerna är en del av ett drift- och övervakningssystem som Aktör E berättade om under intervjun. Eftersom drift och övervakningssystemet kontinuerligt bidrar med information samt anses beröra hela elnätet, bedöms Aktör E arbeta med *tekniska system för informationsinsamling* i högre grad.
- Under intervjun berättade Aktör E att de har system som kan slå av strömmen direkt om det behövs. Dessa system samlar in information och slår av strömmen automatiskt vid en störning, systemen bedöms därmed analysera den insamlade informationen. Aktör E har i varken intervju eller enkät nämnt tekniska system utöver dessa som kan användas för analys. Aktör E har istället sagt att information gällande omvärldsanalys sammanställs utan stödsystem. Aktör E bedöms därför arbeta med *tekniska system för att analys* insamlad information i lägre grad.

Robusthet

Organisatoriska faktorer

- Övningar för att vara robust mot störningar har Aktör E inte nämnt, de övningar som Aktör E berättade om är mer kopplat till återhämtning av elnätet. En bedömning hur väl Aktör E arbetar med *övningar kopplat till robusthet* har därför inte gjorts.
- Aktör E berättade under intervjun att de följer N-1 kriteriet, vilket anses vara en strategi mot oönskade händelser. Det nämndes även att de arbetar med systemplaner och har gemensamma strategier med flera länder i Norden för att upprätthålla Sveriges Elförsörjning. Aktör E bedöms arbete med *planer och strategier för oönskade händelser* i högre grad.
- Under intervjun gav Aktör E exempel på hur de tidigare har fått hjälp av andra aktörer i Sverige för att motverka störningar vilket bedöms ha påverkat Elförsörjnings robusthet

positivt. På aktörens hemsida beskrivs dessutom flera samarbeten med länder i både Europa och i Norden, exempel på hur samarbeten med andra länder bidrar till robusthet är möjlighet till elimport ifall det inte kan levereras tillräckligt med el i Sverige. Aktör E bedöms arbeta med *samarbete med andra aktörer* kopplat till robusthet i högre grad.

Tekniska faktorer

- I intervjun med Aktör E framkom det inte ifall det finns någon buffert i systemet som skulle bidra till robusthetsförmågan. I vilken grad Aktör E arbetar med *buffert* kunde därför inte fastställas.
- Aktör E beskrev själv verksamheten som semi-redundant under intervjun. Det som kan anses som redundant är att det finns möjlighet att leda om el för att upprätthålla energiförsörjningen. Aktör E bedöms arbeta med *redundanta system eller en inbyggd redundans i systemen* i lägre grad.

Återhämtning

Organisatoriska faktorer

- Aktör E berättade under sin intervju att personal snabbt ställer upp om något skulle hända. Vid en störning kan det, enligt aktören, komma fler personer än vad som behövs. Personaltillgången vid en störning bedöms vara en organisatorisk resurs som delvis bidrar till deras förmåga att återhämtas. Aktör E bedöms därför arbeta med *organisatoriska resurser* i lägre grad.
- Från aktör Aktör E:s hemsida framkom det att de är med i ett samarbete som har utbildningar med fokus på resurshantering vid en störning. Det finns även styrande dokument där det framgår att Aktör E arbetar med att leda och samordna resurser inom Elförsörjning vid specifika störningar. Aktör E har dessutom verktyg för att fördela el i samhället vid elbrist. Om det blir en elbrist på grund av en störning kan Aktör E således bidra till återhämtningsförmågan inom Elförsörjning genom att koordinera och se till att elen används effektiv. Utöver detta har Aktör E en tjänsteman i beredskap, vilket är en funktion som bidrar till koordinering av resurshanteringen för den egna verksamheten vid en kris. Aktör E arbetar med *ledning och koordination för resurshantering* för både den egna verksamheten och för den kritiska infrastrukturen i högre grad.
- Det samarbete som Aktör E har med andra aktörer, som påverkar återhämtning, har utlästs från aktörens hemsida. Det som kan anses bidra till återhämtning efter en störning är att resurser från andra länder kan användas för att hjälpa till att återbygga systemet. Eftersom det finns ett internationellt samarbete som hjälper den kritiska infrastrukturens återhämtning bedöms Aktör E arbeta med *samarbete och förtroende till andra aktörer* i högre grad.
- Aktör E beskrev under intervjun flera olika övningar som anses bidra till återhämtningsförmågan. Aktör E berättade att de genomför samverkansövningar tillsammans med andra aktörer där en störning i Elförsörjning simuleras i ett program. Aktör E genomför även övningar i reparationsberedskap. Aktör E bedöms därför arbeta med övningar *kopplat till återhämtning* i högre grad.
- Flera dokument från Aktör E:s hemsida beskriver hur kriser inom infrastrukturen Elförsörjning ska hanteras. Dokumenten från krishantering är vägledningar som beskriver bland annat krisens olika faser samt hur dessa ska hanteras. Dessutom nämnde Aktör E i

intervjun att de har manualer för återställning efter en störning. Aktör E bedöms därför arbeta med *strategier med fokus på återhämtning* i högre grad.

Tekniska faktorer

- I intervjun med Aktör E framkom det att det finns ett lager för material men vad som lagras beror på kostnaden av materialet. Allt material som behövs för att effektivt kunna återhämtas förväntas därför vara begränsad. Aktör E bedöms arbeta med *tekniska resurser* i lägre grad.

Anpassning

Organisatoriska faktorer

- I intervjun beskrev Aktör E att de gör analyser innan en åtgärd implementeras, men inte efter. Eftersom Aktör E endast utvärderar åtgärder innan de implementeras och inte följer upp efteråt bedöms Aktör E arbeta med *uppföljning och utvärdering i lärande syfte* i lägre grad.
- I intervjun berättade Aktör E att de implementerar åtgärder för att anpassas, men kunde inte ge exempel på sådana åtgärder. Det finns däremot planer på Aktör Es hemsida som hanterar långsiktiga lösningar för att tillgodose infrastrukturens Elförsörjningsförmåga. Dock saknas det tillräcklig information om detta för att kunna göra en bedömning om Aktör E arbetar med *organisatoriska åtgärder*.
- Det finns samverkan med andra aktörer, bland annat genom en nationell samverkansgrupp. I samverkansgruppen delar aktörer med sig av erfarenheter och lärdomar och diskuterar åtgärder. Information om Aktör E:s medverkan i samverkansgruppen kommer från dokumentsökning. Eftersom aktör E själva inte tog upp samarbetet i under intervjun bedöms Aktör E arbeta med *erfarenhetsutbyte med andra aktörer* i lägre grad.

Tekniska faktorer

- Det angavs inte några tekniska system som kan användas för uppföljning och utvärdering i lärande syfte. Det kan därför inte göras någon bedömning till vilket grad Aktör E arbetar med *tekniska system*.
- Aktör E poängterade i intervjun att det är svårt att genomföra tekniska åtgärder för att stärka infrastrukturen eftersom det tar lång tid att implementera samt är kostsamt. Däremot nämnde Aktör E att de tar fram planer för implementering av åtgärder och att de tittar mycket på kontinuitetshantering för att bygga bort det som de kan bygga bort. Aktör E bedriver även ett arbete med långsiktiga anpassningsåtgärder som exempelvis uppgradering av system för att möta omställningar, produktionssätt och nya förmågor. Aktör E bedöms därför arbeta med *tekniska förebyggande och proaktiva åtgärder* i högre grad.

Aktör F

Förutseende

Organisatoriska faktorer

- Aktör F har tydliga mål på vad som ska skyddas. Bedömningen bygger på att aktören under intervjun berättade att de har tydliga nyckeltal på avbrottsdata och kriterier för spänningskvalitet där funktionen inte längre anses upprätthållas. Aktör F anses arbeta med *tydliga mål* i högre grad.
- Under intervjun med Aktör F framkom det inte ifall det finns några organisatoriska system för informationsinsamling som bidrar till förutseendeförmågan. I vilken grad Aktör F arbetar med *organisatoriska system för informationsinsamling* kan därför inte bedömas.
- Enligt Aktör F arbetar de med att analysera underhållsbehovet i driftnätet för att vara förutseende mot komponentfel. Aktör F uppgav under intervjun att de gör konsekvensbedömningarna på hela nätet för att se över förmågan att kunna koppla om nätverket vid störningar. Aktörens beskrivning av deras organisatoriska analysmetoder tolkas som att de främst inriktar sitt arbete på att analysera interna störningar och inte lika mycket på analys av störningar som kan uppkomma på grund av externa förhållanden. Aktör F bedöms därför arbeta med *organisatoriska analysmetoder* i lägre grad.
- Aktör F angav i intervjun flera olika sätt att både samla in information och att analysera informationen. Aktör F granskar flera olika parametrar så som information från SCADA-system, från driftrum, deras underhållstrategier och väderprognoser genom organisatoriska- och tekniska system. Kombinationen av system, som både kan hantera översiktlig information (exempelvis underhållsstrategier) och specifika data (exempelvis SCADA-system), bedöms användas för att uppmärksamma olika typer av förändringar i systemet. Aktör F bedöms därför arbeta med att *uppmärksamma otydliga signaler och indikationer* i högre grad.

Tekniska faktorer

- Aktör F använder SCADA-system, väderprognoser från SMHI, Network Information System (NIS), Order Management System (OMS) och Geographic Information System (GIS) för att samla in information. Dessa system bidrar till förutseendeförmågan genom att bland annat samla in information om status på driftkomponenter. Dessa system samlar in information från flera olika områden och visade att Aktör F arbetar med *tekniska system för informationsinsamling* i högre grad.
- SCADA-system och GIS som används för informationsinsamling är även system som kan hantera och analysera information. GIS kan dessutom användas för att lösa mer komplexa problem (Esri Sverige, 2020). Eftersom systemen anses som större system samt att det finns möjlighet att lösa mer komplexa problem bedöms Aktör F arbeta med *tekniska systemen för analys* i högre grad.

Robusthet

Organisatoriska faktorer

- De övningar som Aktör F berättade om under intervjun hade ingen tydlig koppling till robusthet utan till återhämtning. Eftersom det inte tydligt framkom att Aktör F inte har övningar som skapar robusthet inom Elförsörjning har en bedömning av Aktör F:s arbete med *övningar som bidrar till förmågan för robusthet* inte gjorts.
- Aktör F har planer inför oönskade händelser som bidrar till robusthetsförmågan. Aktör F berättade under intervjun att de har avtal med kunder om att kunderna kan kopplas bort med kort varsel när tillgänglighet elkapacitet riskerar att överskridas. Att koppla bort vissa användare i dessa fall gör att man kan undvika att det sker en störning till, och dessa avtal bidrar därför till Elförsörjnings robusthet. Aktör F har alltså *planer för att motstå oönskade händelser* vilka ökar robustheten, men dessa planer anses inte omfattande. Aktör F:s bedöms därför arbeta med denna faktor i lägre grad.
- Under intervjun berättade Aktör F att de samarbetar med andra aktörer inom Elförsörjning kring underhållet av elnätet. Underhållet gör att man bättre motstår en störning i elnätet och samarbetet bidrar därför till robustheten inom Elförsörjning. Detta var det enda samarbetet kopplat till robusthet som framkom under informationsinsamlingen och Aktör F bedöms därför endast arbeta med *samarbeten som bidrar till robusthet* i lägre grad.

Tekniska faktorer

- I varken enkät, intervjun eller dokumentsökning framkom det ifall Aktör F har någon buffert, varken för externa beroenden eller buffert för el. I vilken grad Aktör F arbetar med *buffert* kunde därför inte bedömas.
- Under intervjun framkom det att Aktör F har redundans i flera kritiska system inom deras verksamhet för att undvika störningar. Exempelvis kan Aktör F omkoppla el ifall en viss ledning slutar fungera. Aktör F bedöms arbeta med *redundans* i högre grad eftersom det finns redundans hos de system som anses kritiska för funktionen.

Återhämtning

Organisatoriska faktorer

- Aktör F nämnde i intervjun att det är en komplicerad process att återställa funktionen efter ett större elbortfall, som är en typ av störning. Tillgången till kompetent personal som kan återställa systemet blir därför en viktig resurs för att kunna återhämta funktionen. Aktör F har därför flera utbildningar för personalen för att se till att de har tillgång till kompetent personal. En annan organisatorisk resurs är att Aktör F har tillgång till extern förstärkning i form av personal vilket förväntas bidra till en snabbare återhämtning. Eftersom tillgång till kompetent personal anses vara en viktig faktor för att kunna återhämta systemet inom Elförsörjning, bedöms Aktör F arbeta med *organisatoriska resurser* i högre grad.
- Aktör F arbetar med planer och koordinering av resurser för snabbare återhämtning av funktionen efter en störning. Aktör F berättade bland annat att de är snabba på att fördela resurser så att de kan ersätta komponenter som går sönder. Dock berättade Aktör F i intervjun att de inte alltid har kontroll på de lager som de förvarar nödvändiga resurser på, vilket tidigare har resulterat i att resurser sinat eller inte varit godkända då de behövts. Aktörens arbete med *planer och koordinering för resurshantering* bedöms har alltså vissa brister men Aktör F bedöms ändå arbeta med faktorn i högre grad.

- Aktör F har utarbetade samarbeten för att låna resurser av andra aktörer inom Elförsörjning, exempelvis större reservkraftverk. Detta är ett samarbete som bidrar till återhämtningsförmågan. Eftersom detta var det enda samarbete med koppling till återhämtning som framkom under informationsinsamlingen bedöms Aktör F arbeta med *samarbete för återhämtning* i lägre grad.
- Aktör F sa under intervjun att de genomför samverkansövningar tillsammans med andra aktörer för olika driftstörningar inom Elförsörjning. Störningarna simuleras med hjälp av ett simuleringsprogram. Aktör F förklarade att personalen under övningarna bland annat får träna på återställningsplaner. Aktör F berättade även under intervjun att de genomför andra samverkansövningar med aktörer inom Elförsörjning där de övar på resurshantering. Aktör F delar vissa resurser med andra aktörer, och övningarna syftar därför till att resurserna ska användas effektivt vid en störning. Aktör F genomför även övningar för användning av Rakel. Genomförandet av övningarna anses omfatta flera olika störningar som kan påverka funktionen inom den kritiska infrastrukturen. Aktör F: bedöms arbeta med *övningar för återhämtning* i högre grad.
- Under intervjun förklarade Aktör F att det är svårt att successivt kunna komma tillbaka efter ett elbortfall. Enligt Aktör F stressas systemet mycket av en återställning och att det då lätt kan överbelastas. Aktör F bedöms ha planer för att återställa systemet eftersom det är svårt att successivt komma tillbaka. Däremot går det inte att utläsa hur eventuella planer ser ut från den insamlande informationen. Det går därför inte bedöma till vilken grad Aktör F arbetar med *strategier med fokus på återhämtning.*

Tekniska faktorer

- Enligt Aktör F finns det tillgång till reservmaterial så som svårinförskaffade komponenter, tillfälliga träställningar och reservkablar. Det finns även tillgång till bandvagnar, helikoptrar och reservkraftverk. Vissa av resurserna finns inom Aktör F:s egen organisation, medan andra finns tillgängliga via samarbeten med andra aktörer. Dessa tekniska tillgångar angavs under intervjun, och anses vara av varierande karaktär och täcka så pass olika områden att Aktör F bedöms arbeta med *tekniska resurser* i högre grad.

Anpassning

Organisatoriska faktorer

- Aktör F berättade under intervjun att de använder sig av film och litteratur för att följa upp tidigare händelser i lärande syfte. Under intervjun berättade Aktör F att de borde arbeta mer med att se till att de har tillgång till rätt resurser, detta då det tidigare har hänt att resurser varit utdaterade eller inte fanns på den plats där de behövdes. Både film och litteratur samt den egna bedömningen av tidigare händelser bedöms vara sätt som Aktör F arbetar med för utvärdering i lärande syfte. Aktör F arbetssätt med utvärdering anses vara varierad och därmed bidra till lärande inom verksamheten på olika sätt. Aktör F bedöms arbeta med *utvärdering och uppföljning i lärande syfte* i högre grad.
- En organisatorisk åtgärd som Aktör F berättade om under intervjun är att de har säkerhetsklassad personal. Aktör F förklarade att de implementerar säkerhetsklassning hos sin personal, ser till att personalen har adekvat kompetens och att personalens access begränsas till det som endast är nödvändigt. Säkerhetsklassningen hos personalen är en strategi för att undvika störningar i funktionen genom exempelvis oauktoriserade intrång. De filmer och litteraturer som används för att lära från tidigare händelser kan också ses som

en organisatorisk åtgärd. Dessa två åtgärder anses inte vara starkt bidragande till att anpassa Elförsörjning mot störningar och Aktör F bedöms därför arbeta med *organisatoriska åtgärder* i lägre grad.

- I varken enkät, intervju eller dokumentsökning har det framkommit några exempel på hur Aktör F utbyter erfarenheter med andra aktörer i lärande syfte. Till vilken grad Aktör F *utbyter erfarenheter med andra aktörer* kan inte bedömas.

Tekniska faktorer

- SCADA-systemet och GIS-systemet som används av Aktör F samlar in data om tidigare händelser, så som omfattning och geografiskt läge, och sammanställer informationen. Informationen antas användas av Aktör F i lärande syfte. Genom SCADA-system antas även Aktör F få en kontinuerlig utvärdering av driftstatusen. Aktör F bedöms därför arbeta med *tekniska system för uppföljning och utvärdering i lärande syfte* i högre grad.
- En teknisk åtgärd som Aktör F arbetar med är ett digitalt verktyg för att öka utnyttjandegraden i elnätet. Verktyget skapar en flexibilitet i nätet som motverkar kapacitetsbrist. Denna åtgärd berättade Aktör F om under intervjun och mer information om verktyget har hittats på aktörens hemsida. Aktör F nämnde även under intervjun att det är viktigt att kunna implementera åtgärder för att minska sådana risker som inte går att bygga bort. Aktör F berättade att det sker ett kontinuerligt underhåll av elnätet. De åtgärder som Aktör F beskrev att de implementerat är säkerhetslås, staket och elskydd, som alla är fysiska åtgärder för att motverka antagonistiska hot. Det ovanstående visar att Aktör F:s arbetar med t*ekniska förbyggande åtgärder* i högre grad.

Appendix E – Sammanställning av insamlat material för Telekommunikation

De aktörer som medverkade i analysen för den kritiska infrastrukturen Telekommunikation hade mer övervakande roller och driver inget eget nät. Däremot hade både Aktör G och Aktör H bra insikt i hur flertal aktörer inom Telekommunikation arbetar. I bedömningarna har därför Aktör G och Aktör H egna arbeten tagits hänsyn till, men även andra aktörers arbeten inom den kritiska infrastrukturen har till viss grad bedömts utifrån den information som framkommit. För Aktör G har både dokument och information från aktörens hemsida använts som komplement till enkät och intervju. Dokumenten och informationen från hemsidan skickades av Aktör G via mejl. Totalt mejlade Aktör G tre dokument och fyra länkar till hemsidan. För Aktör H har ett vägledande dokument som hittades på Aktör H:s hemsida används som komplement till intervju och enkät. Nedan presenteras hur Aktör G och Aktör H arbetar med ramverkets faktorer inom respektive förmåga för resiliens. För att tydliggöra vilken faktor som avses i punktlistorna har faktorerna skrivits ut kursivt.

Aktör G

Förutseende

Organisatoriska faktorer

- I enkäten uppgav Aktör G att de arbetar utifrån lagar och förskrifter som berör den kritiska infrastrukturens funktion. På hemsidan finns dessutom deras grundläggande mål vilka berör dels marknaden, dels konsumenternas intressen. I mejlkontakt med Aktör G framkom det att det finns aktiviteter kopplade till dessa mål som följs upp kontinuerligt. Bedömningen är att Aktör G har tydliga mål på hur funktionen upprätthålls inom sektorn Information och kommunikation, och att dessa mål kontinuerligt följs upp. Aktör G bedöms arbeta med *tydliga mål* för den kritiska infrastrukturen Telekommunikation i högre grad.
- Under intervjun med Aktör G framkom det att de samlar in information via en nationell samverkansgrupp som är ett samarbete med aktörer inom sektorn Information och kommunikation. Genom samarbetet får Aktör G information så som statusuppdateringar från aktörer från olika delar av samhället för att kunna bedöma hot mot kritiska komponenter. Exempelvis berättade Aktör G att de genom den nationella samverkansgruppen fått in statusuppdateringar från andra aktörer under skogsbränderna 2018. Detta gjorde att Aktör G kunde vara förutseende mot hur skogsbranden hotade kritiska komponenter för den kritiska infrastrukturen, exempelvis noder. I ett mejl skrev Aktör G att de har samarbete med andra aktörer som *”är viktigt utifrån planeringsförutsättningar och uppbyggnad”*. Samarbetet mellan aktörer inom den kritiska infrastrukturen bedöms därför bidra med information som Aktör G använder i sin planering. Samarbeten var den typ av organisatoriska metoder för informationsinsamling som framkom under intervjun, dokument och mejlkontakt. Aktör G bedöms därför arbeta med *organisatoriska system för informationsinsamling* i lägre grad.
- Enligt Aktör G görs det många olika slags analyser för att stödja aktörerna inom Telekommunikation. Aktör G har inom sin organisation analyskompetenstydliga analysavdelningar som täcker olika aspekter av den kritiska infrastrukturen Telekommunikation. Bland annat gör Aktör G risk- och sårbarhetsanalyser analyser för

telekommunikationsmarknaden. Intervjuobjektet förklarade att det, på den avdelning som denne arbetar, är människor som analyserar information utan stöd av tekniska analysverktyg, det vill säga en form av expertbedömningar. Hur andra avdelningar inom Aktör G:s verksamhet analyserar information kunde denne inte svara på. Aktör G nämnde även under intervjun att de har en TIB som kontrollera data som kommer in från vissa informationsinsamlingssystem. Det framkom inga specifika metoder för analys, men Aktör G anses arbeta med analyser på många olika sätt och över hela organisationen. Detta gör att Aktör G anses arbeta med *organisatoriska analyssystem* för aktörer inom Telekommunikation i högre grad.

- Det är svårt att bedöma om de system som Aktör G använder för att vara förutseende kan användas för att upptäcka otydliga signaler med avseende på funktionen, eftersom det inte framkom hur systemen används i detta syfte. Aktör G har själva ingen nätövervakning men det finns inom den kritiska infrastrukturen Telekommunikation. Utifrån denna information har ingen bedömning kunnat göras till vilken grad aktören eller den kritiska infrastrukturen kan *uppmärksamma otydliga signaler och indikationer* för att vara förutseende.

Tekniska faktorer

- Det som framkom under intervjun gällande tekniska system för informationsinsamling är att Aktör G använder system som GIS, WIS och SOS-portalen. Exempelvis så finns det en telekommunikationsflik i SOS-portalen där information om operatörernas störningar och avbrott visualiseras och som Aktör G:s TIB följer kontinuerligt. Aktör G har själv ingen egen nätövervakning men berättade att aktörerna inom Telekommunikation har kontinuerlig övervakning av näten. Operatörerna gör bland annat trafikanalyser för att identifiera ett onormalt trafikmönster. Dessa system bedöms samla in information om flera områden som kan påverka Telekommunikations funktion. Aktör G bedöms därför arbeta med *tekniska system för informationsinsamling* i högre grad.
- Under intervjun berättade Aktör G om några av de tekniska program de använder för analys. Aktör G beskrev att för att vara förutseende samlar aktören årligen in data kring hur långt bredbandsutbyggnaden i Sverige gått och i det arbetet används bland annat GIS-kartor. Aktör G berättade även under intervjun att de använder aktörsdata för att göra marknadsanalyser kopplat till konkurrensreglering. Enligt Aktör G är de olika analyserna viktiga för att säkerställa aktörens olika uppdrag och kunna få en överblick över den kritiska infrastrukturen. Aktör G bedöms arbeta med *tekniska systemen för analys* i högre grad.

Robusthet

Organisatoriska faktorer

- Aktör G beskrev under intervjun att de övningar som genomförs inom Telekommunikation bland annat stress-testar upprätthållandet av funktionen och därmed hur väl den kritiska infrastrukturen kan motstå och absorbera störningar. I intervjun berättade Aktör G att de har sektorsövningar med andra aktörer inom bland annat telekommunikation där de övar på olika scenarier som, utifrån Aktör G:s beskrivning, anses ha tydliga kopplingar till robusthet. Scenarierna innefattar exempelvis bränslebrist och hur det ska hanteras, men fokus för övningarna är ofta med betoning på samverkan mellan olika aktörer. Övningen om bränslebrist antas förbättra hanteringen av den kritiska infrastrukturens elberoende innan en störning inträffar. Det framkom även att Aktör G övar på beslutskedjor,

informationsflöden och lägesbilder. Eftersom det inte var så många av de beskrivna övningarna som fokuserar på robusthet bedöms Aktör G arbeta med *övningar kopplat till robusthet* i lägre grad.

- Aktör G berättade under intervjun att de har en krisstab som arbetar nu under covid-19 pandemin. Krisstabsfunktionen har även varit igång vid andra tillfällen, t.ex. under skogsbränderna 2018. För att säkerställa bemanningen av krisstaben görs en bemanningsplan som sträcker sig över flera veckor och involverar personer som är utbildade och vana att arbeta i krisstaben. Att linjeverksamheten finns på plats, som stöd för krisstaben, är också en viktig del av arbetet. Under intervju framkom även att krisstaben gör långsiktiga planeringar för bemanning. Detta för att det alltid ska finnas personal på plats som kan upprätthålla verksamheten. Aktör G berättade under intervjun att Sverige inte har haft några kapacitetsproblem med sina telekommunikationsnät så som vissa länder i övriga Europa när nätanvändningen ökade under Covid-19 pandemin. Detta eftersom Sverige generellt har mycket god tillgång till fiberinfrastruktur och därmed mycket hög kapacitet i näten i förhållande till belastning. Att Sverige har en god kapacitet i sina nät innebär att det finns en motståndskraft mot kapacitetsrelaterade störningar inom Sveriges telekommunikation. Att Sverige har bra kapacitetsmöjligheter antas komma från en god planering inom den kritiska infrastrukturen inför oväntade händelser. Aktörerna inom telekommunikation bedöms, utifrån Aktör G:s beskrivning, arbeta med *planering inför oönskade händelser* i högre grad.
- Det samarbete som beskrivits av Aktör G bidrar till förmågan robusthet eftersom det genom samarbetet görs satsningar i tekniska robusthetsåtgärder. Aktör G berättade under mejlkontakt att det inom Telekommunikation förekommit att tillgängliga resurser genom samarbete använts för att öka robusthet inom den kritiska infrastrukturen. Ett exempel på detta är under skogsbränderna 2018 då Aktör G:s transportabla mobilbasstationer användes för att räddningsledare (extern aktör) skulle få tillgång till mobiltäckning för att underlätta insatser för att släcka skogsbranden. Eftersom skogsbranden riskerade att skapa en störning för mobilkommunikationen, som är en del av telekommunikationen, bidrog samarbetet med den externa aktören till Telekommunikations robusthet. Även om åtgärderna är tekniska är samarbetet i sig en organisatorisk faktor som ökar robustheten inom den kritiska infrastrukturen. Samarbetet inom den kritiska infrastrukturen bedöms vara ett *samarbete kopplat till robustheten* som aktörerna arbetar med i lägre grad.

Tekniska faktorer

- Under intervjun samt i mejlkontakt uppgav Aktör G att de samverkar med andra aktörer inom telekommunikation för att planera specifika robusthetshöjande åtgärder. Aktör G uppgav att de finansierat utökad kapaciteten i vissa av de fasta reservkraftverk som finns inom Telekommunikation. Aktör G berättade även att det inom den kritiska infrastrukturen finns transportabla reservkraftverk som de har finansierat. Detta är något som ökar robustheten inom den kritiska infrastrukturen Telekommunikation eftersom det skapas en buffert för att bättre stå emot störningar orsakade av elavbrott. Aktör G bedöms arbeta med *bufferts* inom den kritiska infrastrukturen i högre grad.
- Aktör G förklarade under intervjun att det i näten finns redundans i form av flera parallella fiberkablar ifall en skulle grävas av. Detta är något som gjorts inom den kritiska infrastrukturen Telekommunikation. Ett annat exempel på redundans som Aktör G

berättade om var att det inom den kritiska infrastrukturen finns transportabla mobilbasstationer som stärker upp mobilnätet, vilket bedöms vara redundans i den egna kapaciteten. Både Aktör G och andra aktörer inom den kritiska infrastrukturen bedöms, utifrån informationen, arbeta med *redundanta system eller en inbyggd redundans i systemen* i högre grad.

Återhämtning

Organisatoriska faktorer

- Under intervjun berättade Aktör G att de kan bidra med samordning vid en störning för att stödja återhämning av den kritiska infrastrukturen. Det framkom inga fler resurser som kan bedömas som organisatoriska. Aktör G bedöms arbeta med *organisatoriska resurser* för återhämtning inom den kritiska infrastrukturen i lägre grad.
- Aktör G berättade under intervjun att de arbetar med att bemanna krisstaben enligt bemanningsschema där de har tagit hänsyn till att personal ska kunna återhämta sig vid långsiktiga störningar. Abetet med bemanningsschemat anses vara en plan för resurshantering inom Akötr G:s egna verksamhet. Aktör G bedöms endast arbeta med *planer för ledning och koordination för resurshantering* i lägre grad.
- Aktör G samarbetar främst med andra aktörer genom en nationell samverkansgrupp där Aktör G bidrar med informationsdelning. Syftet med samarbetet i den nationella samverkansgruppen är att ge stöd för att återställa den kritiska infrastrukturen efter störningar. Detta framkom del under intervjun, dels från mejlkontakt med Aktör G. Eftersom samarbetet för återhämtning enbart inriktar sig på informationsspridning bedöms Aktör G endast arbeta med *samarbete för återhämtning* inom den kritiska infrastrukturen i lägre grad.
- Aktör G har flera utbildningar med fokus på att stödja ökad krishanteringsförmåga inom den kritiska infrastrukturen. Utbildningarna finns beskrivna på Aktör G:s hemsida. Aktör G övar på informationsflöden och lägesbilder vilket troligen bidrar till förmågan för återhämtning inom den kritiska infrastrukturen eftersom information är viktigt för att kunna vidta rätt åtgärder för snabbare återhämtning. Aktör G övar även på att gå in i höjd beredskap med övningar där de har motspel och testar olika scenarier. Aktör G anses ha övningar för återhämtning både för sin egen verksamhet och för återhämtningsförmågan inom den kritiska infrastrukturen. Aktör G bedöms arbeta med *övningar kopplade till återhämtning* inom den kritiska infrastrukturen i högre grad.
- Aktör G förklarade under intervjun att det finns flera kontinuitetsplaner inom den kritiska infrastrukturen som aktörer arbetar med kontinuerligt. Planerna har exempelvis uppdaterats under Covid-19 pandemin. Aktör G berättade även att de har kontinuitetsplaner för de egna kritiska systemen, exempelvis IT-systemen. Aktör G förklarade att det finns flera kontinuitetsplaner för både verksamheten och infrastrukturen samt att dessa uppdateras kontinuerligt. Det bedöms att det sker ett arbete med *strategier med fokus på återhämtning* inom den kritiska infrastrukturen i högre grad.

Tekniska faktorer

- Under mejlkontakt berättade Aktör G att de har finansierat reservkraftverk och transportabla mobilstationer som finns ute hos operatörer inom Telekommunikation. Reservkraftverken bedöms vara tekniska resurser för återhämtningen eftersom de kan användas efter en

störning orsakat av elavbrott. De transportabla mobilbasstationerna bedöms vara en teknisk resurs för återhämtning eftersom de gör att tillfälliga stationer kan sättas upp för att återhämta funktionen, exempelvis om kritiska noder i telekomnätverket slås ut. Eftersom de tekniska resurser som finns inom Telekommunikation enbart berör el-relaterade störningar bedöms Aktör G och andra aktörer inom den kritiska infrastrukturen arbeta med *tekniska resurser för återhämtning* inom den kritiska infrastrukturen i lägre grad.

Anpassning

Organisatoriska faktorer

- Aktör G följer upp och utvärderar hur andra aktörer inom telekommunikation arbetar med anpassning. Under mejlkontakt framkom det att detta görs på olika sätt, bland annat genom planerad eller händelsestyrd tillsyn av andra aktörer inom Telekommunikation eller genom utvärderingar. Under intervjun berättade Aktör G att de efter större störningar, så som stormar och skogsbränder, har gjort utvärderingsrapporter. Rapporterna resulterade i listor med åtgärder som dels behövdes göras inom Aktör G:s egna verksamhet, dels inom den kritiska infrastrukturen. Aktör G anses stödja arbetet med *uppföljning och utvärdering i lärande syfte* inom den kritiska infrastrukturen i högre grad.
- En organisatorisk åtgärd som Aktör G berättade om under intervjun är att de, baserat på tidigare störningar, tydliggjort vad som gäller om man kallas in under semestern. Man har även nyligen uppdaterat styrande dokument så som krisplanen, bland annat utifrån lärdomar från Covid-19 pandemin. I krisplanen uppdaterades exempelvis TIB rollen och information om när krisplanen ska aktiveras. Listorna med åtgärder som angavs i faktorn ovan anses vara en organisatorisk åtgärd som Aktör G använder för att få andra aktörer inom den kritiska infrastrukturen att anpassas. De organisatoriska åtgärderna som Aktör G presenterade under intervjun bedöms påverka anpassningen både för Aktör G och för flertal aktörer inom den kritiska infrastrukturen. Aktör G bedöms därför arbeta med *organisatoriska åtgärder* i högre grad.
- I den nationella samverkansgruppen som Aktör G ingår i sker det, enligt Aktör G, utbyte av erfarenheter exempelvis lärdomar från tidigare händelser. Inom gruppen diskuteras även tänkbara åtgärder. Aktör G berättar att den nationella samverkansgruppen bygger på förtroende mellan aktörerna och de har fysiska möten ungefär två gånger om året. Eftersom det endast finns ett forum som används vid erfarenhetsutbyte bedöms Aktör G arbeta med *erfarenhetsutbyte med andra aktörer* i lägre grad.

Tekniska faktorer

- Det enda tekniska systemet som Aktör G nämnde under intervjun som kan användas för uppföljning och utvärdering i lärande syfte är GIS. Det anses inte finnas tillräckligt med information om hur GIS används som *tekniskt system för uppföljning och utvärdering i lärande syfte* för att göra en bedömning av Aktör G:s arbete med faktorn.
- Under intervjun framkom flera tekniska anpassningsåtgärder, exempelvis har känslig utrustning anlagts i bergrum, noder säkrats genom att gräva ner dem och sjökablar förstärkts för att minska risken för skada orsakat av fartygsankare. Aktör G berättade även under intervjun att de lägger ledningar under vattendrag istället för på broar för att inte riskera att påverkas av dammbrott som kan rasera broarna. Ytterligare tekniska åtgärder framkom under mejlkontakt då Aktör G berättade att de arbetar med andra åtgärder inom den kritiska

infrastrukturen genom privatoffentlig samverkan, det vill säga där åtgärder görs i operatörernas nät men finansieras från Aktör G. Det är åtgärder kopplade till förstärkning av noder och nät. Eftersom det framkom flera exempel på hur Aktör G arbetar med tekniska åtgärder inom den kritiska infrastrukturen Telekommunikation bedöms Aktör G arbeta med *tekniska åtgärder* inom den kritiska infrastrukturen i högre grad.

Aktör H

Förutseende

Organisatoriska faktorer

- Från intervju, enkät och information från Aktör H:s hemsida framkom det att Aktör H dels har målet att tillgodose det digitala behovet, dels göra det möjligt för alla att använda digitala tjänster. Aktör H bedöms arbeta med *tydliga mål* för den kritiska infrastrukturen i högre grad.
- Under intervjun med Aktör H framkom det att de samlar in information via en nationell samverkansgrupp, MSB och andra forum där det enligt Aktör H förs dialoger och utbyts information. Enligt Aktör H måste man aktivt gå med i nätverken och de anser att det är för många nätverk för att kunna gå med i alla. Aktör H berättade att de upplever att nuvarande situation gällande nätverk inte är effektiv och utryckte under intervjun att det saknas något som knyter samman alla nätverk. Även om Aktör H säger att det inte är effektivt att samla in information från de forum som finns så bedöms Aktör H genom sin medverkan i flera olika nätverk arbeta med *organisatoriska system för informationsinsamling* i högre grad.
- Från intervjun berättade Aktör H att det finns personal inom Telekommunikation som analyserar systemen dygnet runt för att detektera händelser. Den metod som Aktör H själv använder för att analysera information är genom de forum Aktör H medverkar i. Enligt Aktör H används forumen för att diskutera vilka åtgärder som behövs göras inom Telekommunikation. Inom den kritiska infrastrukturen bedöms, utifrån Aktör H:s intervjusvar, insamlad information analyseras både på nätnivå och generellt för den kritiska infrastrukturen. Detta gör att Aktör H anses arbeta med *organisatoriska system för analys* i högre grad.
- Aktör H bedöms själv inte ha förmåga att uppmärksamma signaler då de inte har egna övervakande system och enbart får rapporter om störningar när de redan hänt. Däremot samlar Aktör H in viss information från andra aktörer via forum och analyserar denna. Dessutom berättade Aktör H att andra aktörer inom Telekommunikation använder SCADA-system. Aktör H har alltså en förmåga att samla in och hantera information samtidigt som Aktör H berättade att det inom Telekommunikation finns en förmåga att hantera och analysera specifika data (SCADA-system). Även om det inte är Aktör H som i sig arbetar med SCADA-system så ses Aktör H som en representant för de aktörer inom Telekommunikation som gör det. Baserat på detta bedöms Aktör H arbeta med att *uppmärksamma otydliga signaler och indikationer* i högre grad.

Tekniska faktorer

- Det tekniska system Aktör H angav under intervjun som de själva använder för informationsinsamling är operational technology (OT). Inom den kritiska infrastrukturen nämnde Aktör H att SCADA-system används för insamling av information inom

Telekommunikation. De tekniska system som används för informationsinsamling inom Telekommunikation samlar in information från flera områden som kan påverka funktionen. Den kritiska infrastrukturen bedöms arbeta med tekniska *system för informationsinsamling* i högre grad.

- Under intervjun berättade Aktör H att SCADA-system används inom Telekommunikation för att analysera information. Det nämndes inget annat tekniskt analyssystem som används inom den kritiska infrastrukturen. Eftersom SCADA bedöms vara ett omfattande system för att analysera information bedöms den kritiska infrastrukturen arbeta med *tekniska system för analys* i högre grad.

Robusthet

Organisatoriska faktorer

- Från det insamlade materialet framkom det inga exempel på övningar som kan kopplas till robusthet. Det anses inte finnas tillräcklig information om hur Aktör H arbetar med *övningar kopplat till robusthet* för att göra en bedömning om arbetet med denna faktor.
- Under intervjun berättade Aktör H att aktörer inom den kritiska infrastrukturen följer vägledningar som stödjer säkerhetsarbetet och ökar robustheten inom telekommunikationen. Enligt Aktör H har dessa vägledningar höjt säkerhetsstandarden inom den kritiska infrastrukturen och därmed ökat robustheten. Vägledningarna anses vara en typ av plan för ökad robusthet. Från mejlkontakt med Aktör H framkom det även att vägledningarna har förbättrat möjligheterna kring framtida underhållsarbeten och utveckling inom Telekommunikation vilken också bidrar till den kritiska infrastrukturens robusthet. Aktör H nämnde under intervjun att telekommunikationens funktion inte drabbats under Covid-19 pandemin trots ökningen i användningen, vilket anses tyda på en god planering inför oönskade händelser. Aktörerna inom telekommunikation bedöms utifrån Aktör H:s beskrivningar arbeta med *planer för oönskade händelser* i högre grad.
- Aktör H berättade under intervjun att de vägledningar som finns inom Telekommunikation har implementerats av majoriteten av aktörerna inom den kritiska infrastrukturen. Vägledningarna är frivilliga och faktumet att dessa används av nästan alla aktörer inom Telekommunikation visar på att det finns ett samarbete mellan aktörerna. Aktör H bedöms arbeta med *samarbete kopplat till robusthet* inom den kritiska infrastrukturen i lägre grad.

Tekniska faktorer

- Under intervjun med Aktör H framkom det ingen information om Aktör H bidrar eller stödjer lager, reserver eller annan typ av buffert för den kritiska infrastrukturen. Till vilken grad Aktör H arbetar med *buffert* inom den kritiska infrastrukturen kan därför inte bedömas.
- Under intervjun berättade Aktör H att alla system inom den kritiska infrastrukturen är redundanta. Exempel som gavs av Aktör H är att en standardnod inom den kritiska infrastrukturen har sju till åtta redundanta system för att klara av basnivån vid en störning. Aktör H förklarade även att det finns krav på redundanta lösningar, både på passiv nivå så som kablar och på aktiv nivå. Aktör H bedöms arbeta med *redundanta system eller en inbyggd redundans i systemen* i högre grad.

Återhämtning

Organisatoriska faktorer

- Under intervjun berättade Aktör H att man inom den kritiska infrastrukturen kan låna personal av varandra vid störningar. Stödet med personal går smidigt eftersom personalen har kompetens som gör att de kan bistå i andra aktörers arbete utan ytterligare utbildning. Eftersom tillgång till kompetent personal anses vara en viktig faktor för att kunna återhämta systemet inom telekommunikationen, bedöms Aktör H arbeta med *organisatoriska resurser* i högre grad.
- Aktör H berättade under intervjun att det finns ett forum för att koordinera resurser inom den kritiska infrastrukturen vid en störning. Forumet innebär att aktörer inom den kritiska infrastrukturen kan göra förfrågningar om resursförstärkningar vid störningar. Genom forumet anses Aktör H, tillsammans med andra aktörer inom telekommunikationen, bidra till en *plan för ledning och koordination för resurshantering* inom telekommunikation vid en störning och bedöms därför arbeta med denna faktor i högre grad.
- Det samarbete som finns mellan aktörer inom den kritiska infrastrukturen bidrar till att frigöra både organisatoriska som tekniska resurser som kan användas vid återhämtning efter en störning i telekommunikationen. Aktör H samarbetar även med andra aktörer i den kritiska infrastrukturen genom en nationell samverkansgrupp där det sker informationsdelning. Samarbetet antas bidra till att effektivare återställa funktionen efter en störning genom att information om materialtillförsel, skydd och lägesbilder delas. Eftersom samarbetet för återhämtning av den kritiska infrastrukturen riktar sig på både informationsspridning och delandet av resurser, bedöms Aktör H arbeta med *samarbete för återhämtning* inom den kritiska infrastrukturen i högre grad.
- Under intervjun berättade Aktör H att de varje år övar på hotbilder som anses kritiska. Övningarna fokuserar på agerande efter att en störning inträffat och anses därför ha fokus på återhämtning. Aktör H berättade även under intervjun att de ska genomföra övningar med Rakel. Tekniska resurser bidrar till förmågan att återhämtas, och Aktör H sa under intervjun att de kontinuerligt testar att de tekniska resurserna fungerar som de ska. Sammantaget arbetar Aktör H med flera slags övningar kopplade till återhämtning för den kritiska infrastrukturen och Aktör H bedöms därför arbeta med *övningar kopplade till återhämtning* i högre grad.
- Aktör H arbetar med andra aktörer för att det ska finnas en gemensam strategi för att hantera störningar. Ett exempel på detta är att Aktör H tillsammans med andra aktörer arbetar med att noder inom telekommunikationen ska vara överföringsbara mellan aktörer via ett utbytesprogram så att en nod snabbt kan ersättas om den går sönder. Från intervjun framkom det att Aktör H lägger mycket fokus på att skapa gemensamma strategier och Aktör H bedöms därför arbeta med *strategier med fokus på återhämtning* inom den kritiska infrastrukturen i högre grad.

Tekniska faktorer

- Under intervjun berättade Aktör H att det finns reservnoder och Rakel-system som båda är exempel på tekniska resurser. Det finns även ett tekniskt verktyg som används för att underlätta koordinationen av resurser mellan aktörer vid en störning inom telekommunikationen. Det tekniska verktyget har en funktion som skickar ut viktig information i olika kommunikationskanaler vilket underlättar koordineringen av resurser.

Telekommunikation är en kritisk infrastruktur där det finns mycket tekniska resurser bland aktörerna som används av aktörerna för att upprätthålla funktionen. Eftersom Aktör H ingår i samarbeten där resurser delas och lånas mellan aktörer (se ovan) så tillgängliggörs de tekniska resurserna bland aktörer för hela den kritiska infrastrukturen vid en störning. Aktör H bedöms därför arbeta med faktorn *tekniska resurser för återhämtning* inom den kritiska infrastrukturen i högre grad.

Anpassning

Organisatoriska faktorer

- Aktör H följer upp och utvärderar hur andra aktörer inom telekommunikation arbetar med vägledningarna kopplat till robusthet. Utvärderingen av detta görs genom enkäter och utbildningar kring vägledningarna. Aktör H beskrev även under intervjun att de finns besiktningsmän som följer upp hur väl vägledningarna används av aktörer inom den kritiska infrastrukturen. En annan utvärdering Aktör H berättade om under intervjun att de har återkommande workshops där de diskuterar och utvärderar tidigare störningar inom telekommunikationen med andra aktörer i lärande syfte. Bland annat utvärderas hur tidigare störningar hanterades, och hur större störningar ska hanteras i framtiden. Aktör H anses bidra till arbetet med *uppföljning och utvärdering i lärande syfte* inom den kritiska infrastrukturen i högre grad.
- Under intervjun förklarade Aktör H att det är vanligare med störningar av antagonistiska slag när det sker vid uppdatering av nät (4G byts till 5G) och att de som åtgärd inför höjd beredskap för att stå emot dessa. En annan organisatorisk åtgärd som Aktör H berättade att de infört vid uppdatering av nät är att det görs sociala kampanjer, detta för att upplysa samhället och därigenom förebygga de antagonistiska störningarna som påverkar den kritiska infrastrukturen Utöver detta berättade Aktör H att de släpper nya vägledande dokument varje år där de inkluderar lärdomar från workshops som andra aktörer inom den kritiska infrastrukturen kan ta till sig. I de vägledande dokumenten listas ett antal organisatoriska minimikrav för den kritiska infrastrukturen så att funktionen upprätthålls. Eftersom de organisatoriska åtgärderna berör hela den kritiska infrastrukturen både genom åtgärder som Aktör H implementerar och genom stöd för att implementera åtgärder inom den kritiska infrastrukturen. Aktör H bedöms därför arbeta med *organisatoriska åtgärder* inom den kritiska infrastrukturen i högre grad.
- Aktör H är med i en nationell samverkansgrupp där det, enligt Aktör H, sker utbyte av erfarenheter. Även i det forum för resurskoordinering som Aktör H ingår samt de workshops som Aktör H deltar i sker det erfarenhetsutbyte kring tidigare störningar som aktörer drabbats av. Under intervjun framkom det alltså exempel på hur Aktör H utbyter erfarenheter med andra aktörer, men Aktör H underströk att erfarenhetsutbytet endast sker mellan aktörer inom telekommunikation i deras ’’telekombubbla’’. Enligt Aktör H sker det inget erfarenhetsutbyte med andra samhällsaktörer, och Aktör H ansåg att detta var en brist i deras arbete. Eftersom utbyte med aktörer även utanför den kritiska infrastrukturen anses viktig för förmågan att anpassas så bedöms Aktör H arbeta med *erfarenhetsutbyte med andra aktörer* i lägre grad.

Tekniska faktorer

- Inom den kritiska infrastrukturen används SCADA system vilket är ett tekniskt system som anses kunna användas för att följa upp tidigare händelser. Detta eftersom systemet bland annat samlar in information från tidigare händelser och sammanställer denna. Detta var det system som Aktör H under intervjun berättade om som kan kopplas till tekniska system för uppföljning och utvärdering i lärande syfte. Eftersom SCADA-system anses vara ett stort system för analysering bedöms den kritiska infrastrukturen arbeta med *tekniska system för uppföljning och utvärdering* i högre grad.
- Under intervjun med Aktör H framkom inga större tekniska åtgärder som genomförts i förebyggande syfte. Exempel som gavs under intervjun är att kameror installerats för att förebygga antagonistiska störningar. I de vägledande dokumenten som Aktör H arbetar med inom den kritiska infrastrukturen listas ett antal tekniska minimikrav. Hur väl kraven implementerats inom den kritiska infrastrukturen kan däremot inte bedömas. Informationen om Aktör H:s arbete med att *implementera tekniska förebyggande åtgärder* anses inte vara tillräcklig för att göra en bedömning av hur Aktör H arbetar med denna faktor.