



OKTOBER 2022

Resilient och trygg elförsörjning

En syntesrapport om forskningsläget och framtida
forskningsbehov

Rapportförfattare:

Jesper Werneskog & Johanna Barr, Power Circle

på uppdrag av Energimyndigheten

Innehållsförteckning

Sammanfattning	3
1 Syfte	6
2 Bakgrund	7
2.1 Vad innebär resilient och trygg elförsörjning?	8
3 Forskning på området resilient och trygg elförsörjning idag	9
3.1 Tematiska forskningsområden	9
3.2 Vilka bedriver forskningen?	11
3.2.1 Akademi och forskningsinstitut	11
3.2.2 Näringslivets aktörer	13
3.2.3 Offentlig sektor	14
3.3 Vilka finansierar forskningen?	15
3.3.1 Energimyndigheten	16
3.3.2 Energiforsk	16
3.3.3 Myndigheten för samhällsskydd och beredskap (MSB)	17
3.3.4 Svenska kraftnät	17
3.4 Större projekt och satsningar	17
3.4.1 Swedish Centre for Smart Grids and Energy Storage (SweGRIDS)	18
3.4.2 Resilient Information and Control Systems (RICS)	18
3.4.3 Centre for Critical Infrastructure Protection research (CenCIP)	18
3.4.4 Center for Resilient Critical Infrastructures (CERECS)	18
3.4.5 Centrum för cyberförsvar och informationssäkerhet (CDIS)	19
3.4.6 Cyber range och Cyber Range and Training Environment (CRATE)	19
3.4.7 Digital Futures	19
3.4.8 Systemförändring: Energigemenskaper	19
3.4.9 Resilient Energy Systems Competence Centre (RESILIENTa)	20
3.5 Internationell utblick	20
4 Tillämpning av forskningen	22
5 Identifierade behovsområden för framtida forskning	23
5.1 Resilient och trygg elförsörjning i ett elektrifierat och digitaliserat samhälle	24
5.2 Systemperspektiv och tillräcklighet	25
5.3 Drift och underhåll av elnätet	26
5.4 Informations-, kommunikations- och cybersäkerhet	27
5.5 Utveckling av modellverktyg och testbäddar	28
5.6 Humanistisk och samhällsvetenskaplig forskning	28
5.7 Tillgång till kompetens	29
Referenslista	31

Bilaga A: Medverkande respondenter	33
Bilaga B: Genomförande	34
Förstudie	34
Intervjustudie	34
Enkätstudie	34
Skrivbordsstudie	35
Analys av inhämtad information	35



Sammanfattning

Det svenska energisystemet genomgår just nu stora förändringar. Samhället elektrifieras och produktionsmixen förändras och decentraliseras, vilket leder till nya utmaningar för att säkerställa tillräcklighet, elsystemets stabilitet och elens kvalitet. Elnätets komponenter digitaliseras och kopplas upp, vilket skapar nya möjligheter men också nya sårbarheter. Samtidigt påverkas Sverige av händelser i vår omvärld; med klimatkris, den globala pandemin och den pågående invasionen av Ukraina.

Sammantaget leder detta till nya utmaningar med att upprätthålla en resilient och trygg elförsörjning med ett påföljande behov av forskning och utveckling på området. För att ge en bild av det nuvarande forskningsläget på området har Power Circle fått i uppdrag av Energimyndigheten att ta fram denna syntesrapport. Syntesen baseras till stor del på intervjuer med, och enkätsvar från, forskare och behovsägare som arbetar med frågor kopplade till området. Syntesrapporten har till syfte att ge en översiktlig sammanställning av den forskning som bedrivs på området i Sverige idag, och forskningsbehov kopplade till området, samt att återge en bild av hur forskningen som tas fram finansieras och tillämpas i praktiken.

Det är tydligt att forskningsområdet resilient och trygg elförsörjning är brett och innefattar många discipliner och ämnesområden, men också att synen på innebörden av resilient och trygg elförsörjning inte är entydig bland respondenterna. Begreppen *resiliens* och *trygg elförsörjning* betonar olika perspektiv och kompletterar varandra. Det har lyfts fram att ett resilient system inte behöver vara tryggt, och tvärt om. Båda begreppen har däremot samma slutmål: att elen ska levereras till kunden på ett tillförlitligt sätt, både under normala driftsförhållanden och i en beredskapssituation.

Syntesrapporten har ett huvudfokus på tekniska aspekter av området och från intervjustudien framgår det att i stort sett alla lärosäten som bedriver forskning inom elektronik eller datavetenskap kommer i kontakt med frågor som berör resilient och trygg elförsörjning. I denna studie har forskare med bakgrund i ämnesområden såsom elkraftteknik, energivetenskap, nätverk och systemteknik, energisystem, informationsteknologi och realtidssystem bidragit med sina perspektiv. I studien har också näringslivsaktörer, såsom energi- och elnätsbolag samt teknikleverantörer, fått ge sina inspel. Baserat på intervju- och enkätstudien har den pågående forskningen som bedrivs i Sverige idag, kategoriserats in i följande tematiska områden:

- Tillförlitlig design och drift
- Systemets tillräcklighet
- Prediktivt och optimerat underhåll
- Digitaliseringen av elnäten
- Säker informationshantering
- Cybersäkerhet
- Samhällsviktig infrastruktur i ett bredare perspektiv.

Inom de tematiska områdena kan frågeställningar röra både leveranssäkerhet under normala driftsförhållanden, samt beredskap vid kriser och angrepp.

I tillägg till den tekniska forskningen bedrivs det forskning inom humanistiska och samhällsvetenskapliga discipliner, och många respondenter nämner ett ökande fokus på tvärvetenskaplig forskning inom området.

Till följd av områdets breda omfattning finns det många aktörer som finansierar dagens forskning. Energimyndigheten och Energiforsk har nämnts som ett par av de större finansiärerna. Andra finansiärer är MSB, Formas, Vinnova, Vetenskapsrådet, RISE, FOI, Svenska kraftnät, näringslivsaktörer, stiftelser och olika typer av EU-finansiering. **Det finns ett flertal större finansieringssatsningar på området, i form av forskningscentrum där kompetens och långsiktiga forskningsmiljöer byggs upp.** Majoriteten av de identifierade pågående satsningarna har en teknisk inriktning, med fokus på frågor kring informationssäkerhet, cybersäkerhet och digitalisering, men det finns även multidisciplinära satsningar med fokus på bland annat ökad förståelse för samhällets beroende av samhällsviktig infrastruktur.

När det kommer till framtida forskningsbehov kräver många av dagens frågor ett fortsatt fokus även i framtiden. Eftersom omställningen av elsystemet medför att det uppstår nya frågor och utmaningar efterlyser studiens respondenter i tillägg fler satsningar för att bygga upp en bred och långsiktig kompetens på området.

De identifierade områdena med behov av ökad kunskap och forskning har kategoriserats in i tematiska områden. Inom området **Resilient och trygg elförsörjning i ett elektrifierat och digitaliserat samhälle** finns behovet av kunskap och gemensam förståelse för vilka faktorer och värden som ska uppfyllas för att elsystemet ska anses vara tryggt och resilient. Frågor inom området är: *Hur definierar vi ett resilient elsystem och borde bilden av vad ett resilient elsystem är uppdateras när samhället går mot ett allt större elberoende? Hur lång tid klarar sig olika kunder under ett elavbrott? Vilka hotbilder finns framöver och hur kan de mötas upp?*

Inom **Systemperspektivet och tillräcklighet** efterfrågas forskning med ett brett systemperspektiv för att klargöra hur resilient och trygg elförsörjning kan uppnås parallellt med omställningen av energisystemet. Frågor som behöver besvaras är: *Vilka utmaningar står systemet inför med förändrad produktionsmix, hur ska systemets tillräcklighet hanteras, särskilt vid effektunderskott som kan ske under vintrar eller kriser? På vilket sätt kan energilager, flexibilitetslösningar och mikronät bidra till tillräckligheten under normaldrift och i kris?*

Drift och underhåll av elnätet behöver utvecklas i takt med omställningen för att säkra systemets stabilitet, elkvalitet, och driftsäkerhet. Arbetet ställs om från analogt och reaktivt till digitaliserat och proaktivt, vilket ger nya möjligheter att optimera drift och underhåll samt reducera risker. Frågor som tagits upp är: *Hur påverkas övertoner, rotationsenergi och kortslutningseffekt av en ökad andel kraftelektronik i systemet? och Hur kan digitalisering bidra till att öka elnätets resiliens med hjälp av övervakning och riskbedömningar i realtid?* Flera gånger

under studien har vikten av att undersöka vilka, positiva och negativa, konsekvenser nya skydds- och styrsystem får på elsystemet för att minimera oförutsedda effekter. För att säkra driften av systemet vid kriser ses också ett behov av mer kunskap kring vilka delar av leveranskedjan som är kritiska för att systemet ska fungera och som är beroende av ett annat land.

Till följd av digitaliseringen av elnätet finns det ett stort behov av arbete med **Informationskommunikations- och cybersäkerhet**. Det efterfrågas forskning och utveckling kring design av säkra system och identifiering av intrång, bland annat genom AI. Det finns behov av att besvara frågor likt *hur känsliga är nya komponenter och system för cyberattacker?* och *Vilka konsekvenser riskerar att uppstå vid samordnade överbelastningsattacker mot informations- och kommunikationsinfrastrukturen i elsystemet, och hur kan konsekvenserna minimeras?*

En problematik som har lyfts fram i studien är avsaknaden av testanläggningar för komponenter i elsystemet samt målkonflikten kring tillgång till modeller som bygger på verklig data från elsystemet för akademien. Inom **Utveckling av modellverktyg och testbäddar** efterfrågas därför testanläggningar där nya komponenter kan testas i större system samt vidare arbete med hur målkonflikten kring sekretess och tillgång till data kan hanteras.

Trots syntesens tekniska fokus har under arbetets gång flertalet frågor inom **Humanistisk och samhällsvetenskaplig forskning** identifierats, då det finns både ekonomiska, juridiska och beteendemässiga dimensioner av ett tryggt och resilient system. Frågor är exempelvis: *Hur påverkar priset på el den av kunderna upplevda tillräckligheten och trygghet?* *Vilka samhällskostnader uppstår om elnätet inte är resilient?* *Vilka nya risker kan uppstå i ett samhälle som är allt mer beroende av elsystemet, och hur ska riskerna värderas mot varandra?* Det finns även frågor som rör individers och organisationers beteende i beredskapssituationer.

Om än inte ett strikt forskningsbehov, så lyfts även kompetensförsörjning som ett viktigt tema framåt, där ett delbehov är kompetensförsörjningen hos mindre aktörer såsom lokala elnätsbolag.



1 Syfte

Denna syntesrapport är framtagen av Power Circle inom ramen för det upphandlade stödprojektet Sprida SamspeL och ska bidra till att ge Energimyndigheten en översiktlig sammanställning av pågående forskning, finansiärer av forskningen och behovsområden för framtida forskning på området resilient och trygg elförsörjning. Dessutom ska syntesrapporten återge en överblick av hur forskningen som tas fram tillämpas i praktiken.

Rapporten ska fokusera på resilient och trygg elförsörjning, med utgångspunkt i avgränsningen infrastruktur, produktionsanläggningar, IT-säkerhet och energigemenskaper. Avgränsningen har legat till grund vid valet av respondenter till syntesrapportens intervju- och enkätstudie, och har därmed riktat in arbetet mot primärt tekniska frågor. Under arbetets gång har emellertid även samhällsvetenskapliga aspekter fångats upp.

Syntesrapporten ämnar att återge en översikt av området resilient och trygg elförsörjning och forskningens roll i detta, samt att besvara följande frågeställningar:

- Hur tillämpas den forskning och utveckling som tas fram?
- Vilket behov av forskning inom resilient och trygg elförsörjning finns i Sverige idag?
- Vad är behovet av resurser och insatser (såsom exempelvis finansiering, samarbeten, pilotprojekt, etc.) för att kunna genomföra forskning inom området?

Det ska nämnas att området är brett och analysen ger en översiktlig, men inte komplett, bild av området och dess forskningsfront. Syntesrapporten gör även en kort internationell utblick, där respondenterna fått svara på frågor om goda exempel på forskning i utlandet och i vilken mån det förekommer forskningssamarbeten mellan svenska och internationella aktörer.



2

Bakgrund

Det svenska energisystemet genomgår just nu stora förändringar. Samhället elektrifieras och produktionsmixen förändras och decentraliseras, vilket leder till nya utmaningar för att säkerställa tillräcklighet under årets alla timmar, elsystemets stabilitet och elens kvalitet. Elnätets komponenter digitaliseras och kopplas upp, vilket möjliggör ett mer resurseffektivt och optimerat system, men vilket också skapar nya sårbarheter.

Sveriges elnät blir även alltmer sammankopplat med andra länder. Samtidigt påverkas Sverige av händelser i vår omvärld – med klimatkris, den globala pandemin och den pågående invasionen av Ukraina. Sammantaget leder detta till nya utmaningar med att upprätthålla en resilient och trygg elförsörjning. Under 2020 och 2021 har antalet cyberattacker fortsatt att öka samtidigt som deras påverkan blir allt större¹. European Union Agency for Cybersecurity (ENISA) har också sett att fler cyberattacker riktar in sig på samhällsviktig infrastruktur så som sjukvård, transport och energi. Cyberattacken som slog ut Ukrainas elnät 2015 har av många respondenter i denna studie pekats ut som det stora uppvaknandet i samhället.

Den nationella elektrifieringsstrategin tar upp trygg elförsörjning som ett av tolv fokusområden med bakgrund av att ett elsystem med hög leveranssäkerhet, låg miljöpåverkan och el till konkurrenskraftiga priser har varit och kommer fortsätta vara avgörande för Sveriges välbefinnande. Strategin betonar att en elförsörjning som inte upplevs som trygg och tillförlitlig kommer att bromsa elektrifieringen. En trygg elförsörjning definieras av leveranssäkerhet och beredskap – där det tidigare fokuserar på tillräcklighet och driftsäkerhet i systemet, och det senare behandlar förmågan att hantera kriser och motstå angrepp. I strategin finns det beskrivet att mål för leveranssäkerheten ska sättas, att effektreservens framtid ska tydliggöras och en effektiv tillsynsverksamhet för driftsäkerheten ska utvecklas. Förmågan att hantera kriser ska utvecklas med hjälp av internationellt samarbete kring beredskapsfrågor och en utvecklad elberedskap. Enligt strategin är grunden i en trygg elförsörjning ett väl fungerande samspel mellan aktörer. För att samspelet ska fungera är effektiva elmarknader en förutsättning, vilket möjliggörs via digitaliseringen som i sin tur ställer krav på en god informations- och cybersäkerhet.²

Sveriges regering beslutade även 2017 om en nationell strategi för samhällets informations- och cybersäkerhet. I strategin nämns vikten av säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet för att öka säkerheten i nätverk, produkter och system samt stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra IT-incidenter. Möjligheten till att förebygga och bekämpa it-relaterad brottslighet ska också

¹ Enisa (2022), [ENISA THREAT LANDSCAPE 2021](#)

² Regeringen (2022), [Nationell strategi för elektrifiering – en trygg, konkurrenskraftig och hållbar elförsörjning för en historisk klimatomställning](#).

förbättras. Strategin betonar också vikten av att öka kunskapen och främja kompetensutvecklingen samt stärka det internationella samarbetet.³

I Sverige pågår också etableringen av ett nationellt centrum för cybersäkerhet⁴. Centrets syftet är att stärka Sveriges förmåga att förebyggande, upptäcka och hantera cyberangrepp. Centret ska även förmedla råd och stöd avseende hot, sårbarheter och risker samt verka som en nationell plattform för samverkan och informationsutbyte med privata och offentliga aktörer. Etableringen av verksamheten påbörjades 2020 och förväntas vara i full drift 2025. Centret består av FRA, Försvarmakten, MSB och Säkerhetspolisen. I juni fick MSB mot bakgrund av det förändrade säkerhetspolitiska läget dessutom i uppdrag av regeringen att stärka det nationella stödet för förebyggande och hantering av it-incidenter⁵, med målgrupper som andra myndigheter, företag, regioner och kommuner.

2.1 Vad innebär resilient och trygg elförsörjning?

För att kunna beskriva forskning som berör *resilient och trygg elförsörjning* behöver vi först förstå vad begreppet egentligen syftar till. Utifrån intervjustudien är det tydligt att området är brett och att det finns många olika perspektiv som ingår i det, men också att respondenterna i viss mån har olika syn på innebörden av resilient och trygg elförsörjning. Begreppen *resiliens* och *trygg elförsörjning* betonar olika perspektiv och kompletterar varandra. Det har lyfts fram att ett resilient system inte behöver vara tryggt, och tvärt om. Båda begreppen har däremot samma slutmål: att elen ska levereras till kunden på ett tillförlitligt sätt.

För att särskilja begreppen *resiliens* och *trygg elförsörjning* framgår det från respondenternas svar att *resiliens* fokuserar mer på hotbilder ur producenternas och leverantörernas perspektiv. Att elförsörjning är resilient har av de intervjuade beskrivits som infrastrukturens möjlighet att vara motståndskraftig, stå emot påfrestningar och förändringar, stora som små, samt återhämtningsförmåga. Påfrestningar kan vara av förutsedd eller oförutsedd natur, och orsaken bakom kan variera. Det kan handla om exempelvis tekniska, marknadsekonomiska, organisatoriska, klimatrelaterade eller antagonistiska hot. Vad som innefattas i begreppet beror också på hur systemgränserna sätts; fokus kan ligga på en enskild energigemenskap eller på det nationella transmissionsnätet. Frågor såsom återhämtningsförmåga och förmågan att anpassa sig till snabba förändringar och nya hotbilder har också lyfts in i begreppet.

Till begreppet *trygg elförsörjning* associeras flera områden som relaterar till att systemet levererar som det ska, samt ett större fokus på användarsidan. En trygg elförsörjning beskrivs som en elförsörjning där allt fungerar som förväntat och att kunderna har förtroende för systemet. Systemet har hög leveranssäkerhet, en tillförlitlig och förutsägbar drift och levererar el till ett rimligt pris. Ur ett nationellt perspektiv kan det handla om frågor kring huruvida landet har tillräckligt med produktion för att täcka konsumtionsbehovet.

³ Regeringen (2018), [Nationell strategi för samhällets informationsoch cybersäkerhet](#)

⁴ Nationellt cybersäkerhetscenter (2022), [Vårt uppdrag](#)

⁵ Regeringen (2022), [MSB stärker förebyggandet och hanterandet av it-incidenter](#)

3 Forskning på området resilient och trygg elförsörjning idag

I detta kapitel besvaras frågor om vad den svenska forskningen kring resilient och trygg elförsörjning innehåller i termer av frågeställningar och forskningsområden, vilka som bedriver forskningen, samt vilka som finansierar den.

3.1 Tematiska forskningsområden

Vid svenska universitet och högskolor samt näringslivet pågår det forskning och utveckling inom många områden som bidrar till en resilient och trygg elförsörjning. Till följd av den tekniska inriktningen på syntesrapporten har främst forskare som arbetar vid avdelningar likt elkraftteknik, energivetenskap, nätverk och systemteknik, energisystem, informationsteknologi och realtidssystem, samt näringslivsaktörer såsom energi- och elnätbolag och teknikleverantörer, intervjuats eller ombetts att besvara enkätstudien. De forskare och näringslivsaktörer som har intervjuats har framför allt bakgrunder inom matematik, elkraftteknik, reglerteknik, datavetenskap, IT, kemi och energisystem.

För att skapa en uppfattning om vilka frågeställningar som aktörerna arbetar med i dagsläget har intervju- och enkätstudiens respondenter fått berätta om pågående projekt. Utifrån detta har ett antal tematiska forskningsområden identifierats. Inom de tematiska områdena kan frågeställningar röra både leveranssäkerhet under normala driftsförhållanden, samt beredskap vid kriser och angrepp.

- **Tillförlitlig design och drift**, däribland frågor som rör utvecklingen av risk- och tillförlitlighetsmodeller samt -analyser; systemstabilitet, elkvalitet och stödtjänster; och skydd och tekniker för självläkande nät, mikronät och en ökad integration av HVDC. Ingår gör även tillgång till reservdelar och reservkraft, dödnätsstart och tekniska lösningar för extrema event såsom ödrift, samt klimatets påverkan på produktion och infrastruktur.
- **Systemets tillräcklighet**, med frågeställningar som rör hur vi bygger ut och optimerar elsystemet, både med tanke på tillräcklighet och resurs- och kostnadseffektivitet. Här ingår teman som energilager, efterfrågefleksibilitet, energigemenskaper, ödrift, mikronät, och lokal elproduktion.
- **Prediktivt och optimerat underhåll**, med bland annat utvecklingen av metoder och modeller för att optimera underhåll på exempelvis transformatorer och vindkraftverk.
- **Digitaliseringen av elnäten**, med frågor som rör digitalisering av komponenter i elsystemet, datadrivna analysverktyg, användningen av artificiell intelligens (AI) och machine learning (ML). Dessa frågor kan inte helt skiljas från "prediktivt och optimerat underhåll" och "tillförlitlig design och drift", då digitaliseringen är ett verktyg för att

utveckla dessa områden. Det pågår också projekt som fokuserar på att bygga digitala tvillingar för reglering och prediktion av komplexa system.

- **Säker informationshantering**, med frågeställningar såsom hur vi kan lita på och kontrollera att informationen som matats in i systemet är korrekt, hur kan vi spåra information som finns i systemet och garantera dess riktighet, hur vi hanterar kritisk information på ett säkert sätt samtidigt som vi digitaliserar, och hur vi bedömer säkerheten i olika system. Det pågår också projekt kring robust reglering och styrning, det vill säga hur automationssystem görs okänsliga mot störningar, och hur de hanterar olika scenarion med bristande eller fördröjd informationsinsamling och mätning.
- **Cybersäkerhet** är ett område som är integrerat i alla ovan nämnda områden, för att säkra driftsäkerheten i alltmer digitaliserade elsystem och verksamheter. Det pågår bland annat arbete med fokus på hur hot mot IT-system ska bemötas, upptäckas och hur systemen görs motståndskraftiga, utveckling och förbättring av metoder och modeller för att mäta och utvärdera säkerheten i system, för att identifiera svagheter och för att bygga upp en ökad säkerhet i elsystemet.
- **Samhällsviktig infrastruktur i ett bredare perspektiv**, med frågor såsom förståelse för hur samhällsviktiga infrastrukturer samverkar, samhällets beroende av energisystemet och vice versa, energisystemets beroende av tillgångar såsom bränsle, personal och kompetens.

Eftersom en resilient och trygg elförsörjning handlar om att elen ska levereras till konkurrenskraftiga priser under normaldrift, i tillägg till en beredskap för krissituationer, inbegriper området de flesta teman som relaterar till elsystemets funktion och utveckling. Många av de tematiska områdena ovan behandlas därför även inom andra forskningsprogram och satsningar (se bild nedan). Naturen på frågeställningarna kan dock skilja sig något. Exempelvis: flexibilitet och energilager är dellösningar för att skapa tillräcklighet i elsystemet och en fråga som hamnar inom ramen för forskning kring resilient och trygg elförsörjning kunna vara *Hur hanterar vi potentiella effektunderskott och vilken roll kan flexibilitet och energilager spela?* En fråga på samma tema som kan sägas hamna utanför ramen för området i denna syntes är *Hur ska lokala flexibilitetsmarknader utformas?*, även om denna fråga naturligtvis är nödvändig för att flexibilitet ska kunna bidra till systemets tillräcklighet.

För andra områden, exempelvis utveckling av optimerad drift och underhåll finns frågeställningar som fångas upp inom ramen för denna syntes, men som skulle kunna adresseras även i andra sammanhang. Å andra sidan, för flera av de tematiska områdena, såsom cybersäkerhet, säker informationshantering, digitalisering och samhällsviktig infrastruktur, handlar forskningen inte nödvändigtvis specifikt om elsystemet, men kan appliceras på det.

Respondenter som medverkat i kartläggningen har också påpekat vikten av den forskning som fokuserar på humanistiska och samhällsvetenskapliga aspekter av resilient och trygg elförsörjning, inom exempelvis statsvetenskap, nationalekonomi, företagsekonomi, sociologi och psykologi. Frågor som har nämnts är ekonomiska konsekvenser av ett icke-fungerade

system, juridiska frågor kopplade till digitalisering och användandet av data samt rättvisaspekter av omställningen.



3.2 Vilka bedriver forskningen?

Forskning och utveckling på området bedrivs inom akademi, näringslivet och inom offentlig sektor. I intervjustudien finns forskare från Kungliga Tekniska högskolan, Linköpings universitet, Luleå tekniska universitet, Lunds universitet, Mälardalens universitet och RISE representerade. I tillägg till detta har forskare från Mittuniversitetet, Mälardalens universitet, Högskolan i Skövde, Chalmers tekniska högskola, Blekinge tekniska högskola, Högskolan Väst och RISE svarat på enkäten. Från näringslivet finns Hitachi, Svenska kraftnät, Vattenfall, Jönköpings Energi, Ferroamp, Energiföretagen och Teknikföretagen representerade i intervjustudien. I tillägg till dessa har även elnäts- och energibolag samt länsstyrelser besvarat enkäten.

3.2.1 Akademi och forskningsinstitut

När det kommer till akademien är ett vanligt återkommande svar vid intervjuerna att i stort sett alla tekniska högskolor, forskningsinstitut och universitet som bedriver forskning inom området elkraft eller datavetenskap, kommer i kontakt med frågor som berör resilient och trygg elförsörjning. Det finns också forskningsprojekt som arbetar med frågor som relaterar till området resilient och trygg elförsörjning utan att ha den etiketten.

Forskning inom området kan ofta bedrivas på flera avdelningar på ett och samma universitet/högskola/institut. För att illustrera detta beskrivs nedan några exempel på den forskning som bedrivs vid organisationer som finns representerade bland syntesrapportens respondenter.

Kungliga Tekniska högskolan

Vid KTH bedrivs forskning som angränsar till området resilient och trygg elförsörjning inom områdena kraftsystem, datateknik, algoritmer, polymerer, elmarknadens aspekter, kraftelektronik, lågspänning och elmaskiner, reglerteknik och AI. Kompetenscentrumet SweGRIDS bedrevs tidigare vid KTH och i nuläget har tre centrubildningar som fokuserar på frågor som angränsar till området identifierats: Center for Resilient Critical Infrastructures (CERECS), Centrum för cyberförsvar och informationssäkerhet (CDIS) och Digital Futures. Samtliga av dessa beskrivs i avsnitt 3.4. Forskare vid KTH driver också projektet Nätverk för cybersäkerhet, som riktar in sig mot bolag inom energisektorn och elnätsbolag⁶.

Luleå tekniska universitet

Vid Luleå tekniska universitet berörs området framför allt ur ett elkrafttekniskt perspektiv, med frågor inom kort- och långtidsplanering av elnätet, extrema påfrestningar på elnätet och tillförlitlighet hos komponenter. Tre områden har lyfts fram som extra viktiga är *Acceptansgränsberäkningar* för att undersöka hur mycket ny produktion eller konsumtion som elnätet tolererar, med fokus på att ta fram standardmetoder för ändamålet, *Metoder för att öka acceptansgränsen* på sätt som är snabbare och billigare än utbyggnad av elnätet, genom bland annat nya marknadslösningar, dynamisk överblick och en bättre kommunikation samt *Elkvalitet* med fokus på negativ interaktion mellan enheter anslutna till nätet, som stör utrustningens funktion.

Lunds universitet

Vid Lunds universitets bedrivs det bland annat forskning inom samhällsviktig infrastruktur, däribland kraftsystem. Frågor som behandlas är risk, sårbarhet och resiliens hos komplexa system och samhällets beroende av tjänsterna som dessa levererar. Vid universitetet finns Centre for Critical Infrastructure Protection research (CenCIP), som beskrivs i avsnitt 3.4.

Linköpings universitet

Vid Linköpings universitet finns en forskargrupp som fokuserar på realtidssystem. Realtidssystem omfattar system i vilka tiden för en beräkning eller reaktion till en händelse är lika viktig som själva resultatet för beräkningen eller reaktionen. Där undersöks pålitlighet och resursallokering i distribuerade system med nätverkande delar, informationssäkerhet i det framtida elsystemet och hur AI och ML kan användas för anomalidetektering, automatiserad process som identifierar data som inte hör till i en uppsättning eller mönster, inom samhällsviktig infrastruktur⁷. Vid universitetet finns också centrumet Resilient Information and Control Systems (RICS), som också beskrivs i avsnitt 3.4.

Mälardalens universitet

Vid Mälardalens universitet bedrivs tvärvetenskaplig forskning inom ett område som kallas Framtidens Energi och som behandlar förnybar energi, digitalisering och resurseffektivisering⁸. Ämnen som angränsar till resilient och trygg elförsörjning är bland annat kraftvärmens roll i

⁶ Energiforsk, [Nätverk för cybersäkerhet](#).

⁷ IDA (2021), [Real-Time Systems Laboratory](#).

⁸ MDU(2022), [Framtidens energi](#).

energisystemet, energilagring, resurseffektivitet och flexibilitet⁹. Inom digitaliseringsområdet utvecklas nya matematiska metoder för att utveckla modellbaserad diagnostik, beslutsstöd, och optimering och styrning¹⁰. Det forskas även på frågor rörande cybersäkerhet. I nuläget utökar universitetet sin kompetens inom elnät och elektronik och under våren startas kompetenscentrumet Resilient Energy Systems Competence Centre (RESILIENTa Energisystem Kompetenscentrum) upp, se avsnitt 3.4.

Research Institutes of Sweden (RISE)

Vid RISE bedrivs det forskning inom bland annat cybersäkerhet, energilager, ödrift, vätgasproduktion och -användning, energigemenskaper, samt olika frågor rörande systemstabilitet och tillförlitlighet. RISE har också aktiviteter för att samla och utveckla kompetens för att möta behovet av forskning och innovation inom två så kallade strategiska förstärkningsområden: *Totalförsvar och krisberedskap* respektive *Robust och flexibelt energisystem*. Dessutom pågår utveckling av cybersäkerhetsområdet, bland annat vid testanläggningen Cyber Range, se avsnitt 3.4. RISE driver även Cybernoden, en nationell innovationsnod för cybersäkerhet vars syfte är att accelerera forskning och innovation inom cybersäkerhet i näringsliv och offentlig sektor¹¹. RISE är även delaktiga i RESILIENTa Energisystem Kompetenscentrum, se avsnitt 3.4.

3.2.2 Näringslivets aktörer

Forskning och utveckling bedrivs även inom näringslivet hos aktörer såsom energi- och elnätbolag och tillverkare och leverantörer av komponenter och tekniska system. Aktörer som blir allt viktigare på området till följd av digitaliseringen är IT- och telekombolag. Fokusområden som har nämnts under intervjuerna är utveckling av tillförlitliga och säkra nät, utveckling av skydds- och varningssystem, självläkande nät, mikronät och ödrift, dödnätsstart, digitalisering av transformatorstationer, utveckling av nya analysverktyg för att hantera insamlad data, digitala styrsystem samt utveckling och design av säkra informations- och kommunikationssystem. Intervju- och enkätstudierna har visat att det inte finns någon nämnvärd skillnad mellan de tematiska områden som akademin och näringslivet arbetar med, men att projekten inom näringslivet har ett mer praktiskt och tillämpat fokus på verkliga system.

Utöver egna projekt är aktörer från näringslivet ofta indirekt delaktiga i forskning genom att medverka i styrgrupper för forskningsprogram, samt genom att bistå med kompetens och finansiering till olika forskningsinstitutioner och projekt som ligger inom ramarna för verksamheternas egna intressen. Det finns även samarbeten mellan akademi och näringsliv, men dessa projekt är ofta av en mer generell natur jämfört med de projekt som bedrivs internt hos näringslivsaktörer, på grund av att området är känsligt och omfattas av sekretess.

Aktörer som nämnts under intervjuerna, men som bara är exempel på aktörer som bedriver forskning och utveckling på området, är Svenska kraftnät, Vattenfall, Ferroamp, ABB, Hitachi Energy, Schneider Electric, Siemens Energy, General Electric, Foreseeti, Ericsson och

⁹ MDU (2022), [Förnybar energi](#).

¹⁰ MDU (2022), [Digitalisering](#).

¹¹ Cybernode (2022), [Om noden](#).

Microsoft. Fem regionala energibolag finansierar tillsammans Utvecklingsklustret Energi AB, som bland annat bedrivit projekt kring kritisk informationshantering inom energisektorn. Energiföretagen driver nätverket Energibranschens säkerhetsgrupp, ESG, vars fokus är att samla branschen och bistå med kunskap kring säkerhetsskydd, informations- och cybersäkerhet samt beredskapsfrågor inom total- och civilförsvaret¹².

3.2.3 Offentlig sektor

Aktörer och verksamhet inom offentlig sektor spelar en viktig roll i säkerställandet av en resilient och trygg elförsörjning. Detta syntesarbete har dock endast gjort nedslag i hur forskning och utveckling bedrivs inom sektorn, i form av en genomgång av FOIs verksamhet samt perspektiv från ett antal länsstyrelser.

Totalförsvarets forskningsinstitut (FOI)

FOI är en statlig myndighet som bedriver forskning och expertstöd inom försvar- och säkerhetsfrågor på samtliga samhällsnivåer. Vid FOI finns det forskare med flera olika ämnesbakgrunder för att skapa en förståelse för hur samhälls- och teknikutvecklingen samverkar vilket ger möjligheten att tidigt identifiera hot och risker.¹³ Ett av FOI:s forskningsområden inom krisberedskap och civilt försvar är energiområdet. FOI analyserar både dagens energisystem men också framtidens energisystem. Exempel på områden som analyseras är svensk och europeisk försörjningstrygghet, krisberedskap samt kopplingen mellan klimatpolitik och energisäkerhet. FOI arbetar med metod- och begreppsutveckling, säkerhetspolitiska analyser samt översikter och synteser av befintlig kunskap om olika delar av energisystemet och energipolitiken. Dessutom används olika scenarier för att analysera exempelvis energikutvecklingen och hotbilder mot energiförsörjningen.¹⁴ FOI är bland annat delaktiga i RICS, CERECs och CRATE, se avsnitt 3.4.

Länsstyrelser

De länsstyrelser som svarat på enkäten har varit tydliga med att resilient och trygg elförsörjning är ett området som ses som allt viktigare. Fokus ligger naturligt på lokala och regionala aspekter av omställningen, med frågeställningar kring lokal produktion och flexibilitet, lokal förankring och acceptans, elförsörjning till samhällsviktiga verksamheter och samhällsekonomiska effekter av omställningen. Utvecklingsinsatser bedrivs i projektform för att uppfylla regionala och nationella miljömål. Genom att bidra till dessa mål ökar länets – och på så sätt rikets – resiliens, och en tryggare elförsörjning uppnås.

Exempel på utvecklingsprojekt som nämnts är *Fånga vinden*, med fokus på att identifiera hinder och möjliga lösningar för ökad vindkraftsproduktion, och *Planera i medvind – Vindbruksplanering för lokal förankring*, som syftar till att öka kommuners kapacitet att arbeta proaktivt med vindbruksplanering för att hantera intresse- och målkonflikter i ett tidigt skede. Ett annat pågående projekt är *Styrel*, som utförs i samarbete med Energimyndigheten, och som ska

¹² Energiföretagen (2022), [Säkerhet/cybersäkerhet](#).

¹³ FOI (2021), [Om FOI](#)

¹⁴ FOI (2021), [Energi](#)

resultera i en kartläggning av samhällsviktiga verksamheter och vilka som ska prioriteras vid effektbrist på kommunnivå. Insatser inom ramen för de regionala elektrifieringslöftena har också tagits upp.

Även om det inte är ett forsknings- eller innovationsprojekt hänvisar en länsstyrelse till regeringsuppdraget *Förutsättningar för en trygg elförsörjning* som viktigt på området. 2019 fick länsstyrelserna i Skåne, Västra Götaland, Stockholm och Uppsala i uppdrag av regeringen att analysera dagens och framtidens situation och förutsättningar för elförsörjningen regionalt. I den sammanfattande rapporten identifierades följande områden som viktiga i dagsläget och framöver¹⁵:

- Vikten av att transmissionsnätstärkningar blir klara i tid
- Produktions- och användarflexibilitet
- Lokal elproduktion vintertid
- Regional samordning
- Långsiktiga prognoser som tar hänsyn till effektfrågan på regional nivå.

Länsstyrelserna i rapporten skriver också att arbetet har undersökt förutsättningarna vid normal drift och att det inte betyder att frågor kring säkerhet, robusthet och resiliens är lösta.

3.3 Vilka finansierar forskningen?

Baserat på svaren i intervjustudien finns det många olika aktörer som finansierar forskningen i dagsläget. Bland respondenterna är det vanligast att den forskning de bedriver finansieras av svenska aktörer, men det förekommer också EU-finansiering och nordiska samarbeten. Respondenterna till intervjustudien har svarat att följande aktörer har finansierat forskning på området:

- | | |
|---------------------|---------------------------------------|
| • Energimyndigheten | • Wallenbergsstiftelsen |
| • Energiforsk | • RISE |
| • Svenska kraftnät | • Nordic Energy Research |
| • MSB | • Stiftelsen för strategisk forskning |
| • Vinnova | • EU-finansiering |
| • Formas | • Näringslivsaktörer. |
| • Vetenskapsrådet | |

Energimyndigheten har av många av respondenterna nämnts som den vanligaste finansiären av forskning inom området. Även Energiforsk har nämnts som en av de större finansiärerna. Nedan beskrivs några av finansiärerna närmare. Exempel på EU-finansierade program som tagits upp av respondenterna är: Horizon 2020 & Horizon Europe, EU Security Fund och European Reference Network for Critical Infrastructure Protection (ERN-CIP).

¹⁵ Länsstyrelserna i Skåne län, Stockholms län, Uppsala län, Västra Götalands län (2020). *Förutsättningar för en trygg elförsörjning*.

3.3.1 Energimyndigheten

Energimyndigheten har i uppdrag att verka för försörjningstrygghet och ett hållbart energisystem, och ska arbeta med att utveckla och samordna samhällets krisberedskap inom energiberedskapsområdet, samt stödja andra myndigheter med expertkunskap¹⁶. År 2020 utsågs Energimyndigheten till behörig myndighet enligt EU:s riskbedömningsförordning för elsektorn, där syftet är att förbättra EU:s förmåga att hantera elkriser.

Under intervjuerna har flera relevanta satsningar från Energimyndigheten nämnts. Bland annat den stora satsningen på elva nya forskningscenter, där RESILIENTa Energisystem Kompetenscentrum lyfts fram som en viktig satsning. Forskningsprogrammen SamspEL och VindEL har också nämnts som viktiga.

Energimyndigheten är även med och samfinansierar två program inom Nordic Energy Research som relaterar till resilient och trygg elförsörjning. Nordic Energy Outlooks Nordic Energy System Research Program (NEOs) har målet att stärka kompetensen i Norden genom syntesrapporter, erfarenhetsutbyte och samarbeten. Programmet har två arbetspaket som relaterar till området: *Increased electrification - new electricity generators and consumers* och *Energy efficiency and conservation in a Nordic perspective*¹⁷. Nordgrid Program är det andra programmet, och där är målet att stärka samarbetet mellan de nordiska länderna kring utmaningar som variabel elproduktion och cybersäkerhetsarbete¹⁸.

3.3.2 Energiforsk

Energiforsk har flertalet forskningsprogram med fokus på energiforskning men de två program som har starkast koppling till området är *Risk och tillförlitlighetsanalys* samt *Elnätens digitalisering och IT-säkerhet*.

Forskningsprogrammet *Risk och tillförlitlighetsanalys* har funnits sedan 2011 och har genomförts i flera omgångar sedan dess. Programmet har finansierat både forskning inom akademien och stöd till näringslivet i syfte att effektivisera, stärka metoder och verktyg för att minska risker och öka tillförlitligheten kopplat till de svenska eldistributionsnäten. Under den nuvarande perioden, 2021–2025, fokuserar programmet på att stötta tvärvetenskapliga kunskapsutbyten och fortsatt utveckling av metoder och verktyg som kan tillämpas inom näringslivet.¹⁹

Programmet *Elnätens digitalisering och IT-säkerhet* är en vidareutveckling av programmet *Smarta Elnät* som bedrevs 2014–2018. Syftet med det nuvarande programmet är att analysera och utvärdera vilka möjligheter digitalisering och ny teknik medför för elnätet. Programmet har fyra mål: ökad kunskap kring hur klimatpåverkan kan minska med hjälp av att mäta, styra och planera elnätet; att identifiera tekniska möjligheter och testa dem i pilotprojekt; att sprida resultaten från projekten; samt att projekten ska vara en brygga mellan akademi och näringsliv.

¹⁶ Energimyndigheten (2022). [Trygg elförsörjning](#).

¹⁷ Nordic Energy Research (2021). [The structure of the Nordic Energy Outlooks](#).

¹⁸ Nordic Energy Research (2021). [Nordgrid Program](#).

¹⁹ Energiforsk. [Programbeskrivning – Risk och Tillförlitlighetsanalys \(år 2021–2025\)](#).

En viktig del i programmet är också att de projekt som får finansiering ska ta hänsyn till IT-säkerhet när det är relevant.²⁰

3.3.3 Myndigheten för samhällsskydd och beredskap (MSB)

MSB finansierar i nuläget forskning inom framför allt två områden som relaterar till resilient och trygg elförsörjning: *Civilt försvar, samhällsviktig verksamhet, och krisberedskap* samt *Informationssäkerhet*. Inom *Civilt försvar, samhällsviktig verksamhet och krisberedskap* finansierar MSB framför allt grundforskning som tittar på hur extremhändelser, såsom väderpåverkan, klimatförändringar och antagonistiska hot, påverkar samhällsviktig infrastruktur, samt hur systemet kan återställas till normal drift på bästa sätt efter en incident. Bland annat pågår projektet *Kritiska flöden, försörjningskedjor och samhällskriser*, där energiförsörjning är ett fokusområde²¹. Mellan 2015–2020 finansierade även MSB uppbyggnaden av forskningscentrumet CenCIP, som beskrivs i avsnitt 3.4. I dagsläget pågår en avtrappning i finansiering för att centrumet ska bli självgående.

Inom informationssäkerhet finansierar MSB mer tillämpar forskning med fokus på samhällsviktiga tjänster i samhället, där elsystemet är en viktig del. Bland annat finansierar MSB två större projekt som fokuserar på aspekter av cyberfysiska system, CERES och RICS, som beskrivs i avsnitt 3.4. MSB avser att under 2022 att satsa på forskning inom "Cybersäkerhetens ekonomi", där syftet är att estimerar kostnaden för adekvata åtgärder och brister för att skapa bättre beslutsstöd.

3.3.4 Svenska kraftnät

Svenska kraftnäts forsknings- och utvecklingsplan för tidsperioden 2021–2024 fokuserar på fyra strategiska områden: ny teknik, digitalisering, systemutmaningar och kompetensförsörjning²². Svenska kraftnät finansierar FoU genom Energiforsk, konsultfirmor, stöd till akademiska forskningsprojekt samt doktorandprojekt och examensarbeten. Svenska kraftnät deltar också i internationella och europeiska forskningssamarbeten.

3.4 Större projekt och satsningar

Nedan presenteras större satsningar som har identifierats under syntesarbetet. Satsningarna består av både större pilotprojekt och forskningscentrum där kompetens och långsiktiga forskningsmiljöer kan byggas upp. Majoriteten av de identifierade centrumen har en teknisk inriktning, men det finns även multidisciplinära satsningar med fokus på bland annat ökad förståelse för samhällets beroende av samhällsviktig infrastruktur. Av de satsningar som beskrivs nedan är alla pågående, med undantag för SweGRIDS som avslutades vid årsskiftet och RESILIENTa som startas upp under våren 2022.

²⁰ Energiforsk, [Program för Digitalisering och IT-säkerhet 2018–2022](#).

²¹ MSB (2021), [Forskning inom civilt försvar, samhällsviktig verksamhet, krisberedskap](#).

²² Svenska kraftnät (2020), [Forsknings- och utvecklingsplan 2021–2024](#).

3.4.1 Swedish Centre for Smart Grids and Energy Storage (SweGRIDS)

SweGRIDS har under perioden 2011–2021 varit ett svenskt centrum för forskning inom framtidens elnät och energilagring. Syftet med centrumet var att bedriva forskning inom flexibla kraftsystem, digitalisering av kraftsystemet, styrbara kraftkomponenter och ny materialteknik för elnät och energilagring. Forskningen bedrevs antingen via postdoktorala projekt eller via doktorandprojekt vid KTH eller Uppsala universitet. Centret var ett samarbete mellan akademi, industri och myndigheter, där respektive aktör stod för en tredjedel av finansieringen²³. Inom SweGRIDS fanns det exempelvis två projekt inom IT-säkerhet, som tittade på penetrationer och säkerhetstestning, det vill säga hur svårt det är att ta sig in i och manipulera eller förstöra systemkomponenter.

3.4.2 Resilient Information and Control Systems (RICS)

Målet med RICS under de fem första åren var att bygga upp långsiktig forskning och ökad kompetens inom IT-säkerhet för samhällsviktig infrastruktur. Centrumet är ett samarbete mellan Linköpings universitet, KTH, Chalmers och FOI. RICS fick finansiering av MSB mellan 2015–2020, och har fått förlängning för en andra fas mellan 2021–2023 som fortfarande är under planeringsstadiet²⁴. Forskningen har fokuserat på risk- och sårbarhetsanalyser och detektion av oönskade händelser²⁵.

3.4.3 Centre for Critical Infrastructure Protection research (CenCIP)

Det övergripande målet med forskningscentrumet CenCIP är att bidra till utvecklingen av ett mer resilient samhälle som kan förutse och anpassa sig till påfrestningar, och snabbt återuppta viktiga samhällsfunktioner²⁶. Forskningscentrumet är etablerat vid Lunds universitet och finansierades av MSB mellan 2015–2020. I nuläget pågår en avtrappning där finansieringen gradvis minskar tills centrumet är självgående. CenCIP fokuserar brett på att öka kunskap och förståelse för samhällsviktig infrastruktur. Kunskapen som tas fram ska ligga till grund för att ta fram koncept, metoder, system och verktyg som ska underlätta arbetet med att skydda samhällsviktig verksamhet.

3.4.4 Center for Resilient Critical Infrastructures (CERECS)

Forskargrupper på KTH arbetar inom CERECS tillsammans med FOI för att identifiera framtida hot mot, och verktyg för, att bevara säkerheten i industriella informations- och styrsystem. Centrumet fokuserar på fyra områden: säkerhet i inbyggda system, trådlös kommunikation, kommunikation och beräkningsstrukturer, samt resilient reglering av cyberfysiska system²⁷. Centrumet finansieras av MSB²⁸.

²³ Energimyndigheten (2018), [SweGRIDS](#).

²⁴ MSB (2021), [Resilient Information and Control Systems \(RICS\)](#).

²⁵ MSB (2021), [Forskning inom informationssäkerhet](#).

²⁶ Lunds universitet (2021), [CenCIP:s Syfte och mål](#). Error! Hyperlink reference not valid.

²⁷ MSB (2018), [Infrastrukturer skyddas från cyberhot](#).

²⁸ KTH (2021), [CERES- Center for Resilient Critical Infrastructures](#).

3.4.5 Centrum för cyberförsvar och informationssäkerhet (CDIS)

CDIS är ett samarbete mellan KTH, Försvarsmakten och MSB som startade 2020. Centrumet fokuserar på forskning inom cyberförsvar och informationssäkerhet för att möta de utmaningar som har uppstått till följd av den snabba digitaliseringen. I nuläget har CDIS nio pågående forskningsprojekt med fokus på exempelvis självlärande system för cyberförsvar, lägesförståelse i cybermiljön, och simuleringsbaserat driftstödssystem för cybersäkerhet²⁹.

3.4.6 Cyber range och Cyber Range and Training Environment (CRATE)

Cyber range och CRATE är två satsningar som har nämnts av flera respondenter som viktiga för att öka kompetensen och förståelsen för cyberattacker riktade mot samhällsviktig infrastruktur och organisationer. Båda anläggningarna är virtuella testanläggningar, vilket innebär att det går att bygga upp virtuella miljöer eller tvillingar som återspeglar verkliga system. Fördelen med detta är att det då går att bedriva forskning samt tester av hur system och komponenter påverkas av olika cyberattacker innan de implementeras i det verkliga systemet. Vid de båda anläggningarna erbjuds det också utbildning av personal som arbetar med IT-säkerhet, för att höja deras kunskap kring hur de ska agera för att minimera intrång och skada vid attack^{30,31}. Cyber range får finansiering från Vinnova, RISE och ICT Sweden³². CRATE finansieras av MSB tillsammans med Försvarsmakten och i nuläget pågår en satsning för att bygga ut verksamheten.

3.4.7 Digital Futures

Digital Futures är ett multidisciplinärt forskningscentrum med en vision att lösa samhällsutmaningar i bred bemärkelse med hjälp av digitalisering. Forskningscentrumet är ett samarbete mellan KTH, Stockholms universitet och RISE. Det finansieras av den svenska regeringen och etablerades 2020³³. Digital Futures finansierar forskning genom en lång rad utlysningar, där exempel på tidigare utlysningar som är relevanta i sammanhanget har inriktat sig mot cybersäkerhet, samhällsviktig infrastruktur och energisäkerhet. Projekt som fått finansiering i dessa utlysningar har bland annat handlat om användningen av machine learning-metoder inom kraftelektronik och elkraftsystem.

3.4.8 Systemförändring: Energigemenskaper

RISE driver i samarbete med KTH två pilotprojekt där energigemenskaper undersöks: Tamarinden Örebro och Hammarby Sjöstad. Inom projekten ska riktlinjer för upphandlingar, lagar och regelverk utformas så att tjänster, innovationer och affärsplaner kan skapas och realiseras. Ytterligare aktörer som är inblandade är Örebro Kommun, ÖrebroBostäder, ElectriCITY, E.ON, KTC, Enstar, Siemens och Ellevio³⁴.

²⁹ KTH (2022), [Centrum för cyberförsvar och informationssäkerhet](#).

³⁰ RISE (2021), [Cyber range stärker svensk kompetens inom cybersäkerhet](#).

³¹ MSB (2019), [Nationell cyber range och testbädd](#).

³² RISE (2022), [Cyber range – testbädd för cybersäkerhet](#).

³³ Digital futures (2022), [About](#).

³⁴ RISE (2022), [Systemförändring med lokalt delad energi](#).

3.4.9 Resilient Energy Systems Competence Centre (RESILIENTa)

Målet med RESILIENTa är att ta fram kunskap, verktyg och praxis ur ett brett systemperspektiv för att skapa en säker och optimal energiförsörjning i ett hållbart och fossilfritt system. Kompetenscentrumet kommer fokusera på att utveckla kunskap kring hur sektorskoppling mellan transportinfrastruktur, industri och bebyggd miljö, inklusive affärsmodeller och organisation, kan skapa resiliens i energisystemet³⁵. Kompetenscentrumet kommer bland annat titta på hur produktionen av energi kan ske på bästa sätt framöver ur ett regionalt perspektiv, där hänsyn tas till bland annat kapacitetsbegränsningar i elnätet. Kompetenscentrumet, koordineras av Mälardalens universitet och består av fem forskningsorganisationer samt cirka 30 företag och offentliga aktörer. Finansieringen är tredelad mellan akademien, näringsliv, offentlig sektor och Energimyndigheten och gäller mellan åren 2022–2026.

3.5 Internationell utblick

På frågor kopplade till hur respondenterna i intervjustudien upplever utvecklingen i Norden har svaren genomgående varit att det inte är någon större skillnad mellan ländernas kunskaper inom resilient och trygg elförsörjning. Den skillnad som har nämnts är att respektive land har olika goda kunskaper inom olika produktionsslag. Norge är duktiga på vattenkraft, Finland är duktiga på kärnkraft och Danmark har kunskap kring integrering av en hög andel vindkraft.

Tyskland och Holland lyfts fram som duktiga på cybersäkerhetsfrågor. Länder som England, Singapore, Kina och Kanada lyfts fram som duktiga på sannolikhetsmetoder. Relaterat till forskning som fokuserar på att öka resiliens inom infrastruktur har Infrastructure Transitioning Research Consortium (ITRC) i Storbritannien och Critical Infrastructure Resilience Institute (CIRI) i USA nämnts som goda exempel. Forskningen vid ITRC bidrar med koncept, modeller och underlag för planering av resilient infrastruktur på nationell, regional och lokal nivå³⁶. Vid CIRI bedrivs forskning och utbildning för att förbättra resiliens i USA:s kritiska infrastruktur och inom de verksamheter och organisationer som äger och driver systemen³⁷.

Internationella samarbeten förekommer inom forskningsområdet. Inom akademien har samarbeten inom elkraft med Norges tekniska-naturvetenskapliga universitet (NTNU) i Trondheim, samt Danmarks Tekniska universitet (DTU) i Lyngby, lyfts fram. Bland akademiska samarbetsprojekt har också samarbetsprojekt relaterade till utlysningar från EU framkommit.

Det finns även flera internationella samarbeten inom industrin; dels inom globala företag och dels mellan de nordiska TSO:erna, i sammanslutningar mellan industri och akademi. Svenska kraftnät deltar bland annat i projektet *Nordic Early Warning Early Prevention System (NEWEPS)*, samt i det nyligen avslutade *MultiDC*. NEWEPS är ett internationellt samarbete mellan Svenska kraftnät, det norska forskningsinstitutet SINTEF, RISE, KTH, NTNU och Statnett. Syftet är att utveckla ett gemensamt informationssystem för att övervaka stabiliteten och styrningen av det

³⁵ Energimyndigheten (2021), [Kompetenscentrum 2022–2026](#).

³⁶ ITRC (2020), [Who we are](#).

³⁷ CIRI (2022), [About Us](#).

nordiska kraftsystemet³⁸. Målet med MultiDC var att utveckla metoder för optimal koordinering av flera HVDC kablar och HVDC nät med en hög andel förnybar elproduktion³⁹. Samarbetspartners var Svenska kraftnät, KTH, Hitachi Energy, DTU, EnergiNET, Innovation Fund Denmark och Liege universitet.

Resilient Digital Sustainable Energy Transition (REDISET) är ett internationellt projekt som består av ett samarbete mellan KTH, FFI – Norwegian Defence Research Establishment, University of Vaasa, The Norwegian SmartGrid Centre, Statnett, Svenska kraftnät, Fingrid och företaget Gambit. Målet är att identifiera sårbarheter, utveckla systemdesigner och olika resilienskriterier för att säkra systemdriften ur ett socio-tekniskt perspektiv.^{40,41}

Det finns flera internationella organisationer, där kunskapsutbyten sker mellan akademi och näringsliv, som har lyfts fram av respondenterna. Bland dessa ingår IEEE Power and Energy Society, IEEE Computer Society och International Council on Large Electric Systems (CIGRE)⁴².

Inom EU finns även samarbetsorgan som är relevanta i sammanhanget. ENTSO-E bidrar med utveckling och implementering av standarder, nätkoder, plattformar och verktyg för att säkerställa säkra system och marknader. Organisationen är dessutom ansvarig för att koordinera forskning, utveckling och innovation bland TSO:er.⁴³ Den nystartade organisationen EU-DSO ska arbeta med att främja samarbete och kunskapsutbyte mellan alla DSO:er i Europa, samt bidra till samarbetet mellan DSO:er och TSO:er⁴⁴. EU-DSO samarbetar exempelvis med ENTSO-E, på uppdrag av EU-kommissionen och ACER, med utvecklingen av cyberlagstiftningen.

ENISA arbetar för att uppnå en hög standard på cybersäkerheten i hela Europa. ENISA jobbar bland annat med att identifiera framtida hot och öka beredskapen i Europa genom att organisera träning, simulering av kriser, konferenser och informationskampanjer⁴⁵.

I nuläget pågår etablering och utformning av European Cybersecurity Competence Network and Centre (ECCC). Målet med ECCC är att stärka EU:s förmåga och konkurrenskraft inom cybersäkerhet, bland annat genom att utveckla unionens kapacitet inom forskning och innovation, samt genom att etablera samarbeten och möjlighet till erfarenhetsutbyten.⁴⁶ ECCC kommer utforma och hantera utlysningar för cybersäkerhet inom forskningsprogrammen Horizon Europe och DIGITAL EU samt etablera nationella samordningscentrum. MSB är ansvariga för Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet, NCC-SE. NCC-SE ska hjälpa till att främja EU-finansiering i Sverige.⁴⁷

³⁸ Svenska kraftnät (2022), [Nordiskt varnings- och skyddssystem](#).

³⁹ MultiDC (2022), [MultiDC](#).

⁴⁰ Nordic Energy Research (2021), [The project Resilient Digital Sustainable Energy Transition](#).

⁴¹ Energimyndigheten (2022), [Projektinformation REDISET](#).

⁴² Cigre (2022), [Introducing CIGRE](#).

⁴³ ENTSO-E (2022), [ENTSO-E Mission Statement](#).

⁴⁴ EU-DSO (2022), [Missions](#).

⁴⁵ ENISA (2022), [About ENISA](#).

⁴⁶ ECCC (2022), [European Cybersecurity Competence Centre and Network](#).

⁴⁷ MSB (2022), [About NCC-SE](#).

4 Tillämpning av forskningen

I detta kapitel besvaras frågeställningen om hur den forskning kring resilient och trygg elförsörjning som tas fram tillämpas.

Hur forskningen tas vidare inom området varierar beroende på om det är akademisk grundforskning eller tillämpad forskning där näringslivet medverkar. Grundforskning har beskrivits som viktig för att utveckla nya komponenter, system och operativa driftsfall samt utveckling av möjliggörande tekniker likt AI. För grundforskning är det ofta en lång väg till implementering, och det krävs ofta att en aktör tar till sig kunskapen och bearbetar den för att resultaten ska bli tillämpbara. Forskare som bedriver utbildning har nämnt att den kunskap som tas fram i forskningsprojekt implementeras som underlag i utbildningar. Utöver detta sprids kunskapen bland annat via workshops och seminarier. En perspektiv som har nämnts av flera respondenter är även att all forskning inte måste tillämpas, beroende på frågeställningens natur.

Tillämpad forskning har beskrivits som viktig för att integrera olika tillgängliga verktyg för att skapa en effektiv lösning som kan implementeras i energisystemet. De forskningsprojekt som bedrivs i samarbete med näringslivet upplevs av respondenterna implementeras på ett bra sätt. Särskilt då näringslivet är med som finansiär och efterfrågar kunskap inom specifika områden. Referensgrupper är ett bra sätt att föra kunskap vidare från forskningsprojekt till de aktörer som medverkar, och examensarbeten nämns som ett bra sätt att kombinera kunskap från både akademi och näringsliv. Oavsett form är dialogen mellan akademi och näringsliv kritisk för att skapa goda förutsättningar för tillämpning. Här upplevs dialogen fungera olika bra beroende på vilka parter som är inblandade. Flera respondenter lyfter fram att samarbetet mellan akademien fungerar bra i Sverige jämfört med andra länder.

Pilotprojekt har nämnts som väldigt viktiga dels för att testa nya tekniker och lösningar i verkligheten men också för att visa aktörer att tekniken finns. Ett annat gott exempel på forskning som tillämpas väl är CRATE och Cyber range, vars testmiljöer används för både forskningsprojekt och utbildningar för näringslivet, vilket gör att resultaten från forskningen får tydliga mottagare. Konceptet är svårare att överföra till frågor som rör den fysiska infrastrukturen, eftersom produktion och elnät är i kontinuerlig skarp drift. Detta lyfts även fram som ett framtida forskningsbehov i kapitel 5.



5 Identifierade behovsområden för framtida forskning

För att åstadkomma en överblick över de identifierade forskningsbehoven för resilient och trygg elförsörjning har denna syntesrapport utgått från att hitta samband mellan respondenternas inspel. Utifrån dessa samband har de kunskapsmässiga behoven kunnat kategoriseras in under fem tematiska behovsområden (som till viss del överlappar varandra, på grund av områdets systemorienterade natur):

- Resilient och trygg elförsörjning i ett elektrifierat och digitaliserat samhälle
- Systemperspektiv och tillräcklighet
- Drift och underhåll av elnätet
- Informations-, kommunikations- och cybersäkerhet
- Utveckling av modellverktyg och testbäddar

Elsystemet är ett socio-tekniskt system och även om syntesrapporten har en teknisk inriktning har behov inom humanistisk och samhällsvetenskaplig forskning också identifierats och redovisas i ett eget avsnitt. Om än ej ett strikt forskningsbehov, så lyfts i tillägg kompetensförsörjning som ett viktigt tema framåt, där ett delbehov är kompetensförsörjningen hos mindre aktörer såsom lokala elnätsbolag.

Ett vanligt återkommande intervjusvar kring framtida forskningsbehov är att många av de frågor som vi arbetar med idag kräver ett fortsatt fokus även i framtiden. Eftersom omställningen av elsystemet medför att det uppstår nya frågor och utmaningar efterlystes i tillägg fler satsningar för att bygga upp en bred och långsiktig kompetens på området. Precis som beskrivet i avsnitt 3.1 är området resilient och trygg elförsörjning omfattande och det möjligt att vissa av de frågor som tagits upp av respondenterna även skulle kunna adresseras inom satsningar eller forskningsprogram med andra kontexter.



Flera av respondenterna upplever att utformningen på utlysningar under de senaste åren har breddats till att inkludera samhällsaspekter och användarperspektiv, då det tidigare var svårt att hitta utlysningar för multidisciplinära projekt. Breddningen upplevs som nyttig då elsystemet är ett socio-tekniskt system och det nya kompetenscentrumet RESILIENTa har lyfts som ett bra exempel på en sådan satsning. Flera respondenter belyser dock vikten av att det fortsatt måste finnas långsiktiga utlysningar som fokuserar på grundforskning inom enskilda discipliner som därefter kan tillämpas.

Under intervjustudien har det lyfts fram att dagens utlysningar inte är optimalt utformade för mindre aktörer, samtidigt som just mindre aktörer samtidigt som kompetensförsörjningen hos just dessa anses vara särskilt viktig. Mindre bolag har ofta lägre tillgång till ekonomiska resurser och arbetskraft för att driva forskningsprojekt och tiden mellan utlysning och då ett projekt kan börja upplevs vara för lång. Det efterfrågas också fler utlysningar som möjliggör ett samarbete med aktörer över nationsgränser, framförallt nordiska, för att kunna utvecklas och ta lärdom av våra grannländer.

I följande avsnitt görs nedslag i de behovsområden som identifierats. En generell kommentar angående de identifierade områdena är att majoriteten omfattar frågeställningar som rör både leveranssäkerhet vid normaldrift samt beredskap och hantering av kriser.

5.1 Resilient och trygg elförsörjning i ett elektrifierat och digitaliserat samhälle

Till att börja med efterfrågas det mer kunskap kring vad som borde ingå i begreppet resilient och trygg elförsörjning. I dagsläget kan vi prata om delfrågor, exempelvis tillförlitlighet eller risk- och sårbarhetsanalyser. För att kunna ta fram standardiserade metoder för att göra en bedömning och besvara frågan "*Hur resilient är elförsörjningen?*" krävs dock en gemensam förståelse för hur ett resilient system ska definieras.

Ett behov av att kartlägga vilka faktorer som är relevanta för att elsystemet ska upplevas som tryggt för olika aktörer har också lyfts fram för att kunna besvara frågan "*Hur trygg är elförsörjningen?*". Exempelvis handlar det om en stabil prisbild, kontinuitet i leveransen, förtroendekapital mot elleverantör, eller huruvida elförsörjningen kan säkras under en eventuell krigshändelse? Har elnätsbolag och kunder samma bild?

Frågeställningar som är viktiga inom området är: Borde bilden av vad av ett resilient elsystem är uppdateras när samhället går mot ett allt större elberoende? Vad är en acceptabel nivå av resiliens i infrastrukturen, och hur skapas en bra balansgång mellan alternativa åtgärder? Hur lång tid kan privatpersoner respektive samhällsviktiga aktörer klara sig under ett elavbrott? Vilka hotbilder finns framöver och hur kan de mötas upp? Är det acceptabelt att systemet anses vara resilient vid normal drift men inte under en förhöjd hotbild?

Något som inte faller strikt under kategorin forskning och innovation, men som har framförts av näringslivsaktörer, är att det föreligger ett stort behov av att få uppdaterade krav och riktlinjer för resilient och trygg el- och energiförsörjning i scenarier vid olika grader av konflikt. Krav på riktlinjer kan gälla exempelvis bränslelager och material, men även frågor som skalskydd, skyddsavstånd, och personskydd. De kan även gälla anställdas roller inom totalförsvaret, värn, samt samövningar med andra aktörer och myndigheter inom totalförsvaret, civilsamhälle och privata aktörer som bedriver samhällsviktig verksamhet samt underleverantörer.

5.2 Systemperspektiv och tillräcklighet

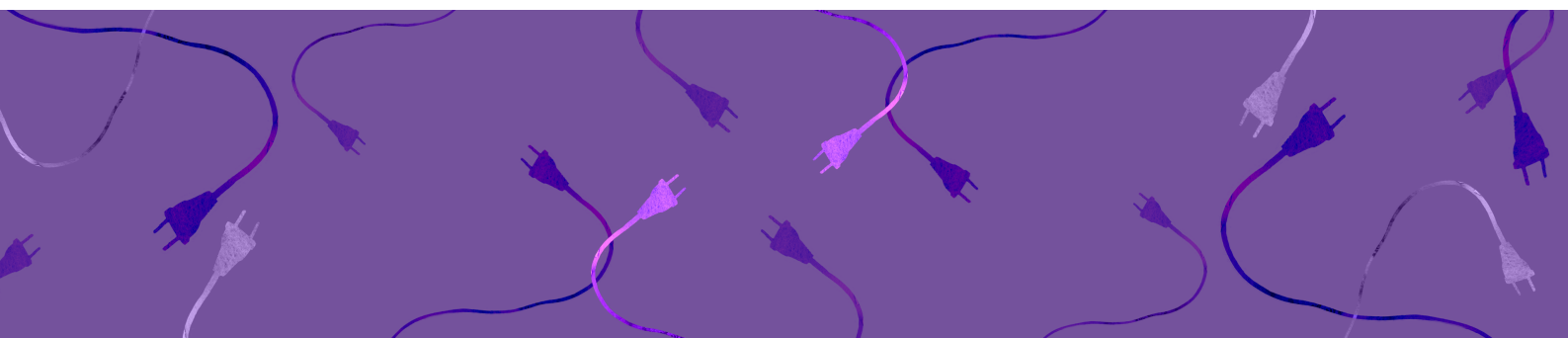
Respondenter har lyft fram ett behov av forskning med systemperspektiv, för att klargöra hur resilient och trygg elförsörjning kan uppnås parallellt med elektrifieringen och omställning av energisystemet, eller med omställningen som medel.

Frågor som har lyfts är: Hur kommer en ökad elektrifiering inom industri och transportsektor att påverka elsystemet? Vilka utmaningar uppstår med en kraftigt ökad andel förnybar energi i nätet? Vilka synergieffekter finns mellan de olika produktionskällorna, och hur ska styrningen av produktionen göras vid produktionsöverskott? Vilka nyttor finns det med ökad sektorskoppling, och hur kan vi utnyttja det på bästa sätt? Hur motverkar vi trenden att generatorer i kraftvärmeverk kopplas bort, och att vi därmed går miste om möjligheten att använda dem som reservkraft i lokalnät?

En ökad förståelse behövs också för hur vi ska hantera systemets tillräcklighet, särskilt vid effektunderskott under normalvintrar eller under kriser. Är det exempelvis kallt i Sverige borde det vara det i våra grannländer också – vad händer när de också har ett underskott i sin elproduktion? Hur stort är behovet av att investera i reservkraft eller andra alternativa åtgärder som kan aktiveras vid effektunderskott?

Energilagring i olika former har lyfts fram av många intervjuade aktörer som en viktig del i att skapa ett resilient system. Frågor som har nämnts är: Vilken lagringsteknik är lämplig för vilket syfte? Vilken mix av energilager behövs framöver? Det behövs också ökad kunskap kring hur lagringen utnyttjas på bästa sätt för att avlasta elsystemet och kapa effekttoppar.

På samma sätt lyfts flexibilitetslösningar som en viktig resurs för att skapa resiliens i systemet, men de väcker samtidigt frågan kring vad som är en bra balans mellan flexibilitetslösningar och utbyggnad av ledningar. Hur stor är egentligen potentialen i flexibla resurser? Det efterfrågas också mer kunskap kring vilken flexibilitet som finns på produktionssidan, och om det finns ett behov av att ta fram en objektiv bedömning av vilket produktionsslag som ska spillas vid effektöverskott som inte enbart är baserat på produktionskostnad.



En rad frågor tas upp relaterat till energigemenskaper och förmåga till ödrift. Framöver förutspås en ökad medvetenhet hos användare och en vilja att kunna vara självförsörjande vid behov, vilket kan bli en viktig del i att skapa ett tryggare elsystem. Här efterfrågas kunskap kring hur lokala mikronät och fastigheter som klarar av att leverera el vid avbrott kan byggas upp i större omfattning, och hur de kan bidra till återuppbyggnad av systemet. FOI publicerade nyligen en rapport där de lyfter fram förslag på forskningsfrågor kopplade till lokala elnät⁴⁸:

- Är det möjligt att göra svenska förläggningar autonoma och fria från extern energitillförsel (elnätet och bränsletillförsel) genom att använda ett lokalt nät (även kallad öförsörjning), bestående av t.ex. olika batterier, solceller, bränsleceller, vindkraftverk, generatorer och lokal produktion av biogas/biodiesel från närliggande industri, exempelvis skogs- och massaindustrin?
- Är det möjligt att driva sensorstationer helt autonomt? Hur kan ett system bestående av solceller, bränsleceller och batterier designas för ändamålet?
- Vilka komponenter konstruerade för växelström skulle även kunna drivas av likström?

Ett brett perspektiv som också lyfts är att elförsörjningen är beroende av transporter, personal, bränsle, osv, för att kunna uppehållas. Viss personal och produktion av bränsle och komponenter etc. är förlagd utomlands vilket försvårar totalförsvarsplaneringen och krigsplacering – hur säkerställer vi att dessa resurser kan tillhandahållas vid kris- eller krigssituationer? Hur klarar vi driften av vårt elsystem utan att vara beroende av ett annat land? Framöver efterfrågar länsstyrelserna ökad kunskap och metoder kring hur lokal och regional energiplanering kan genomföras på ett bra sätt.

5.3 Drift och underhåll av elnätet

Med större andel förnybar produktion, nya konsumenter och en ökad andel kraftelektronik i systemet uppstår behovet att undersöka hur systemets stabilitet, elkvalitet, och driftsäkerhet påverkas till följd av dessa förändringar och därmed hur resilient det är. Ett behov finns för att fortsätta utveckla acceptansgränsberäkning, och att implementera dessa beräkningar på verkliga system för att förbättra förståelsen för hur mycket kapacitet det finns i nätet. Framöver behövs också kunskap kring hur utmaningarna i elsystemet skiljer sig åt i olika delar av landet och vilka förmågor som behövs på lokal och region nivå. Exempelvis behovet av planerbar reglerbar effekt i södra Sverige. En potential ses i fortsatt utveckling av smarta elnät och nya metoder för en effektivare drift, men det belyses också som viktigt att lägga resurser på att kartlägga oförutsedda (negativa) konsekvenser och risker.

Frågeställningar som har identifierats på området är: Vilka skydds- och styrsystem behövs i elsystemet framöver? Vilken påverkan riskerar all den nya kraftelektronik som installeras i elnätet att orsaka? Hur påverkas exempelvis övertoner, rotationsenergi och kortslutningseffekt? Hur ska investeringar i smart teknik vägas mot investering i ny infrastruktur? Hur ska risker som uppstår vid över- och underinvesteringar vägas mot varandra? Hur kan användningen av energi

⁴⁸ FOI (2021), [Energisystem för robust energiförsörjning](#).

styras på bästa sätt för att minska belastningen på elnätet när det är som mest ansträngt? Hur anpassar vi driften av infrastrukturen utefter klimatförändringar?

Nya möjligheter öppnas även upp till följd av digitaliseringen. AI och big data kan ge förutsättningar till robust och autonom drift av produktion och nät, automatisk identifiering av störningar och bättre beslutsfattande men det behövs fortsatt utveckling av analys- och styrsystemen. Ett område att undersöka är hur digitalisering kan bidra till att öka elnätets resiliens med hjälp av övervakning och riskbedömningar i realtid, samt proaktiv riskreducering. Det finns också en potential i att fortsätta vidareutvecklingen av digitala tvillingar för att kunna testa och utvärdera olika lösningar virtuellt.

5.4 Informations-, kommunikations- och cybersäkerhet

Flera respondenter har nämnt att det finns brister i kunskapen kring säkerhetsfrågor inom informations- och kommunikationsinfrastrukturen. Detta till följd av att digitaliseringen har gått väldigt fort och att säkerheten inte alltid har prioriterats vid utveckling av lösningar, trots att systemen är kritiska för att infrastrukturen ska fungera. Ytterligare en utmaning är hantera information och kommunikation när små och distribuerade resurser blir en viktig del av elsystemet. En särskild utmaning i Sverige är dessutom att vi har ovanligt många individuella elnätbolag varav många är små, vilket gör oss särskilt sårbara för koordinerade attacker. Forskning och utveckling kring hur energisystemet kan skyddas mot skador och antagonistiska hot mot de komplexa system som kopplar samman elmarknaden, infrastrukturen, samt konsumenter och producenter av olika storlek och karaktär efterfrågas därför. Det pågår idag forskning kring hur säkra system kan byggas och bevisas, men utveckling av nya cybersäkerhetstekniker behöver hela tiden fortgå då även antagonister som försöker angripa systemen utvecklas kontinuerligt.

Frågeställningar och områden som identifierats som viktiga är: Hur designar vi säkra informations- och kommunikationssystem? Hur känsliga är nya komponenter och system för cyberattacker? Vilka konsekvenser riskerar att uppstå vid samordnade överbelastningsattacker mot informations- och kommunikationsinfrastrukturen i elsystemet, och hur kan konsekvenserna minimeras? Vilka konsekvenser riskerar att uppstå om flera elnätbolag utsätts för en attack samtidigt? Hur ska avvägningen göras mellan detektering av intrång i systemen kontra skydd mot intrång? Behövs det analog teknik som backup till digitala system? Det behövs även fortsatt utveckling av AI för att identifiera icke-normala beteenden i systemen.

I flera intervjuer har det lyfts fram att förståelsen för cybersäkerhet behöver öka på ledningsnivå inom organisationer. Flera respondenter upplever att det i dagsläget inte finns tillräckligt med kunskap och förståelse kring vilka konsekvenser och kostnader en cyberattack mot organisationen skulle medföra, och hur organisationen ska agera om den blir utsatt för en attack. Därför efterlyses forskning kring hur en medvetenhet kan skapas hos ledningsgrupper för att de ska tillföra mer resurser och ha en tydlig plan på organisatorisk nivå, samt att cybersäkerhet tas med som en viktig aspekt vid business impact-analyser. En fras som har nämnts är *"Cybersäkerhet är inte ledningsproblem tills det är det"*. Ett relaterat organisatoriskt

problem är att det i dagsläget finns kompetens på IT-avdelningar kring skydd av data, medan det är andra delar av organisationen som har kunskap om vad som är kritisk information.

Näringslivet efterfrågar också ett informationsnätverk kopplat till IT-säkerhet mellan elbolag i Sverige och Europa, för att snabbare få och sprida information om incidenter, vilket skulle leda till ökad säkerhet. Detta är dock på väg att implementeras via NIS2.0.

5.5 Utveckling av modellverktyg och testbäddar

En problematik som flera respondenter har lyft fram är att driften av elsystemet hela tiden är skarp, vilket leder till begränsade möjligheter att testa nya komponenter och system, samt simulerade fel och attacker. I dagsläget finns testanläggningarna Cyber range och CRATE där det går att testa komponenter och digitala system, men det efterfrågas större testanläggningar även för elnät.

Respondenter har också efterfrågat datamodeller som bygger på det verkliga systemet för att exempelvis analysera inverkan av förändringar i produktionen och användarnas behov, förändringar av laster, såsom värmepumpar och solceller, samt för att identifiera utmaningar och konsekvenser i systemet på lång sikt. Vid framtagandet av modeller som bygger på verkligheten finns det en målkonflikt då elnäten är belagda med sekretess, vilket leder till att det är svårt att etablera samarbeten där verkliga data kan delas mellan elnätsbolag och akademi och offentlig sektor. En utmaning framöver är därför hur denna problematik ska kunna lösas på ett säkert sätt.

Till följd av klimatförändringar behövs också modeller som kan analysera hur klimatet kommer förändras framöver, och vilken påverkan olika scenarion får på resiliensen i systemet och på elproduktion från vind-, sol- och vattenkraft.

5.6 Humanistisk och samhällsvetenskaplig forskning

Även om syntesrapporten har ett huvudfokus på tekniska perspektiv, och majoriteten av respondenterna verkar inom de tekniska och naturvetenskapliga disciplinerna, har många lyft forskningsbehov inom humaniora och samhällsvetenskap. Det finns ett behov av att komplettera teknisk forskning med dessa perspektiv för att få en ökad förståelse för hur systemets resiliens och trygghet kan påverkas av icke-tekniska faktorer, samt de ekonomiska och beteendemässiga dimensionerna av vad som anses vara ett resilient och tryggt system. Teman som har nämnts är omställningens påverkan på priset för el, ekonomiska konsekvenser av ett icke-fungerande system, juridiska frågor kopplade till digitalisering och användandet av data, samt rättvisaspekter av omställningen.

Exempel på frågeställningar och områden som har identifierats under syntesarbetet är: Hur påverkar priset på el den av kunderna upplevda tillräckligheten ur ett ekonomiskt perspektiv? Hur påverkas prisbilden i olika delar av landet av omställningen och elnätets sammankoppling med Europa? Vilka samhällskostnader uppstår om elnätet inte är tryggt och resilient? Å andra sidan, hur mycket får ett tryggt och resilient system kosta? Just den ekonomiska avvägningen av robusta och säkra system är ett tema som tagits upp i flera intervjuer. Exempelvis: hur skapar vi digitaliserade transformatorstationer som är säkra och tillförlitliga, samtidigt som de är ekonomiskt motiverbara?

Vidare har frågor tagits upp såsom: vilka nya risker kan uppstå i ett samhälle som är allt mer beroende av elsystemet, och hur ska riskerna värderas mot varandra? Hur ställs olika intressen såsom klimat, miljö, ekonomi och försvar mot varandra? Hur kommer människor påverkas av omställningen - finns det risk att det uppstår klasskillnader till följd av utvecklingen? Hur garanterar vi individers integritet vid datainsamling? En fråga som har lyfts fram som viktig är risken att intrång och cyberattacker sker på grund av den mänskliga faktorn, samt att medvetenheten bland företag och organisationer måste öka för att uppnå en god säkerhet.

Det efterfrågas också kunskap kring snabba beteendeförändringar och omställningar i samhället, exempelvis informationskampanjer om förbrukningsdämpande åtgärder som snabbt ska kunna sättas in vid behov. Hur mycket energi kan sparas med detta? Hur skiljer det sig över året? Är folk villiga att bidra till detta? Under hur lång tid kan privatpersoner respektive aktörer inom näringsliv och offentlig sektor klara sig utan el? Finns det alternativa planer för att kunna fortsatt bedriva verksamhet med begränsad tillgång till el?

Det finns även ett behov av mer kunskap kring beteenden hos individer kopplat till ödrift. Vilken medvetenhet finns hos dem som bor i områden med ödriftsförmåga, och hur är de beredda att agera? Det beteendevetenskapliga perspektivet påverkar hur den tekniska styrningen kan utformas. Dessutom krävs utveckling både vad gäller teknik, juridik och organisation för att ödrift ska kunna användas lokalt i en krissituation. Det förnybara elsystemets olika delar behöver förberedas och planeras utifrån totalförsvarsaspekter.

5.7 Tillgång till kompetens

Tillgång till kompetens är i sig en viktig aspekt i ett resilient och tryggt elsystem. Inom akademien upplevs det som att det finns ett högt söktryck till doktorandtjänster, med undantag för elkraftsområdet där fler doktorander efterlyses. Däremot upplever akademien att det är svårare att säkra kompetensen på högre nivå; dels på grund av konkurrens med näringslivet om individer, och dels på grund av att en del av de internationella doktoranderna inte stannar i Sverige. En omvänd problematik inom cybersäkerhetsområdet är att vissa svenska bolag har ett krav om svenskt medborgarskap för att individer ska få arbeta med frågorna, vilket istället utesluter internationella kompetenser. Tematiskt upplevs det även finnas en brist på individer med god multidisciplinär kompetens, exempelvis inom elkraft tillsammans med risk- och krishantering, eller elkraft tillsammans med datavetenskap.

Näringslivet upplever en brist på kompetens inom ett antal områden. Hos elnätbolag finns det ett stort behov av ingenjörer med kvalificerad kompetens inom säkerhet, både gällande IT och den fysiska infrastrukturen. Det efterfrågas även spetskompetens inom exempelvis IT i bredare bemärkelse; systemdesign, integration, molntjänster, nät och kommunikation. I likhet med akademien efterfrågas även generalister som kan tillräckligt mycket om de olika områdena för att kunna samordna arbetet. Framöver kommer det också finnas ett behov av utbildad driftspersonal som kan hantera de nya digitaliserade systemen.

Vidare upplevs det att det finns kluster där det finns god tillgång till kompetens, exempelvis i geografiska regioner med stora universitet och inom de större elnätbolagen. Däremot upplevs det svårare att knyta till sig kompetensen hos mindre nätbolag, och i regioner utan stora lärosäten. Det efterfrågas därför kunskapsunderlag som hjälper dessa mindre aktörer att hantera de utmaningar de står inför, exempelvis på områdena digitalisering, förändrad och ny konsumtion och decentraliserad elproduktion. En fråga som har lyfts är också vilka risker som finns för kaskadeffekter om flera små aktörer skulle slås ut. För att motverka detta och skapa ett resilient och tryggt elsystem är det viktigt att alla aktörer är förberedda och har en god kompetens på området.

Slutligen upplevs det inom näringslivet att arbetet med hur företag ska arbeta med cybersäkerhet kan förbättras. Även om det finns information tillgänglig, bland annat via MSB, upplevs det att kunskapen inte är tillräckligt lättillgänglig, och det krävs en grundförståelse för ämnet för att kunna omsätta den i verksamheten. Även här är problematiken större bland mindre bolag.



Referenslista

- 1 Enisa (2022), [ENISA THREAT LANDSCAPE 2021](#)
- 2 Regeringen (2022), [Nationell strategi för elektrifiering – en trygg, konkurrenskraftig och hållbar elförsörjning för en historisk klimatomställning.](#)
- 3 Regeringen (2018), [Nationell strategi för samhällets informationsoch cybersäkerhet](#)
- 4 Nationellt cybersäkerhetscenter (2022), [Vårt uppdrag](#)
- 5 Regeringen (2022), [MSB stärker förebyggandet och hanterandet av it-incidenter](#)
- 6 Energiforsk, [Nätverk för cybersäkerhet.](#)
- 7 IDA (2021), [Real-Time Systems Laboratory.](#)
- 8 MDU(2022), [Framtidens energi.](#)
- 9 MDU (2022), [Förnybar energi.](#)
- 10 MDU (2022), [Digitalisering.](#)
- 11 Cybernode (2022), [Om noden.](#)
- 12 Energiföretagen (2022), [Säkerhet/cybersäkerhet.](#)
- 13 FOI (2021), [Om FOI](#)
- 14 FOI (2021), [Energi](#)
- 15 Länsstyrelserna i Skåne län, Stockholms län, Uppsala län, Västra Götalands län (2020), [Förutsättningar för en trygg elförsörjning.](#)
- 16 Energimyndigheten (2022), [Trygg elförsörjning.](#)
- 17 Nordic Energy Research (2021), [The structure of the Nordic Energy Outlooks.](#)
- 18 Nordic Energy Research (2021), [Nordgrid Program.](#)
- 19 Energiforsk, [Programbeskrivning – Risk och Tillförlitlighetsanalys \(år 2021–2025\).](#)
- 20 Energiforsk, [Program för Digitalisering och IT-säkerhet 2018–2022.](#)
- 21 MSB (2021), [Forskning inom civilt försvar, samhällsviktig verksamhet, krisberedskap.](#)
- 22 Svenska kraftnät (2020), [Forsknings- och utvecklingsplan 2021–2024.](#)
- 23 Energimyndigheten (2018), [SweGRIDS.](#)
- 24 MSB (2021), [Resilient Information and Control Systems \(RICS\).](#)
- 25 MSB (2021), [Forskning inom informationssäkerhet.](#)
- 26 Lunds universitet (2021), [CenCIP:s Syfte och mål.](#) Error! Hyperlink reference not valid.
- 27 MSB (2018), [Infrastrukturer skyddas från cyberhot.](#)
- 28 KTH (2021), [CERES- Center for Resilient Critical Infrastructures.](#)
- 29 KTH (2022), [Centrum för cyberförsvar och informationssäkerhet.](#)
- 30 RISE (2021), [Cyber range stärker svensk kompetens inom cybersäkerhet.](#)
- 31 MSB (2019), [Nationell cyber range och testbädd.](#)

- 32 RISE (2022), [Cyber range – testbädd för cybersäkerhet](#).
- 33 Digital futures (2022), [About](#).
- 34 RISE (2022), [Systemförändring med lokalt delad energi](#).
- 35 Energimyndigheten (2021), [Kompetenscentrum 2022–2026](#).
- 36 ITRC (2020), [Who we are](#).
- 37 CIRI (2022), [About Us](#).
- 38 Svenska kraftnät (2022), [Nordiskt varnings- och skyddssystem](#).
- 39 MultiDC (2022), [MultiDC](#).
- 40 Nordic Energy Research (2021), [The project Resilient Digital Sustainable Energy Transition](#).
- 41 Energimyndigheten (2022), [Projektinformation REDISET](#).
- 42 Cigre (2022), [Introducing CIGRE](#).
- 43 ENTSO-E (2022), [ENTSO-E Mission Statement](#).
- 44 EU-DSO (2022), [Missions](#).
- 45 ENISA (2022), [About ENISA](#).
- 46 ECCC (2022), [European Cybersecurity Competence Centre and Network](#).
- 47 MSB (2022), [About NCC-SE](#).
- 48 FOI (2021), [Energisystem för robust energiförsörjning](#).

Bilaga A: Medverkande respondenter

Informella intervjuer

Tommy Wahlman, Energimyndigheten

Mathias Eksted, Professor, Kungliga Tekniska högskolan

Formella intervjuer

Eva Thorin, Mälardalens universitet

Lina Bertling Tjernberg, Kungliga Tekniska högskolan

Simin Nadjm-Tehrani, Linköpings universitet

Math Bollen, Luleå universitet

Jonas Johansson, Lunds universitet

Inger-Lise Svensson, RISE

Hans Grönqvist, RISE

Senja Nordström, Energimyndigheten

Susanne Stjernfelt, Energiforsk

Jan-Olof Olsson, MSB

Per Wikström, Energiföretagen

Patrik Sandgren, Teknikföretagen

Robert Eriksson, Svenska kraftnät

Anders Åhlgren, Jönköping Energi

Fredrik Carlsson, Vattenfall

Michele Luvisotto, Hitachi Energy

Mats Karlström, Ferroamp

Mejlsvar

Erik Sundström, MSB



Bilaga B: Genomförande

Förstudie

Inför arbetet med syntesrapporten genomfördes en förstudie i december 2021. Förstudien bestod av två informella intervjuer med personer från Energimyndigheten och KTH. Utifrån de inspel som uppkom under intervjuerna bildades en första översikt av området, och relevanta ämnesområden för syntesrapportens kartläggning identifierades. Vid intervjuerna gavs också rekommendationer på relevanta respondenter att kontakta för formella intervjuer.

Intervjustudie

För att besvara rapportens frågeställningar har 19 semistrukturerade intervjuer genomförts under tidsperioden december 2021–mars 2022 (se specifikation i Bilaga A). Respondentgruppen består av forskare, finansiärer av forskningen, samt aktörer från näringslivet och offentlig sektor som arbetar med frågor kopplade till området. Intervjufrågorna har utformats med avsikt att kunna använda respondenternas svar som huvudsakligt underlag för kartläggning av pågående forskning inom området, nuvarande finansiärer, särskilda satsningar som har genomförts, och identifiering av framtida forskningsbehov.

Respondenterna till intervjustudien har inledningsvis valts utifrån de förslag som uppkom i förstudien, och utifrån Power Circles initiala kännedom om aktörer inom området. Ytterligare respondenter har tillkommit under studiens gång på rekommendation av intervjuade respondenter. Respondenterna från näringslivet representerar olika aktörsperspektiv kring resilient och trygg elförsörjning; bland de svarande finns representation från energibolag, teknikleverantörer, tjänsteleverantörer på elmarknaden samt Svenska kraftnät. I respondentgruppen finns också representanter från de organisationer som de intervjuade forskarna har identifierat som centrala finansiärer av forskning på området.

Enkätstudie

I tillägg till intervjustudien har en enkätstudie genomförts för att samla in ett bredare kunskapsunderlag. Enkäten har skickats ut till universitet, högskolor, forskningsinstitut, länsstyrelser och näringslivsaktörer. Urvalet av vilka personer som enkäten skickades till gjordes genom en genomgång av hemsidorna till alla universitet och högskolor i Sverige, för att identifiera kontaktpersoner enligt avgränsningarna, och för kontakter inom näringslivet har Power Circles nätverk använts. Enkäten har även skickats till aktörer och organisationer som har nämnts under intervjuerna, samt till samtliga länsstyrelser i landet. Enkäten har skickats ut till 34 respondenter inom akademien, varav 11 svarade, och till 21 länsstyrelser, varav 8 svarade. Inom näringslivet skickades enkäten till 18 aktörer, varav 4 svarade.

Skrivbordsstudie

Som ett tillägg till intervju- och enkätstudien har en skrivbordsstudie genomförts för att studera kompletterande skriftliga referenser som uppgivits av intervjustudiens respondenter. Referenserna har inkluderat interna underlagsrapporter samt annan publicerad skriftlig information om pågående forskning om resilient och trygg elförsörjning.

Analys av inhämtad information

Utifrån respondenternas svar i intervjustudien och enkätstudien, samt skrivbordsstudiens referensunderlag, har syntesen skapats för att besvara frågeställningarna. Informationen som presenteras i syntesrapporten reflekterar därmed till stor del en sammanställande analys av de intervjuade individernas, respektive de representerade organisationernas, svar på frågor som ställts i intervju- respektive enkätstudien. Analysen syftar till att skapa en översiktlig bild över nuläget och framtida forsknings- och finansieringsbehov. Det ska nämnas att området är brett och analysen ger en översiktlig, men inte komplett, bild av området och dess forskningsfront.

