

Ärende nr: SvK 2024/3555

Datum: 2024-09-27

---

# Risk- och sårbarhetsbedömning för år 2024

**Sammandrag av Affärsverket svenska kraftnäts sammanfattande redovisning**

---

# Svenska kraftnät

---

Svenska kraftnät är systemansvarig myndighet, med uppgift att på ett affärsmässigt sätt förvalta, driva och utveckla ett kostnadseffektivt, driftsäkert och miljöanpassat kraftöverföringssystem. Det omfattar ledningar för 400 kV och 220 kV med stationer och utlandsförbindelser. Svenska kraftnät utvecklar transmissionsnätet och elmarknaden för att möta samhällets behov av en säker, hållbar och ekonomisk elförsörjning. Därmed har Svenska kraftnät också en viktig roll i klimatomställningen.

**Version Rapporten baseras på SvK 2024/3555**  
Org. Nr 202 100-4284

Svenska kraftnät  
Box 1200  
172 24 Sundbyberg  
Sturegatan 1

Tel: 010-475 80 00  
Fax: 010-475 89 50  
[www.svk.se](http://www.svk.se)

# Innehåll

1	En robust elförsörjning .....	6
2	Samhällsviktig verksamhet av nationell betydelse .....	6
2.1	Om kraftsystemet .....	7
2.2	Överföring av el (transmission).....	8
2.3	Distribution av el (region- och lokalnät).....	9
2.4	Produktion av el .....	9
2.5	Elmarknad .....	10
2.5.1	Handel av el .....	10
2.5.2	Balansering .....	10
2.6	Resurser för att hantera olika driftskeden och drifttillstånd .....	11
2.6.1	Stödtjänster, avhjälpande åtgärder och strategiska reserver .....	11
2.6.2	Regional/lokal ö-drift.....	12
2.7	Åtgärder för förstärkt leveranssäkerhet och försörjningstrygghet .....	13
3	Kritiska beroenden för identifierad samhällsviktig verksamhet .....	14
4	Identifierade och analyserade hot och risker.....	15
4.1	Beröringspunkter med andra hot- och trendanalyser .....	16
4.2	Förändringar i den övergripande riskbilden inom elförsörjningen.....	17
4.3	Om fördjupningsområden i årets arbete.....	19
4.3.1	Fördjupningsområde: förmåga till att återuppbygga kraftsystemet efter inträffat nätsammanbrott.....	19
4.3.2	Fördjupningsområde: förmåga att upprätthålla lokal reservkraft (inkl. drivmedelsförsörjning).....	20
4.3.3	Fördjupningsområde: beroende av GNSS inom elförsörjningen.....	20
5	Övergripande förmågebedömning för elförsörjningen .....	21
	Bilaga 1 – De övergripande riskkällorna .....	23
	1.1 Fortsatt integrering av det nationella elsystemet: ökad internationalisering	23
	1.2 Fortsatt integrering av det nationella elsystemet: fortsatt decentralisering av det nationella elsystemet .....	24

<i>1.3 Optimering av kritisk verksamhet inom elförsörjningen: minskad redundans avseende kritiska funktioner .....</i>	<i>25</i>
<i>1.4 Optimering av kritisk verksamhet inom elförsörjningen: outsourcing av kritiska verksamheter .....</i>	<i>26</i>
<i>1.5 Optimering av kritisk verksamhet inom elförsörjningen: bristande säkerhet i IT-leverantörskedjor .....</i>	<i>27</i>
<i>1.6 Optimering av kritisk verksamhet inom elförsörjningen: bristfälliga upphandlingar avseende säkra tjänster och produkter inom IT/OT .....</i>	<i>28</i>
<i>1.7 Cyberrisker och – hot: en allt starkare integration mellan IT och OT .....</i>	<i>29</i>
<i>1.8 Cyberrisker och – hot: ökad komplexitet i IT-system och IT-tjänster .....</i>	<i>31</i>
<i>1.9 Cyberrisker och – hot: bristfälligt säkerhetsskydd avseende IT-miljöer (främst OT) .....</i>	<i>31</i>
<i>1.10 Spionage och olovlig underrättelseinhämtning .....</i>	<i>32</i>
<i>1.11 Omfattande skador på samhällsviktig infrastruktur .....</i>	<i>33</i>
<i>1.12 Omfattande, plötsligt personalbortfall i kritiska funktioner inom elförsörjningen .....</i>	<i>36</i>
<i>1.13 Överlappande och divergerande bestämmelser och lagstadgade krav på aktörer inom elförsörjningen .....</i>	<i>37</i>
<i>1.14 Differentierad informationshantering inom elförsörjningen i stort .....</i>	<i>38</i>
<i>1.15 Otillräcklig kapacitet (avseende både nätkapacitet och effekt) .....</i>	<i>39</i>
<i>1.16 Begränsningar i viktiga förmågor och resurser att hantera olika systemdrifttillstånd .....</i>	<i>40</i>
<i>1.17 Störningar i kritiska beroenden, andra sektorer, kritiska försörjningskedjor eller tjänster som elförsörjningen är beroende av .....</i>	<i>41</i>

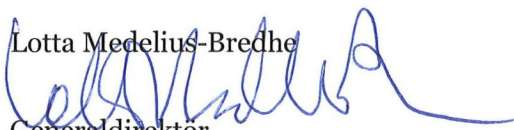
## Förord

Kriget i Ukraina har fortsatt prägla den säkerhetspolitiska utvecklingen i vårt närområde. I Sverige har Säkerhetspolisen höjt terrorhotnivån, som en följd av ett försämrat säkerhetsläge.

I ljuset av den aktuella utvecklingen är sådana initiativ som syftar till att förstärka försörjningstryggheten inom elförsörjningen såväl nationellt som internationellt av en stor betydelse för beredskapsförmågan. Som exempel kan ett intensifierat samarbete mellan systemoperatörerna kring Östersjön under 2023 nämnas. Nationellt har vikten av att förstärka försörjningstryggheten lyfts genom bl.a. regeringsuppdrag. Regeringen har även föreslagit att Svenska kraftnät ska få ett övergripande ansvar för att samordna den långsiktiga planeringen av det nationella elsystemet och sammanlänkningen av detta med andra länder. Den utveckling som nu sker kan återspeglas mot de utmaningar som vi ser i vår omvärld.

Den nationella risk- och sårbarhetsanalysen för elförsörjningen fokuserar huvudsakligen på sådant som - ur ett beredskapsperspektiv - kan utmana förmågan till verksamhet inom det nationella elsystemet. Ett system som sträcker sig från den lokala nivån till den regionala och upp till den nationella nivån – som i sin tur är integrerat med elsystem i andra länder. Ett system som baseras på teknik och fysikens lagar men som utformas av såväl nationell som europeisk lagstiftning och energipolitik. Ett system som till syvende och sist syftar till att säkerställa den grundläggande funktionaliteten i vårt samhälle – där olika typer av aktörer, både offentliga och privata, bidrar till helheten. Denna komplexitet präglar den breda risk- och hotbild inom elförsörjningen som redovisas i rapporten.

Att fortsatt vidta robusthets- och säkerhetshöjande åtgärder kräver en förmåga att navigera i det föränderliga risk- och hotlandskapet och också att kunna förhålla sig till förändrade förutsättningar i omvärlden.

Lotta Medelius-Bredhe  
  
Generaldirektör

# 1 En robust elförsörjning

Elförsörjningen är en nationellt samhällsviktig verksamhet och en förutsättning för samhällets funktionalitet. För att säkra en god leveranssäkerhet ska de mest nödvändiga funktionerna inom elförsörjningen kunna upprätthållas vid svåra påfrestningar i fredstid, men även vid höjd beredskap och krig.

Årets rapport har fokus på sådana förmågor som upprätthåller den samhällskritiska funktionaliteten inom elförsörjningen, särskilt med avseende på förmågor som är viktiga vid störningar i elförsörjningen - där tillgången till lokal reservkraft är av viktig betydelse - samt vid nätåteruppbyggnad efter ett inträffat nätsammanbrott.

Svenska kraftnät analyserar hot och risker inom myndigheten och elförsörjningen.

Svenska kraftnät upprättar en samlad risk- och sårbarhetsanalys för elsektorn enligt förordning om statliga myndigheters beredskap samt elberedskapslagen.

I rapporten ingår även beskrivningar av potentiella riskkällor inom elförsörjningen, vilket utgör en grund för den övergripande riskbilden samt övergripande bedömningar av förmågan inom elförsörjningen.

# 2 Samhällsviktig verksamhet av nationell betydelse

Inom elförsörjningen finns det aktörer som producerar, distribuerar och handlar med el. Ett omfattande elavbrott påverkar bland annat elektroniska kommunikationer, transporter, kommunalteknisk försörjning (t.ex. dricksvattenförsörjning, avloppshantering, väghållning), vård- och omsorg, övrig energiförsörjning och finansiella tjänster. Det finns vissa samhällsviktiga verksamheter som omedelbart avstannar vid ett elavbrott om de saknar egen reservkraft. Ett omfattande, långvarigt elavbrott kan få konsekvenser för flera samhällsviktiga verksamheter.

Den samhällsviktiga verksamheten bedöms omfatta sådana operativa och strategiska funktioner som säkerställer både transmission, distribution, produktion och handel av el, både i normalfall men även vid störningar och krissituationer. Vid allvarliga störningar inom elförsörjningen behövs därtill en förmåga till operativ felavhjälpning samt krisledning - inklusive lägesbild, kriskommunikation, samverkan med övriga aktörer mm.

Med samhällsviktig verksamhet avses verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet.

Efter ett eventuellt inträffat nätsammanbrott är förmågan till återstart av kraftsystemet av yttersta vikt.

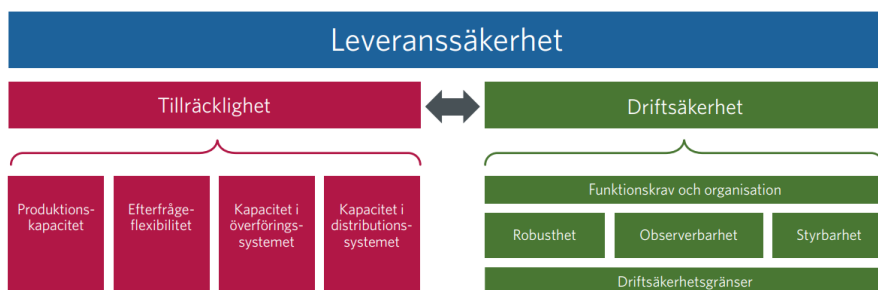
För att upprätthålla funktionaliteten inom elförsörjningen finns ett kritiskt beroende av teknisk infrastruktur, inklusive IT-infrastruktur, som möjliggör den samhällsviktiga verksamheten och

därmed utgör en viktig utgångspunkt för riskanalysen.

## 2.1 Om kraftsystemet

Kraftsystemets syfte är att överföra el från producenter till elanvändare på ett driftsäkert sätt. Överföring och distribution av el kan endast göras när produktion, nät och förbrukning samverkar driftsäkert, där Svenska kraftnät som systemoperatör för överföringssystemet för el har ett övergripande ansvar.

Svenska kraftnät ansvarar för den kortsiktiga effektbalansen samt att kraftsystemet kan hantera störningar och snabbt återställas till normaldrift. Balans mellan produktion och förbrukning av el är en förutsättning för att kraftsystemet ska fungera driftsäkert och för att slutkunden ska få sin el levererad.



Figur 1: Svenska kraftnäts modell för leveranssäkerhet

Det finns ett ömsesidigt beroende mellan aktörer inom elförsörjningen. Den överliggande nivån (Svenska kraftnäts transmissionsnät) som används för att överföra elen över längre sträckor är en förutsättning för de underliggande spänningsnivåernas funktionalitet. Svenska kraftnät är för sin verksamhet beroende av andra elaktörer (elproducenter, elnätsföretag och elhandelsföretag) för att säkerställa den samhällsviktiga verksamhet som Svenska kraftnät som systemansvarig för överföringssystemet för el ansvarar för. Det finns, med andra ord, en del tekniska förmågor som möjliggörs av andra aktörer inom elförsörjningen och som behövs för att elsystemet som helhet ska fungera.

En annan aspekt, kopplad till kraftsystemets tekniska förmågor, handlar om att säkerställa olika förmågor som finns i elanläggningar utspridda över landet. Det är även viktigt med avseende på sådana händelser (t.ex. extremt väder, antagonistiska angrepp, krigshandlingar) som kan innebära en risk för skador på fysisk (fast) infrastruktur. Detta utgör därmed en viktig parameter i en beredskaps- och totalförsvarsplanering som är bunden till en geografisk dimension.

Det svenska kraftsystemet är både tekniskt men även marknadsmässigt sammankopplat med de nordiska länderna inom samma synkronområde, som i sin tur är sammankopplat med de kontinentaleuropeiska kraftsystemen. Därför är det viktigt att i analysen beakta hela synkronområdet, då det svenska kraftsystemet kan påverkas av eventuella risker och sårbarheter i våra grannländer och i vårt närområde – men också för att dra nytta av förmågor i omvärlden.

Kraftsystemet kommer att integreras allt mer med nya ledningar och marknadslösningar, där ett exempel på det senare är det gemensamma nordiska samarbetsprojektet Nordic Balancing Model (NBM), som syftar till att reglera obalanser i varje enskilt elområde istället för synkronområdet som helhet. Vidare samordnas arbetet med införandet av en nordisk kapacitetsmarknad ”Flowbased” och en marknad för automatiska frekvensåterställningsreserver. NBM har också arbetat med att förkorta avräkningsperioden för obalanser från 60 minuter till 15 minuter vilket innebär betydligt fler handelsperioder under dygnet. Detta medför ett ökat informationsflöde och behov av nya robusta tekniska verktyg/system som kräver en markant ökad digitalisering av berörda funktioner.

## 2.2 Överföring av el (transmission)

Svenska kraftnät, systemansvarig för överföringssystemet för el, äger och förvaltar det svenska transmissionsnätet, som består av ledningar och stationer



över hela landet. Transmissionsnätet består av 17 000 km luftledning och 2000 km jordkabel, drygt 200 transformator- och kopplingsstationer samt utlandsförbindelser med både växel- och likström. Genom transmissionsnätet överförs eleffekt från produktionsanläggningar, så som bl.a. vattenkraft och vindkraft, för elförbrukning på de lägre distributionsnivåerna. Det svenska kraftsystemet binds samman med ett flertal utlandsförbindelser mot andra nordiska länder och HVDC-kopplingar till Tyskland, Danmark, Polen och Litauen.

Driftsäkerheten och leveranssäkerheten i transmissionsnätet dimensioneras utifrån N-1 principen, dvs. att det klarar bortfall av varje enskilt objekt eller enskild komponent utan att felet leder till störningar inom elförsörjningen inom 15 minuter.

## 2.3 Distribution av el (region- och lokalnät)

Elen distribueras av nätägare på region- och lokalnätsnivå vidare till slutanvändare. Regionnäten består av 30 000 km luftledning och 2000 km jordkabel och lokalnäten ca 114 000 km luftledning och 426 000 km jordkabel med ett stort antal stationer, utspridda över landet. I Sverige finns idag cirka 170 elnätsföretag som äger och driver lokal- och regionnät. Av dessa är 129 kommunalt ägda bolag.

## 2.4 Produktion av el

Den dominerade ägaren av svensk elproduktion är staten via helägda Vattenfall. Näst största ägaren är Uniper, med tyska staten som

majoritetsägare. Den tredje största ägaren är Fortum, men finska staten som majoritetsägare. Den fjärde största ägaren är Sveriges kommuner.

Elproducenternas skyldighet att producera el bygger på avtal med kunder, och är därmed inget offentligrättsligt krav, utan ett civilrättsligt åtagande.

Vid krig, eller genom särskilt regeringsbeslut, får Svenska kraftnät ett mandat att planera, leda och samordna elförsörjningens resurser, för att tillsammans med övriga totalförsvarsmyndigheter tillgodose samhällets behov av elkraft.

Exempel på kraftslag (andel från 2023) är vattenkraft (42,5% av den totala svenska elproduktionen), kärnkraft (30%), vindkraft (22%), värmekraft (4,5%) och solkraft (1%).

Större vattenkraftsanläggningar finns i norra och mellersta Sverige (elområde SE1 och SE2). Kärnkraftsanläggningarna finns i elområde SE3.

Vindkraftsproduktionen finns i alla elområden (dock är installerad effekt av vindkraft dominerande i SE2 och SE3) medan kraftvärme (fjärrvärme) är dominerande i SE3.

Vattenkraften är, inte minst med dess reglerkraftförmåga, mycket viktig för kraftsystemets leveranssäkerhet. Kärnkraft, vattenkraft och biobaserad kraftvärme bidrar med fossilfri elproduktion som också är synkronansluten till nätet. Synkront ansluten produktion bidrar med rotationsenergi och förmågan att reglera den reaktiva effekten i kraftsystemet, till skillnad från dagens effektelektronikanslutna kraftslag som vind- och solkraft. Vidare tillför kärnkraften även reaktiv effekt, som bidrar till spänningsstabiliteten.

Andelen vindkraft och solkraft förutspås att öka i framtiden. Svenska kraftnät har också börjat motta ansökningar om stora solkraftsparker.

## 2.5 Elmarknad

Elmarknaden kan beskrivas utifrån två huvudsakliga verksamheter: elhandel och balansmarknad.

### 2.5.1 Handel av el

Elmarknaden utgör ramen för elproducenternas operativa produktionsplanering. Den fysiska elhandeln sker mestadels via särskilda elbörser där elhandelsbolag köper el från elproducenter och säljer den vidare till sina kunder. Aktörer på elmarknaden består således av elhandelsföretag, elproducenter, större elanvändare, elleverantörer och balansansvariga aktörer (som åtar sig balansansvaret för elleveransen). Elmarknaden omfattar både dagen före-marknaden och intradagmarknad.

### 2.5.2 Balansering

På reglerkraftmarknaden (RKM) avropar den systemansvariga för el balansenergi bud (dvs. reglerkraft) som kan aktiveras inom 15 minuter för att upprätthålla balans mellan produktion och förbrukning. RKM kommer att genomgå betydande förändringar under de kommande åren med NBM och i och med anslutning till de europeiska marknadsplattformarna för utbyte av

balansenergi MARI (mFRR) och PICASSO (aFRR) – som de nordiska systemansvariga kommer att ansluta sig till.

## 2.6 Resurser för att hantera olika driftskeden och drifttillstånd

För att säkerställa driftsäkerheten i kraftsystemet och därmed förbygga och hantera störningar inom elförsörjningen, är det viktigt att det finns särskilda resurser att tillgå. Nedan följer en mycket övergripande beskrivning av exempel

på sådana resurser, som till stor del är marknadsbaserade.

Svenska kraftnät har enligt elmarknadsdirektivet ett ansvar att säkerställa att det finns tillräckligt med stödtjänster tillgängliga för att upprätthålla driftsäkerheten samt hantera överträdelser.

Som systemansvarig för överföringssystemet för el ska Svenska kraftnät alltid säkerställa att kraftsystemet kan återföras till normaldrift inom 15 minuter efter att ett enskilt fel inträffat.

Det finns även andra verktyg, resurser och metoder för att säkerställa kraftsystemets funktionalitet. Ett exempel är automatisk frånkoppling (AFK) för systemskydd samt manuell förbrukningsfrånkoppling (MFK) vid effektbristsituationer. Även nödeffekt från likströmsförbindelser (EPC) är en resurs för att upprätthålla frekvensstabiliteten.

### 2.6.1 Stödtjänster, avhjälpande åtgärder och strategiska reserver

Vissa elproducenter tillhandahåller upphandlade stödtjänster för att stötta och stabilisera kraftsystemet. Det är viktigt att det finns tillgängliga marknadsbud inom de prisområden där behov uppstår. I egenskap av systemansvarig för överföringssystemet för el upphandlar Svenska kraftnät stödtjänster för att upprätthålla balansen och driftsäkerheten i kraftsystemet. Anmälan om att bli en leverantör av stödtjänster görs till den systemansvariga myndigheten enligt framtaget regelverk.

Om buden på reglerkraftmarknaden inte räcker till för att upprätthålla effektbalansen aktiveras störningsreserven som kan startas vid svåra störningar inom elförsörjningen. Denna har därigenom en avhjälpande effekt att stabilisera frekvensen vid tillfällig eleffektbrist. I dag består störningsreserven i huvudsak av gasturbiner, eftersom de kan startas mycket snabbt och börja producera el.

För närvarande äger staten genom Svenska kraftnät aktiebolaget Svensk Kraftreserv AB, som utgör en knapp majoritet av störningsreserven. Flertalet avtal i störningsreserven löper ut den 31 december 2024, inklusive Svenska kraftnäts avtal med dotterbolaget Svenska Kraftreserv. Sedan 2020 har Svenska kraftnät även gjort en kompletterande upphandling av störningsreserven på årsbasis om ca 300 MW. De nuvarande avtalen för den kompletterande upphandlingen upphör i juni 2024 och Svenska kraftnät har för avsikt att ersätta den årliga upphandlingen med marknaden för mFRR balanskapacitet.

Effektreserven är en strategisk reserv (s.k. kapacitetsmekanism), som finns för att avhjälpa effektbristsituationer under vinterhalvåret. Effektreserven aktiveras först efter det att alla kommersiella bud på reglerkraftmarknaden har avropats. Kapacitetsmekanism är alltså en temporär åtgärd för att säkerställa en nödvändig nivå av resurstillräcklighet.

Enligt EU:s elmarknadsförordning behövs numera ett godkännande från EU-kommissionen för att införa eller förlänga en kapacitetsmekanism. Svenska kraftnät har kontrakterat 562 MW i Karlshamnsverket som effektreserv fram till 15 mars 2025.

### **2.6.2 Regional/lokal ö-drift**

En nationellt sammanhållen elförsörjning och en återuppbyggnad av en sådan nationellt sammanhållen elförsörjning behöver alltid vara en prioritet till följd av hur det svenska kraftsystemet är uppbyggt med stor andel av produktionen i norr och stor andel av förbrukningen i söder. Men i situationer där återuppbyggnaden blir omfattande och långvarig, kan regional/lokal ö-drift vara ett alternativ för att säkerställa att de allra högst prioriterade samhällsfunktionerna får el. Sådan regional/lokal ö-drift har stora utmaningar och därför behöver redundans, återuppbyggnad och reservkraft vara högre prioriterade åtgärder.

Bland ö-driftens begränsningar bör följande nämnas:

- > I många ö-driftområden kommer mängden el som levereras vara kraftigt begränsad och inte räcka till alla som behöver el inom området. Det kommer bli nödvändigt med hårda prioriteringar mellan vilka användare som ska få el under en ö-drift.
- > Vilken faktisk förmåga att leverera el som kommer att finnas inom respektive ö-driftområde kommer vara svår att veta i förväg eftersom den i de allra flesta fall inte kommer gå att testa skarpt fullt ut.

- > Verksamheter som är kraftigt beroende av el kan inte förvänta sig att få el via ö-drift utan behöver ha alternativa lösningar.

För att ö-drift ska fungera krävs förutom ansluten elproduktion bland annat förmåga till frekvens- och spänningsreglering inom det berörda ö-nätet. Denna typ av produktion kan till exempel utgöras av gasturbiner, dieslaggregat, kraftvärmeverk eller vattenkraftverk. De tekniska förmågorna och förutsättningarna för drift av denna typ av delsystem kan variera mellan olika regioner och kan kräva särskilda förutsättningar (t.ex. omkopplingar) i elnätet. En annan viktig förutsättning är att det finns instruktioner och planer för ö-drift, för de inblandade aktörerna inom respektive område.

## 2.7 Åtgärder för förstärkt leveranssäkerhet och försörjningstrygghet

Svenska kraftnät och Energimyndigheten fick i slutet av 2022 ett uppdrag av regeringen att intensifiera arbetet med att stärka försörjningstryggheten i energisektorn på kort och lång sikt, med huvudfokus på trygg elförsörjning. Uppdraget var indelat i sex deluppdrag, med fokus bland annat på kapacitetsmekanismer, driftsäkerhet samt avhjälpande åtgärder och stödtjänster.

För att säkerställa tillräckligt med resurser vid effektbrist föreslår Svenska kraftnät en justering av förordningen om effektreserven så att ytterligare volymer kan upphandlas men också att en ny lag om effektreserv tas fram för perioden mars 2025 till 2032 då en ny, marknadsomfattande kapacitetsmekanism, kan vara på plats. Vad gäller stödtjänster och avhjälpande åtgärder utvärderar Svenska kraftnät kontinuerligt marknader och krav för att uppfylla kraftsystemets behov givet de förändringar som sker.

Den kommande utvecklingen och de föreslagna lösningarna bedöms medföra en diversifiering av förmågan. Dessa lösningar förutsätter dock en fortsatt fungerande elmarknad och innebär också ett ökat beroende av gemensamma och internationella marknader (både nordiskt och också europeiskt).

För att säkerställa en god leveranssäkerhet i det framtida energisystemet med förändrade flöden i nätet behövs även systemförstärkande åtgärder såsom investeringar i transmissionsnätet i form av nya ledningar och stationer men även nya investeringsbeslut i elproduktionen (inklusive geografisk placering) samt införande av nya energibärare (främst vätgas). Att öka flexibiliteten är också av stor vikt för att säkra leveranssäkerheten framöver och öka resurstillräckligheten i kraftsystemet.

Svenska kraftnät bedömer i sin Nätutvecklingsplan 2024-2033 att det behövs ett årligt produktionstillskott motsvarande elförbrukningen i Stockholm från nu fram till år 2045 för att täcka kommande förbrukningsökning, för att klara den gröna omställningen samt ersätta befintlig produktion som går ur tiden.

Svenska kraftnät har under hösten 2023 stöttat Energimyndigheten i Uppdrag om energiförsörjning för totalförsvaret. Regeringsuppdraget syftar till att analysera behoven av energiförsörjning för totalförsvaret. Svenska kraftnät har stöttat Energimyndigheten i uppdraget genom att ta fram en metod för att uppskatta Sveriges normala elbehov i fredstid samt totalförsvarets behov av el inför, under och efter höjd beredskap. Svenska kraftnät har även stöttat genom att föreslå en geografisk områdesindelning av Sverige för att uppskatta normala elbehov samt uppskatta totalförsvarets elbehov.

Resultatet av metoden ska kunna användas för att på en övergripande, nationell nivå kunna styra var elen behövs som mest och även inom geografiska områden kunna analysera tillgången på el och förmågor för att kunna upprätthålla elförsörjningen.

### 3 Kritiska beroenden för identifierad samhällsviktig verksamhet

Nedan redogörs för exempel på kritiska beroenden som upprätthåller den samhällsviktiga funktionaliteten inom elförsörjningen. Exempelen är på en övergripande nivå, och mer detaljerade beskrivningar, inklusive acceptabla avbrottstider för de kritiska beroendena, bör tas fram inom enskilda organisationer som ansvarar för samhällsviktig verksamhet (t.ex. inom ramen för verksamhetens kontinuitetshandling).

I kapitel 2 tas exempel upp på sådana kritiska resurser som upprätthåller de grundläggande tekniska förmågorna inom elförsörjningen. Det bör även noteras att elproduktionen har, utöver vissa andra beroenden som berörs i detta kapitel, även ett kritiskt beroende av produktionskällor/”bränsle” kopplat till ett visst kraftslag (till exempel vatten för vattenkraften, uran för kärnkraften etc.).

Vissa beroenden är kritiska för den dagliga driften, i vissa fall är kritiska för att kunna upprätthålla verksamheten i en kris- eller krigssituation:

- > *Teknisk infrastruktur* – som kan delas in i *elanläggningar* samt *IT-infrastruktur* som behövs för att exempelvis kunna styra och övervaka elnätet och – produktionen.
  - > Utöver elanläggningar finns även andra *viktiga lokaler*, såsom kontrollrum för den operativa verksamheten men även övriga kontorsutrymmen. Tillgång till reservdriftställe som medger teknisk drift om ordinarie driftsställe och IT- system faller bort.
- > *Information* - tillgång till ur ett riktighetsperspektiv *rätt information, data och planer* (t.ex. kopplat till *övervakning och styrning*), samt *kartunderlag och väder – mm. prognoser. Teknisk dokumentation* avseende aktörsbundna kritiska försörjningskedjor. Tillgång till *störningsinformation* och en aktuell och riktig *lägesbild* för att kunna hantera en störningssituation.
- > *Elektroniska kommunikationer*.
- > *Reservdelar och reparationsmateriel* för felavhjälpning vid en störning inklusive lager/depåer.
  - > Framkomlighet för transport av materiel och personal, till exempel vid reparationsarbete.
  - > Omlastningsplatser för av/pålastningar av tung materiel.
- > *Personella resurser* – funktioner med spetskompetens inom samhällsviktig verksamhet inom elförsörjningen. Även externa entreprenörer, leverantörer och tekniker kan vara ett kritiskt beroende.
- > *Samverkan* med andra företag inom elsektorn, till exempel för att kunna kalla fältpersonal från andra företag till reparationsarbete. Stöd från aktörer i samhället, till exempel räddningstjänst, polis, Försvarmakten och frivilligorganisationer.
- > *Beredskapsorganisation*, dvs. en fungerande kris- och krigsorganisation/storstörningsorganisation.

## 4 Identifierade och analyserade hot och risker

Nedan sammanfattas den övergripande riskbild inom elförsörjningen som baseras på identifierade riskkällor. Riskkällorna redovisas i sin helhet i bilaga 1. Syftet är att illustrera det breda spektrum av potentiella risker, hot och sårbarheter inom elförsörjningen som kan få en påverkan på den förmåga som

behöver upprätthållas inom elförsörjningen – och därigenom på samhällets funktionalitet.

Det görs inte någon samlad analys av de ingående riskkällorna utifrån sannolikhet och konsekvens men i bilaga 1 ges exempel på möjliga konsekvenser av de identifierade riskkällorna, samt riskreducerande eller -mitigerande åtgärder. Hur de faktiska konsekvenserna kan bli beror på en rad faktorer – men ytterst handlar det om den enskilda drabbade organisationens förmåga att förebygga, motstå och hantera allvarliga störningar, och också förmågan i stort inom elförsörjningen och i samhället.

## 4.1 Beröringspunkter med andra hot- och trendanalyser

Hot- och risklandskapet inom elförsörjningen är föränderligt. De riskkällor som redogörs för i sammanställningen återspeglar det som är överblickbart eller tänkbart i nuläget. Det säkerhetspolitiska omvärldsläget påverkar hotbilden och den samhälls- och teknikutveckling som sker, både nationellt och internationellt, kan också innebära att nya hot, risker och sårbarheter kan uppstå. Riskbilden reflekterar därmed de utmaningar som finns i vår nutid, vilket aktörer inom elförsörjningen behöver förhålla sig till. Det är därför viktigt att relatera till föreliggande förutsättningar i vår omvärld – givet den djupa sammankoppling och integration vi har med våra grannländer – för att förstå den kontext som elförsörjningens aktörer verkar i.

Svenska kraftnäts omvärldsanalys sammanfattar de omvärldsfaktorer som påverkar energibranschen i allmänhet och Svenska kraftnäts verksamhet i synnerhet och som förväntas kvarstå under en längre tidshorisont.

Av de antagonistiska hoten lyfts cyberhotet i ett flertal trender, kopplat till förändrad hotbild, utmaningar på leverantörsmarknaden samt digitalisering och AI. Detta belyser det kritiska beroendet IT-infrastruktur som utgör grunden för kraftsystemets tekniska infrastruktur och därmed den samhällsviktiga verksamhetens leverans. Potentiella risker och hot kopplat till ovan nämnda områden beskrivs närmare i bilaga 1, se riskkällorna 2.5-2.9.

I Svenska kraftnäts öppna antagonistiska hotbild görs fördjupningar i den aktuella hotbilden inom elförsörjningen. I den senaste öppna hotbilden från våren 2024 konstaterar Svenska kraftnät att de största hoten mot svensk elförsörjning kommer från Ryssland, Kina och Iran. Den sammanfattande bedömning som gjordes 2021 avseende hotets karaktär bedöms vara fortsatt aktuell, dvs.:

”Det troligaste hotet från terrorister eller kriminella för elförsörjningen är skador som en konsekvens av angrepp riktade mot



ett annat närstående mål, antingen fysiskt/geografiskt eller i cyberrymden.”

Likaså bedömningen avseende de potentiella målen inom elförsörjningen anses fortsatt vara aktuell, enligt vilken:

”Mål inom elförsörjningen för ett antagonistiskt angrepp kan vara infrastruktur, IT-system, information (uppgifter) och personal. Infrastruktur kan angripas fysiskt eller via IT-system, t.ex. med en cyberattack.”

Säkerhetspolisen nämner i sin årsbok för 2023-2024 att energiförsörjningen är ett av Rysslands målval när det gäller inhämtning av information avseende Sveriges försvars- och totalförsvarsuppbyggnad. Svenska kraftnät har identifierat cyberhot, fysisk skadegörelse och sabotage, informationsinsamling, uppköp av fastigheter och mark, utkontraktering och leverantörskedjor samt gråzonsproblematik och väpnat angrepp som de främsta antagonistiska hoten gentemot svensk elförsörjning.

Avseende de aktuella cyberhoten har en ökning av cyberattacker globalt mot energisektorn och kritisk infrastruktur noterats under 2023. Phishing och den mänskliga faktorn är fortsatt den vanligaste attackvektorn som en angripare utnyttjar. Utvecklingen av AI innebär både möjligheter och utmaningar som bedöms bli alltmer framträdande under 2024. Ransomware och överbelastningsattacker har pekats ut som ett cyberhot som ökat de senaste åren, elsektorn inkluderat, och det ser ut att kvarstå. Även trenden att exploatera sårbarheter i leverantörskedjan bedöms bestå (jfr även riskkälla 1.5 i bilaga 1).

Vad gäller metoder för antagonistiska angrepp och krigföring kan bland annat följande utveckling noteras i vårt närområde, vars effekter även kan återspeglas i den aktuella hotbilden inom elförsörjningen. I Ukraina har Ryssland använt sig av så kallade Shahed-drönare för att attackera civila mål, bland annat anläggningar inom Ukrainas kraftsystem. Den tekniska utvecklingen av drönare i krigsföring utvecklas snabbt i kriget i Ukraina, likaså motmedel anpassas och utvecklas mot det hot som drönarna utgör.

## 4.2 Förändringar i den övergripande riskbilden inom elförsörjningen

Bedömningar från 2022 års riskanalyser kvarstår till stor del och det har inte skett större förändringar i den övergripande riskbilden inom elförsörjningen. Det som dock kan noteras sedan föregående rapportering (år 2022) kan sammanfattas enligt följande:

- > Det säkerhetspolitiska läget i Sveriges närområde har försämrats ytterligare. Under 2023 har flera incidenter i Östersjöområdet noterats, däribland gasledningarna NordStream och Balticconnector, samt undervatten telekommunikationskablar. Dessa incidenter understryker både säkerhets- och beredskapsaspekter; utökad övervakning av samhällskritisk infrastruktur men även förstärkt redundans och robusthet. Detta är också en gränsöverskridande fråga, då infrastrukturen i vissa fall kan samägas av olika länder, och vara belägen på internationellt vatten – i sammanhanget kan även havsbaserad vindkraft noteras. Den övergripande problematiken inom elförsörjningen beskrivs i riskkällan ”*Skador på samhällsviktig infrastruktur*” (se riskkälla 1.11 i bilaga 1). För energiförsörjningen i stort kan incidenter på förbindelser mellan två länder få en påverkan på europeisk energiförsörjning.
- > De baltiska länderna (Estland, Lettland och Litauen) är för närvarande tekniskt integrerade med det rysk- belarusiska elnätet (BRELL), även om länderna under 2023 har stoppat handeln med kommersiell el. Marknadsmässigt har de baltiska länderna sedan 2010-2013 deltagit på elmarknaden på Nordpool. Frikoppling från det ryska elnätet och synkronisering mot det europeiska elnätet är planerad till år 2025. En plötslig, forcerad frikoppling är en potentiell risk, vilket även kan få en geopolitisk dimension i det alltmer försämrade säkerhetsläget i vårt närområde.
- > Digitalisering och användning av automatiserade lösningar ökar inom elförsörjningen i syfte att kunna övervaka, styra och balansera ett effektivt, tillförlitligt och driftsäkert kraftsystem (jfr även riskkälla 1.16 ”*Begränsningar i viktiga förmågor och resurser att hantera olika systemdrifttillstånd*”).

Artificiell intelligens (AI) har på senare tid blivit alltmer nödvändigt för att hantera ett mer svårplanerat, distribuerat och volatilt kraftsystem med minskad systemstabilitet. Fördelar med AI är bl.a. att bättre kunna optimera användning av kraftsystemet ur ett driftsäkerhets- och ekonomiskt effektivitetsperspektiv (t.ex. genom mer exakta prognoser för elproduktion och -förbrukning).

AI kan även bidra till att förutspå framtida behov av nätkapacitet och -förstärkningar samt prognosticera effekttillräcklighet. Utöver drift av kraftsystemet kan AI nyttjas inom IT, för att t.ex. upptäcka säkerhetsbrister, men också för att få hjälp med felsökningar mm.

För att minimera eventuella risker med AI är det av yttersta vikt att använda tekniken ansvarsfullt och förstå vilka risker som verksamheten tar

genom användande av AI. Fortsatt integrering av AI i några av kraftsystemets mest kritiska processer innebär ett beroende av en självlärande teknik.

Vad gäller cyberrelaterade hot finns potentiell risk för att en antagonist manipulerar data och algoritmer som används av AI. Ett potentiellt hot är också att AI och maskininlärning (ML) används i cyberattacker, vilket gör attackerna mer sofistikerade och anpassningsbara.

## 4.3 Om fördjupningsområden i årets arbete

Inom ramen för arbetet med 2024 års risk- och sårbarhetsanalys har Svenska kraftnät valt att fördjupa sig i ett antal områden, som tar avstamp i viktiga förmågor inom elförsörjningen.

### 4.3.1 Fördjupningsområde: förmåga till att återuppbygga kraftsystemet efter inträffat nätsammanbrott

Vid ett inträffat nätsammanbrott behöver delar eller hela transmissionsnätet återuppbyggas. Återuppbyggnad av hela kraftsystemet kommer att omfatta alla spänningsnivåer men utgår från att transmissionsnätet spänningssätts stegvis enligt en framtagna plan, och möjliggör för att underliggande nät succesivt kan spänningssättas och att produktionsanläggningar kan anslutas. Anslutning av förbrukning och uppreglering av produktion sker sedan stegvis baserat på driftläget.

Kommissionens förordning om nödsituationer och återuppbyggnad avseende elektricitet (ER) fastställer att varje systemansvarig för överföringssystem (TSO) ska ha en återuppbyggnadsplan och identifierar också ett antal tekniska och organisatoriska åtgärder som ska ingå i återuppbyggnadsplanen. Återuppbyggnadsplanen syftar i första hand till att återställa driften av transmissionsnätet och på det sättet möjliggöra för anslutning av förbrukning och produktion. Svenska kraftnät arbetar också i sin roll som elberedskapsmyndighet med att säkerställa förmåga till lokala eller regionala ö-drifter för att försörja samhällsviktig verksamhet om transmissionsnätet av någon anledning inte är tillgängligt eller om återuppbyggnaden av transmissionsnätet tar lång tid.

En annan viktig del av ER är att säkerställa robusthet i verktyg och anläggningar som behövs för genomförandet av återuppbyggnadsplanen. ER ger även Svenska kraftnät möjlighet att kravställa robusthet i viktiga anläggningar på lägre spänningsnivåer.

Svenska kraftnät bedömer att det finns en god förmåga att hantera nätsammanbrott och återuppbyggnad. Denna bedömning utgår från en

fredstida krissituation, eventuella förändringar i hotbilden och situationer med höjd beredskap kan komma att påverka bedömningen. Svenska kraftnät har under 2023 fortsatt arbetet med att förstärka förmågan till nätåteruppbyggnad inom elförsörjningen utifrån både tekniska och organisatoriska aspekter - som även återspeglar utformningen av det framtida kraftsystemet. Samverkan med aktörer inom elförsörjningen är en viktig del i det förmågehöjande arbetet.

#### **4.3.2 Fördjupningsområde: förmåga att upprätthålla lokal reservkraft (inkl. drivmedelsförsörjning)**

En genomlysning av såväl Svenska kraftnät som ett urval av elföretags förmåga till att upprätthålla drivmedelsförsörjning avseende lokal reservkraft genomfördes inom ramen för 2016 års risk- och sårbarhetsanalys. Fokus låg på att utreda hur länge som aktörer inom elförsörjningen kan upprätthålla den mest kritiska verksamheten vid störningar i elförsörjningen, då lokal reservkraft behövs. Under 2023 genomfördes en uppföljning av förmågan inom elförsörjningen. Den sammanfattande bedömningen är att aktörers egna reserver ofta är dimensionerade för att räcka i ett begränsat antal dygn.

Svenska kraftnät vidhåller därför att det är viktigt att den myndighetsgemensamma och sektorsövergripande planeringen med avseende på prioritering och distribution av 90-dagars beredskapslager intensifieras och konkretiseras, då det inte torde vara ekonomiskt försvarbart, och inte heller praktiskt genomförbart, att enskilda aktörer innehar omfattande, egna reserver av drivmedel. Detta bör beaktas i förhållande till totalförsvarets krav på att under minst tre månader kunna hantera en säkerhetspolitisk kris som innebär allvarliga störningar i samhällets funktionalitet (vilket är den dimensionering av förmågan som risk- och sårbarhetsanalysen närmast kan förhålla sig till, i avsaknad av en myndighetsgemensam dimensionering för fredstida kriser).

Viktigt att notera i sammanhanget är att det endast finns ett fåtal privatägda oljeraffinaderier kvar i landet. Sveriges strategiska drivmedelsreserv är även den privatägd.

En ytterligare dimension utgörs av samhällets övergång från fossila bränslen till mer miljövänliga alternativ – vilket behöver tas i beaktande vid det myndighetsgemensamma planeringsarbetet. Dock behöver tillgången till fossila bränslen säkerställas under eventuell övergång till mer miljövänliga drivmedel till lokal reservkraft.

#### **4.3.3 Fördjupningsområde: beroende av GNSS inom elförsörjningen**

Inom elförsörjningen finns ett beroende av GNSS-baserade tjänster för tid- och takthållning, som är viktigt för observerbarhet och styrbarhet av kraftsystemet

samt för sådana komponenter och funktioner som är beroende av korrekta tidsangivelser. GNSS-baserade tjänster behövs även i viss utsträckning för navigering och positionering vid installation, underhåll och felavhjälpning inom elförsörjningen.

Potentiella orsaker till störningar i satellitbaserade tjänster kan härledas till både antagonistiska och icke- antagonistiska orsaker; exempelvis avsiktliga störningar mot satelliter i rymden ("rymdkrig"), solstormar och andra elektromagnetiska störningar men även rymdskrot som kan skada satelliter i omloppsbanan. Signaler från satelliter kan också störas ut genom störningssändare (som är relativt lättillgängliga att köpa t.ex. på Internet), sk. jamming.

Försvarsberedningen noterar i sin senaste rapport att exempelvis Ryssland och Kina "utvecklar och använder olika former av antagonistiskt agerande i rymden". Amerikanska teknikföretaget Cisco Systems har observerat att Ryssland har använt gps-jamming för att störa ukrainska transmissionsnätstationer för el under det pågående kriget. I slutet av 2023 noterades även ökade GPS-störningar över Östersjön.

Svenska kraftnät har under 2023 genomfört en översiktlig analys av beroendet av GNSS-baserade tjänster inom transmissionsnätet och den sammanfattande slutsatsen är att beroendet av exakt och mer noggrann tid kommer att öka i framtida kraftsystemlösningar.

## 5 Övergripande förmågebedömning för elförsörjningen

Inom ramen för 2022 års risk- och sårbarhetsanalys genomfördes en övergripande förmågebedömning inom elförsörjningen. Bedömningen från 2022 kvarstår, dvs. att det finns en förmåga inom elförsörjningen att förebygga, motstå och hantera sådana utmaningar som identifierats inom ramen för de beskrivna riskkällorna. Inträffade händelser de senare åren (exempelvis coronapandemin) och den säkerhetspolitiska utvecklingen i världen (där kriget i Ukraina samt Houthi-rebellernas attacker på fraktfartyg i Röda havet är två aktuella exempel) har aktualiserat risker med bortfall av kritisk personal, störningar i kritiska leveranskedjor, cyberangrepp och därigenom även möjlig påverkan på viktig infrastruktur inom elförsörjningen.

En ytterligare aspekt kopplad till leveranser av kritisk materiel handlar om en ansträngd leverantörsmarknad; att globala och lokala leverantörer som förser elmarknaden har utmaningar att öka kapaciteten i samma takt som behoven för kritiska material och resurser uppstår.

Den generella bedömningen är att elförsörjningens aktörer medvetet arbetar med att säkerställa den egna organisationens förmåga utifrån potentiella risker som ovan nämnda händelser kan medföra; exempelvis att säkerställa kritiska funktioner och leveranser genom kontinuitetsplanering och genomlysning av för organisationen viktiga leveranskedjor och outsourcade funktioner (även internationellt). Även vikten av en säker IT-infrastruktur och att tidigt kunna detektera potentiella cyberangrepp är fortsatt aktuellt, likaså adekvat fysiskt skydd av viktiga anläggningar.

Vidare bedöms det finnas en förståelse inom elförsörjningen om vad som är en acceptabel nivå för den enskilda organisationen, utifrån lagstadgade krav, och för att säkerställa den egna verksamhetens mest kritiska leveranser, även vid krissituationer.

Däremot kan det på den nationella nivån identifieras ett potentiellt gap mellan att enskilda organisationer uppfyller lagstadgade kraven på den egna verksamheten och samhällets behov av en fungerande elförsörjning även vid krissituationer. I detta sammanhang är det värt att notera att elföretag bedriver vinstdrivande verksamhet utifrån den lagstiftning som gäller för sådana aktörer och agerar utifrån dessa ramar. Robusthets- och säkerhetshöjande åtgärder – och även för att vidmakthålla befintliga resurser – kan vara kostnadsdrivande för enskilda verksamheter.

För elförsörjningens aktörer gäller vissa skyldigheter enligt elberedskapslagen. Den lagen ger dock inte utrymme för en generell dimensionering av krisberedskapsförmågan inom elförsörjningen. Därtill omfattas aktörer inom elförsörjningen om lag (1982:1004) om skyldighet för näringsidkare, arbetsmarknadsorganisationer m.fl. att delta i totalförsvarsplaneringen.

# Bilaga 1 – De övergripande riskkällorna

Nedan redovisas de övergripande riskkällorna utan inbördes rangordning.

Urvalet av riskkällor baseras inte på statistik över inträffade händelser eftersom ambitionen är att få en övergripande bild av det aktuella risklandskapet, och att även inkludera risker, hot och sårbarheter som inträffar sällan.

Allriskperspektivet genomsyrar riskidentifieringen, dvs. den innehåller olika typer av tänkbara riskkällor, både av antagonistisk och också icke-antagonistisk härkomst. Även risker och hot kopplat till höjd beredskap och krig beaktas.

Riskbilden inte är bunden till en viss aktör inom elförsörjningen och alla aktörer är inte heller direkt berörda av alla riskkällor. Vissa riskkällor och utmaningar berör mest den nationella – överliggande – nivån, medan andra kan drabba elaktörer på lägre distributionsnivåer, alternativt produktion eller handel av el. Däremot reflekterar riskbilden det ömsesidiga beroendet mellan överliggande och underliggande nät, elproduktion och -förbrukning samt elmarknad.

## **1.1 Fortsatt integrering av det nationella elsystemet: ökad internationalisering**

Ökad internationalisering – dvs. att de europeiska (inkl. nordiska) elsystemen

### Exempel på åtgärder:

- > Beakta aktuell hotbild, även för europeisk elförsörjning, i den egna verksamhetens säkerhetsarbete.
- > Beakta även andra omvärldsfaktorer, till exempel sådana som kan påverka effektillgången inom det nordiska synkronområdet.

integreras allt mer – följer utvecklingen mot en gemensam europeisk elmarknad med ökad regional samordning och styrning.

*Potentiella konsekvenser:* en välfungerande elmarknad är en förutsättning för att upprätthålla samhällsviktig funktionalitet. En ökad internationalisering och integrering av de nationella elsystemen bidrar därmed till redundansen i systemet.

Emellertid innebär en ökad marknadsintegrering att det blir

svårare att säkerställa sådana nationella lösningar som enbart är avsedda för att hantera olika typer av driftsituationer inom den inhemska elförsörjningen. Exempelvis behöver medlemsstater i EU följa EU:s elmarknadsförordning för att få

införa en kapacitetsmekanism (strategisk reserv) – vilket syftar till att inte sneddriva konkurrensen på elmarknaden.

Vidare kan en ökad sammankoppling av olika nationella elsystem medföra att flera länder påverkas av en händelse som har sitt ursprung i ett enskilt land/en enskild region. Detta kan även röra sig om situationer där ett ansträngt försörjningsläge påverkar ett flertal länder samtidigt.

För att uppfylla den europeiska lagstiftningens krav och fullgöra de europeiska samarbetsavtalen utbyts driftrelaterade data om det svenska kraftsystemet bl.a. med ENTSO-e. Inom ramen för samarbetet med andra europeiska systemoperatörer kan även information om eventuella incidenter delas, i syfte att stärka säkerheten på den gemensamma elmarknaden.

Ur ett riskperspektiv bör hotet om underrättelseinhämtning beaktas i en kontext där stora mängder viktiga data samlas in och sammanställs på en europeisk nivå, även över tid. I sammanhanget kan noteras att Kina redan idag har delägarskap i flera nationella transmissionsoperatörer i Europa, vilka ingår i ENSTO-e, och har visat intresse för fler.

### **1.2 Fortsatt integrering av det nationella elsystemet: fortsatt decentralisering av det nationella elsystemet**

Utvecklingen mot ett mer decentraliserat nationellt elsystem - vilket är viktigt

#### Exempel på åtgärder:

- Hantera problematiken med avveckling av större produktionsanläggningar på den nationella nivån.
- Beakta eventuell risk för exponering av lokala system och enheter för intrång.

för att klara av energiomställningen - genom en mer distribuerad produktion och lagerhållning gör kunderna till mer aktiva aktörer i systemet. Kraftsystemet blir därmed mer komplext med en stor mängd produkter, tjänster, marknadslösningar och aktörer som behöver samverka.

*Potentiella konsekvenser:* fler system och enheter ska kunna fjärrstyras eller fjärravläsas, vilket gör att de kan exponeras för intrång då de kopplas upp mot internet. Flera utplacerade mätenheter kan också innebära ökad fysisk sårbarhet lokalt.

Vidare kan en omfattande decentralisering medföra att större produktionsanläggningar blir olönsamma och avvecklas. Om detta sker under en relativt kort tidsrymd och utan att förmågan ersätts, kan konsekvenser uppstå då sådana anläggningar är grundläggande för driften av elsystemet med



avseende på stabilitet och spänningshållning (jfr riskkälla: ”1.15 Otilräcklig kapacitet avseende både nätkapacitet och effekt”).

### **1.3 Optimering av kritisk verksamhet inom elförsörjningen: minskad redundans avseende kritiska funktioner**

Teknikutvecklingen och digitaliseringen medför ökad automatisering av arbetsuppgifter, vilket ställer krav på ny kompetens. Samtidigt riskerar kunskapen om viktiga system - både avseende IT och tekniska system - att

minska hos (drift) personalen när automatiserade lösningar/AI ersätter ordinarie personal.

Utvecklingen under de senaste årtiondena har dessutom medfört en generell trend att redundans avseende kritiska funktioner minskar, t.ex. inom underhållsverksamheten.

I samband med ny- och ombyggnationer av elanläggningar avlägsnas ofta funktioner för lokal styrförmåga av aggregat. I allt högre utsträckning förlitar sig aktörer inom elförsörjningen på att kunna fjärrstyra anläggningar från en driftcentral. Det innebär en ökad sårbarhet för störningar

#### Exempel på åtgärder:

- > Genom kontinuitetshantering: säkerställ rätt dimensionerad bemanning i de kritiska funktionerna, även utifrån situationer som kan innebära svåra påfrestningar.
- > Säkerställ rätt kompetens och kunskap, även om de äldre, manuella driftsystemen (gäller även dokumentation om manuell drift för att säkerställa kompetensöverföring från de som har kunskapen).
- > Överväg huruvida olika digitaliserings-, fjärrstyrnings- och automatiseringsinitiativ alltid är lämpliga ur en säkerhets- och robusthetssynpunkt.

i den centrala styrningen, som exempelvis fel i IT-nätet. Den pågående teknikutvecklingen och vissa marknadskrav innebär även att ännu fler funktioner som fjärrstyrs centralt för kraftsystemet kan och kommer att automatiseras ytterligare.

*Potentiella konsekvenser:* den dagliga användningen av digitala hjälpsystem och en samtidig kompetensförlust via pensionsavgångar av dem som kan de robusta, manuella hjälpsystemen, ökar risken för störningar i verksamheten om de automatiserade lösningarna slutar fungera och behöver ersättas av manuell hantering.

Detta medför i sin tur svårigheter att kunna felavhjälpa och reparera. En sådan situation kan bli mycket allvarlig vid omfattande störningar, inte minst om verksamheten är kritiskt beroende av externa leverantörer och entreprenörer för manuell hantering, då externa resurser inte nödvändigtvis är tillgängliga i samma omfattning som under normala förhållanden.

Vid omfattande störningar kan nedskärningar i personalgrupper också medföra svårigheter kring långvarig bemanning av elanläggningar.

#### ***1.4 Optimering av kritisk verksamhet inom elförsörjningen: outsourcing av kritiska verksamheter***

Med outsourcing (utkontraktering) avses att externa utförare anlitas för att tillhandahålla produkter eller tjänster inom den egna organisationen – även avseende samhällsviktig infrastruktur såsom komponenter, anläggningsdelar etc.

Orsaker till outsourcing handlar om att effektivisera och optimera den egna verksamheten, eller att den egna verksamheten inte besitter all den specialistkompetens som kan behövas för att utföra arbetet.

*Potentiella konsekvenser:* om verksamhetsutövaren inte vidtagit förebyggande åtgärder för att säkerställa en robust förmåga när externa utförare anlitas, kan detta medföra allvarliga brister i verksamhetskritiska leveranser (vid ev. brister eller oförmåga hos extern utförare att leverera enligt uppdrag på en fullgod nivå).

Omfattande störningar kan påverka externa utförares förmåga att tillgodose verksamhetskritiska leveranser till beställaren.

Exempelvis kan en pandemi eller motsvarande händelseutveckling innebära stängda landsgränser, vilket kan påverka kritiska varu- och tjänsteflöden och tillgång till utländska tekniker och experter vid underhåll och felavhjälpling.

### Exempel på åtgärder:

Analysera och ta ställning till huruvida utkontraktering är lämpligt ur säkerhets- och beredskapsperspektiv, bland annat genom att:

- > Fastställa acceptabla avbrottstider för kritiska leveranser.
- > Göra en riskbedömning utifrån leveransens tidskritiskhet avseende geografiskt avstånd till leverantören samt geo- och säkerhetspolitiska aspekter vid utkontraktering utomlands.
- > Överväga "second source supplier" för verksamhetskritiska processer/tjänster.

Vid anlitande av eventuella underleverantörer bör huvudleverantören göra motsvarande riskanalyser på underleverantörens förmåga.

### **1.5 Optimering av kritisk verksamhet inom elförsörjningen: bristande säkerhet i IT-leverantörskedjor**

Kan härledas till:

- > Bristfällig kravställning avseende säkerhet (security) vad gäller hantering av kritisk utrustning (fysisk- eller mjukvara) hos leverantörer, även sådana som är baserade utomlands.
- > Snabba och kostnadseffektiva processer har företräde – ”supply chain security” riskerar att prioriteras ned.
- > Bristfällig förmåga och strategier gällande hur assurans i hårdvaror och mjukvaror kan verifieras.

Utkontraktering av IT eller användning av molntjänster innebär ofta att leverantören placerar olika kunders system och information i samma fysiska datorsystem. Syftet med molntjänster kan vara att öka redundansen i verksamhetens informationslagring, och därmed bidra till ökad säkerhet i verksamhetsnära lösningar.

Användandet av molntjänster kan dock medföra en ökad risk eftersom en störning i en kunds system kan orsaka störningar eller avbrott hos flera andra kunders system. Hamnar en stor mängd skyddsvärd information hos en enskild leverantör riskerar denne dessutom att bli ett attraktivt mål för bland annat andra länders underrättelseinhämtning.

Ur ett säkerhetsperspektiv kan det också vara en utmaning att kontrollera alla leverantörsled avseende sådana IT-tjänster som upphandlas centralt för t.ex. alla transmissionsnätägare på EU-nivå.

Detta gäller även ledningsstrukturer och ägarförhållanden hos berörda underleverantörer som verkar på en global marknad.

Utkontraktering eller användning av molntjänster kan också innebära att risken för cyberspionage ökar. Till exempel försvåras möjligheterna att säkerställa fullgod informationssäkerhet i alla led.

*Potentiella konsekvenser:* en antagonistisk angripare kan hitta ett insteg i en svagt skyddad leverantörskedja. Ju längre leverantörskedja, desto fler potentiella angreppspunkter finns för angriparen. En antagonist kan också, i syfte att komma åt verksamheten, bli en leverantör av kritisk utrustning eller tjänster (jfr även riskkälla: ”1.10 Spionage och olovlig underrättelseinhämtning”).

#### Exempel på åtgärder:

- > Öka säkerhetskraven när det gäller leverantörskedjor av mjukvara och hårdvara.
- > Gör en noggrann avdömning av vilka leverantörer som kan vara lämpliga att anlita samt en bedömning av hur tillgång till kritiska IT-miljöer möjliggörs.
- > Längs med leverantörskedjan – minska möjligheten att identifiera vad en viss utrustning ska användas till och var (exempelvis i en förförsörjningen kritisk verksamhet eller anläggning).

### **1.6 Optimering av kritisk verksamhet inom elförsörjningen: bristfälliga upphandlingar avseende säkra tjänster och produkter inom IT/OT**

Det finns ett flertal faktorer som kan leda till bristfälliga upphandlingar inom IT/OT (operativ teknik)- området, exempelvis:

- > Bristande rutiner vid upphandling.
- > Avsaknad av medveten avvägning mellan funktionalitet och säkerhet.
- > Pressade projekt som skall leverera per visst datum.

- > Lågt fokus på säkerhet i kravställning.

*Potentiella konsekvenser:* att elförsörjningens aktörer upphandlar och installerar undermålig mjukvara med säkerhetsbrister redan från början som sedan kommer att fortleva under relativt lång tid.

Exempel på åtgärder:

- > Öka kompetensen vad gäller kravställning m.a.p. säkerhet i upphandlande projekt.
- > Öka kompetensen vad gäller avtalsskrivning så att leverantörer implementerar en godtagbar säkerhetsnivå.
- > Ställ såväl specifika som allmänna krav på leverantörer och hårdvara vad gäller säkerhet.
- > Tydliggör och öka kraven och kontrollerna vad gäller leveransgodkännanden.
- > Genomför inte upphandlingar under orimlig tidspress.

### **1.7 Cyberrisker och – hot: en allt starkare integration mellan IT och OT**

En allt starkare integration mellan IT och OT inom elförsörjningen drivs av behovet av att utbyta data för att övervaka, styra och balansera ett effektivt, tillförlitligt och driftsäkert kraftsystem med hjälp av algoritmer och IT-stöd.

Det finns ett flertal bakomliggande faktorer, exempelvis:

- > Förändrad produktionsmix och förbrukningsmönster kommer att ställa krav på ny typ av IT-stöd för att hantera komplexiteten i det framtida kraftsystemet.
- > Utvecklingen mot en realtidsmarknad som innebär allt snabbare informationsutbyte inom elsektorn.
- > En önskan att optimera elförsörjningen av marknadsskäl (och till gagn för kunderna).
- > Krav på EU-anpassning och EU-samverkan, vilket kommer att innebära krav på ökad integration med nya aktörer på elmarknaden.

*Potentiella konsekvenser:* ett större antal integrationer och utbyten mellan OT och andra miljöer ökar angreppsytan mot OT-miljön för en antagonistisk angripare. En angripare kan också utnyttja en tät sammankoppling mellan datalager och OT-miljö genom att förutspå hur automatiserade processer och algoritmer fungerar i syfte att kunna störa dem.

Risken för stora konsekvenser som ett resultat av driftproblem eller misstag i mer perifera IT-system kan komma att påverka den operativa driften. Ett angrepp som utgår från internet och får fotfäste i exempelvis kontors-IT-miljön kan sprida sig till för elförsörjningen mer kritiska miljöer och system.

Antagonistens mål kan vara att hindra åtkomst till alternativt skapa oreda eller skada i viktiga IT-system (olovlig manövrering, informationsbortfall) och därigenom orsaka en allvarlig skada för verksamheten.

Målet kan även vara ekonomiskt riktat vilket gör att utpressning kan förekomma.

#### Exempel på åtgärder:

- > Utveckla IT-lösningar som klarar störningar och bortfall av kritiska resurser, planera för alternativa lösningar och genomför beredskapsövningar.
- > Anskaffa och förvalta reservsystem för att hantera kritiska funktioner samt planera för och utbilda IT-driften att hantera situationer där beslutsstödet kan vara bristfälligt.
- > Skapa kompetens om hur dataflöden kan integreras på ett säkert sätt.
- > Minimera utbyten gentemot de kritiska delarna av OT/SCADA-miljöerna som är av yttersta vikt för elförsörjningen.
- > Kontinuerligt granska och testa de integrationer som är nödvändiga.
- > Skapa möjligheter att övervaka automatiska processer och utbyten av data så att eventuell manipulation eller felaktigheter upptäcks.
- > Formulera strategier/principer för hur integrationer mellan IT och OT utformas och hanteras. Visualisera vilka beroenden som finns och vad som inte kan eller bör integreras.

### **1.8 Cyberrisker och – hot: ökad komplexitet i IT-system och IT-tjänster**

Elförsörjningens aktörer anammar teknologier och tjänster, ibland till exempel molnbaserade, som man inte alltid har kompetens eller möjlighet att överblicka fullt ut. Ökad komplexitet i IT-system och IT-tjänster som understöder elförsörjningens operativa verksamhet på olika sätt kan skapa angreppsytor men också beroenden som man inte är medveten om förrän något händer. Dessa utmaningar kan förvärras vid eventuell underbemanning inom viktiga funktioner och/eller kompetensbrist.

Komplexiteten i IT-system och IT-tjänster bedöms öka i takt med teknologikutvecklingen i allmänhet: men också i kombination med kommande utmaningar som elförsörjningen behöver lösa (jfr riskkälla ”1.7 En allt starkare integration mellan IT och OT”).

*Potentiella konsekvenser:* misstag, förbiseenden eller angrepp av tredje part kan störa elförsörjningen. Verksamheten saknar full rådighet över resurser man är beroende av.

#### Exempel på åtgärder:

- > Säkerställ förmågan att granska mjuk- och hårdvara. Att skapa en gemensam bild av utmaningarna inom elförsörjningen och beakta möjliga beroenden och risker i samråd med övriga viktiga aktörer.

### **1.9 Cyberrisker och – hot: bristfälligt säkerhetsskydd avseende IT-miljöer (främst OT)**

Brister i säkerhetsskyddet kan ge angripare åtkomst till miljöer (främst OT) som har ett undermåligt skydd.

Exempel på potentiella orsaker till bristfälligt skydd (som kan förekomma i varierande grad):

- > Bristande säkerhetsmedvetenhet avseende aktuella hot och risker avseende IT-säkerhet.
- > Svagt skalskydd på platser där kritisk IT-utrustning exponeras.
- > Dålig styrning och uppföljning avseende IT-säkerhet.

*Potentiella konsekvenser:* en antagonistisk angripare kan hitta ett insteg i en IT-miljö som bygger på att den är fysiskt skyddad men har ett underdimensionerat IT-skydd ur ett säkerhetsperspektiv. (Jfr även

riskkällorna: 1.13

*Överlappande och*

*divergerande*

*bestämmelser och*

*lagstadgade krav på*

*aktörer inom*

*elförsörjningen, 1.11*

*Omfattande skador på*

*samhällsviktig*

*infrastruktur).*

#### Exempel på åtgärder:

- > Säkerställ tillräckliga säkerhetskrav på elanläggningar eller andra platser där för elförsörjningen viktig IT-infrastruktur finns.

### **1.10 Spionage och olovlig underrättelseinhämtning**

Genom infiltrering i säkerhetskänslig verksamhet kan känslig information om en verksamhet samlas in, t.ex. genom insiders.

Underrättelseinhämtning kan också ske genom informationsinsamling från öppna källor, via affärskontakter eller sociala medier. Detta kan även ske i hela leverantörsledet. Ett annat hot är att avlyssningsutrustning placeras i kritiska

komponenter som används inom elförsörjningen. Detta kan exempelvis ske genom att en kvalificerad angripare planterar avancerad skadlig kod i hårdvara hos leverantörer som sedan köps in och används i samhällsviktiga IT-system, exempelvis i SCADA-system.

En annan variant är "strategiska uppköp", dvs. att en främmande makt, eller personer med kopplingar till en främmande makt, köper mark- eller sjöområden eller fastigheter nära till viktiga elanläggningar, kritiska kommunikationsnoder, eller broar och vägar i antagonistiskt syfte. Även utländskt deläggande i företag

eller strategiska investeringar (av utländska aktörer) i företag kan användas för att få insyn och möjlighet att påverka hur en verksamhet bedrivs.

#### Exempel på åtgärder:

- > Arbeta systematiskt med säkerhetshöjande åtgärder utifrån aktuell hotbild och vidta säkerhetshöjande åtgärder. I detta ingår även aspekter kring upphandlingar och outsourcing ("utkontraktering").
- > Skapa medvetenhet om aktuell hotbild hos anställda och leverantörer.



*Potentiella konsekvenser:* skyddsvärd information kan tillgängliggöras för obehöriga. Detta kan innebära skada på den enskilda verksamheten (även ekonomiska skador) eller landets elförsörjning, men även på Sveriges säkerhet. Underrättelseverksamhet kan också bedrivas i ett förberedande syfte, dvs. som en förberedelse inför en krigssituation.

Genom att få obehörig åtkomst, kontroll eller insyn i samhällsviktig infrastruktur kan en antagonist, förutom att kunna avlyssna, avsiktligt försöka skada infrastrukturen.

### **1.11 Omfattande skador på samhällsviktig infrastruktur**

Med samhällsviktig infrastruktur syftas till viktiga elanläggningar och IT-system, samt andra tekniska system inom transmission, distribution, produktion och handel med el, nätinфраstruktur (inkl. utlandsförbindelser) samt den infrastruktur som möjliggör elektroniska kommunikationer (inkl. driftkommunikationer och kommunikationer för elhandel).

Omfattande skador kan härledas till olika orsaker. Förebyggande och riskmitigerande åtgärder kan delvis vara desamma, oavsett orsak. I vissa fall styr dock hotet och riskens karaktär vilka typ av åtgärder som bedöms mest effektfulla.

Skadorna delas upp i två kategorier: *extrema väderhändelser* och *antagonistiska angrepp*.

#### **Extrema väderhändelser**

Extremt väder som slår ut kritisk funktionalitet eller skadar den samhällsviktiga infrastrukturen inom elförsörjningen omfattar ett flertal yttre händelser, även geomagnetiska stormar.

Exempelvis kan det röra sig om:

- > kraftig åska
- > kraftiga vindar
- > kraftig nederbörd (vatten, snö, isstormar)
- > höga flöden som leder till översvämningar
- > extrem (långvarig) torka/värmebölja som även kan leda till skogsbränder
- > ras och skred (erosion)
- > laviner

- > vulkanutbrott (som sprider vulkanisk aska)
- > jordbävningar
- > tromber, orkaner
- > tsunamis
- > cykloner
- > rymdväder såsom solstormar som kan orsaka koronamassutkastning

Notera att extrema väderhändelser i de länder där viktiga leverantörer kan vara belägna, kan påverka för elförsörjningen kritiska varu- och tjänsteflöden. Detta kan i sin tur ha en negativ påverkan på den egna verksamheten i sådana fall där den egna verksamheten är kritiskt beroende av externa leverantörer.

*Potentiella konsekvenser:*

- > En mycket hög temperatur som håller i sig under flera dagar eller veckor, kan leda till att överföringsförmågan på ledningar påverkas.
- > En förhöjd temperatur på det kylvatten som är nödvändigt för att kyla vissa produktionskällor (till exempel inom kärnkraften) kan försämra möjligheten att producera efterfrågad effekt.
- > Perioder med långvarig värme kan också leda till brist på fjärrkyla av serverhallar.
- > Vid stora regnmängder kan vattenflöden orsaka markförskjutningar och kollaps av större vattenkraftstationer/dammanläggningar.
- > Vid kraftig vind kan ledningsmaterial som stolpar och isolatorer skadas på flera viktiga överföringsförbindelser, vilket kan det orsaka överföringsproblem.
- > Geomagnetiska stormar kan även medföra skador på navigeringssystem, satellitkommunikation (och därigenom påverka tid och takt, IT-system mm.).

Extremt väder, inklusive rymdväder, tar inte hänsyn till nationella gränser. Detta kan i vissa fall innebära att större regioner drabbas samtidigt (t.ex. inom synkronområdet), vilket även kan leda till minskad import/export.

Klimatförändringar kan innebära mer och fler extrema väderrelaterade fenomen på sikt och kan därigenom komma att medföra risk för störningar i elförsörjningen i framtiden. Exempelvis kan långvariga värmeböljor ha

påverkan på vattenkraften eller vindkraften och därigenom leda till produktionsbortfall.

### **Antagonistiska angrepp, stora olyckor och tekniska fel**

Skador kan orsakas genom avsiktliga attentat (fysisk skadegörelse, sabotage, cyberangrepp, även krigshandlingar) mot samhällsviktig infrastruktur inom elförsörjningen. Metoder och omfattningen kan variera, även beroende på hur resursstark angriparen är och vilka mål som angriparen har (se även Svenska kraftnäts öppna antagonistiska hotbild).

Skador på viktig infrastruktur kan även orsakas av stora olyckor, t.ex. dammhaverier, bränder, eller omfattande utsläpp av farliga ämnen som kan hota närliggande elanläggningar. Sådana olyckor kan även inträffa i andra samhällsviktiga sektorer, t.ex. inom transportsektorn.

En potentiell orsak till skador och haverier är också tekniska fel, dvs. att flera olika fel i elnätet skapar problem ungefär samtidigt. Ibland leder ett problem till ett annat och det sker mycket snabbt. Den tekniska utrustningen kan ha svårigheter att detektera var felet har uppstått och orsaken till felet (exempelvis dolda fel såsom felprogrammering). Det kan även vara så att den tekniska utrustningen har en felaktig inställning som orsakat en obefogad fränkoppling. (Jfr Energimyndigheten. 2020. *Nationell riskberedskapsplan för Sveriges elförsörjning*).

*Potentiella konsekvenser:* om skadorna medför att funktionaliteten i den tekniska infrastrukturen inom elförsörjningen inte snabbt går att återställa kan detta leda till allvarliga konsekvenser. Skador kan också uppstå inom sådana sektorer som elförsörjningen är beroende av, t.ex. inom telesektorn.

Omfattande utsläpp av farliga ämnen kan innebära långvarig sanering, och därmed påverka framkomligheten till elanläggningar om dessa ligger i det drabbade området.

Även eventuella brister i dimensionering av reparationsberedskapen -inklusive materiella och personella resurser- kan påverka reparations- och återställningstiden och därmed förlänga hantering av händelsen. Framkomligheten omfattande väg-, och järnvägsburna samt sjö- och lufttransporter är en viktig, tidsättande faktor vid reparationsinsatser.

### Exempel på åtgärder:

I den utsträckning det är möjligt både tekniskt och ekonomiskt:

- > Säkerställ den tekniska infrastrukturen och systemdesignens skydd och robusthet utifrån olika typer av potentiella extrema väderhändelser.
- > Säkerställ det fysiska skyddet utifrån möjliga scenarier där tillvägagångssätt för potentiella antagonistiska angrepp kan variera, men även utifrån storskaliga olyckor och haverier.
- > Säkerställ tillgång till rätt underlag t.ex. kartunderlag, rutiner och checklistor, hotanalyser, prognoser. I detta ingår även att ha framtagna nödfallsplaner bl.a. för att kunna omfördela resurser, förbereda system och prioritera matning av förbrukning.
- > Genomför regelbundna krisövningar.
- > Dimensionera reparationsberedskapen utifrån risker och hot. I sammanhanget bör även leverans- och inställelsetiden beaktas, likaså beroendet av ev. leverantörer.

### ***1.12 Omfattande, plötsligt personalbortfall i kritiska funktioner inom elförsörjningen***

Olika typer av orsaker kan leda till omfattande, plötsligt personalbortfall, om verksamheten inte har tillräcklig redundans i kritiska funktioner, exempelvis:

- > pandemier/epidemier
- > olyckor som drabbar personer i kritiska funktioner
- > terrorattentat
- > krigshandlingar
- > omfattande uppsägningar av kritisk personal vid arbetsvägran eller utbrett missnöje vid arbetsplatsen

*Potentiella konsekvenser:* oförmåga att resurssätta viktiga funktioner inom den drabbade organisationen och därigenom säkerställa en fungerande elförsörjning. Hur allvarliga konsekvenserna kan bli, beror bland annat av redundansen hos de kritiska funktionerna i förhållande till den inträffade

händelsen (jfr även riskkälla: ”1.3 *Minskad redundans avseende kritiska funktioner*”).

Exempel på åtgärder:

Säkerställ redundans hos de kritiska funktionerna bland annat genom:

- > Framtagna kontinuitets- och beredskapsplaner för den egna organisationen, även vid höjd beredskap (exempelvis krigsplacering av personal).
- > Utbildning, kompetensöverföring och övning.
- > Rätt dimensionerad bemanning av kritiska funktioner.
- > Beakta beroendet av leverantör och entreprenörer.

### **1.13 Överlappande och divergerande bestämmelser och lagstadgade krav på aktörer inom elförsörjningen**

Genom lagstiftning ställs en rad krav på elförsörjningens aktörer. Dessa utgår inte alltid från att säkerställa den samhällsviktiga funktionaliteten hos elförsörjningen, utan kraven kan, beroende på syfte, divergera.

En möjlig utmaning är att krav som ställs av miljöskäl kan motverka krav på en säker, robust och tillgänglig elförsörjning.

Exempelvis kan det innebära att vattenkraftanläggningar förändrar sitt driftmönster eller verksamhetsutövaren kommer i stället att ansöka om att avveckla sin verksamhet. Detta kan i förlängningen medföra en minskning av synkront ansluten planerbar elproduktion. Detta kan även få en påverkan på reglerings-, ö-drifts- och dödnätstartsformågan.

Det förekommer även prövningar där bland annat lokala miljökrav ställs gentemot nyetablering av elproduktion såsom vindkraft.

Ökande konkurrens om markområden, i kombination med höjda miljökrav - t.ex. vad gäller artskyddet – kan medföra omfattande utmaningar med att etablera nya ledningar. Därtill kan långdragna koncessionsprocesser för ledningar och kablar gör att det tar lång tid att genomföra förnyelse och förstärkande åtgärder i kraftsystemet.

Strängare nationella och europeiska miljökrav på äldre oljeeldade anläggningar medför att sådana anläggningar kan behöva läggas ner. Denna typ av anläggningar kan fylla en viktig funktion för t.ex. nationell effektillräcklighet vid ansträngda situationer men även för att upprätthålla lokal ö-driftsförmåga.

I viss utsträckning ställs högre säkerhetskrav i den svenska säkerhetsskyddslagstiftningen än i motsvarande lagstiftningar i andra länder. Detta innebär vissa utmaningar i det internationella samarbetet, till exempel vad gäller utlämnande av viss information kopplad till elförsörjningen.

*Potentiella konsekvenser:* den samhällsviktiga verksamheten inom elförsörjningen och dess funktionalitet kan inte alltid prioriteras vid avvägningar gentemot andra intressen som gör anspråk på samma markområden.

#### Exempel på åtgärder:

- > Uppmärksamma eventuella utmaningar, kopplade till lagefterlevnad gällande elförsörjningen, för ökad harmonisering av lagstadgade krav på den nationella nivån.

Det innebär att svåra avvägningar mellan olika krav och målsättningar behöver göras av elförsörjningens aktörer. Utan en samstämmighet i dessa avvägningar riskerar robustheten i elförsörjningen som helhet att försämrats.

Säkerhetsskyddslagstiftningens krav på internationella överenskommelser om

säkerhetsskydd kan innebära utmaningar i upphandlingsprocessen om viktiga leverantörer för elförsörjningen är belägna i sådana länder som för närvarande inte har bilaterala överenskommelser med Sverige.

### **1.14 Differentierad informationshantering inom elförsörjningen i stort**

Elförsörjningens aktörer kan i vissa fall göra olika tolkningar av gällande lagstiftning om vilken information som är känslig eller till och med säkerhetsskyddsklassificerad. Detta kan till exempel gälla sådan anläggningsinformation, driftdata och driftdokumentation som utbyts löpande mellan elaktörer, både nationellt men även internationellt.

Elförsörjningens aktörer agerar inte heller alltid inom samma lagrum (då elförsörjningen består av både myndigheter och företag, både nationella och

utländska företag och så vidare). Detta ökar risken för olika tolkningar och bedömningar som kan påverka informationssäkerheten inom elförsörjningen.

*Potentiella konsekvenser:* om information från olika verksamheter röjs till obehöriga kan detta få betydelse för Sveriges säkerhet. Om information klassificeras onödigt högt riskerar det resultera i en alltför tungrodd hantering av säkerhetskvalificerade uppgifter.

#### Exempel på åtgärder:

- > Det är viktigt att elförsörjningens aktörer har en kontinuerlig dialog kring och samsyn kring bedömningar av informationsresurser, i syfte att bidra till enhetlig informationshantering inom elförsörjningen i stort.

### **1.15 Otillräcklig kapacitet (avseende både nätkapacitet och effekt)**

Otillräcklig nätkapacitet kan bero på att nätstrukturen inte är tillräckligt utvecklad (utbyggd) eller tillräckligt robust för att möta utmaningar ur ett leveransperspektiv både idag men även i framtiden.

Kapacitetsproblem kan också bero på att det inte finns tillräckligt med effekt där behov uppstår. Det sistnämnda kan bero på kapacitetsbrister i nätet men även att den elproduktion som finns inte möter ökade krav från förbrukarsidan –m.a.o. att det inte finns tillräckligt med elproduktion. Problem kan också uppstå utifrån att nätstrukturen ursprungligen har utformats utifrån att viss (lokal) produktion fanns tillgänglig.

*Potentiella konsekvenser:* det ökande importberoendet särskilt i södra halvan av Sverige utmanar förmågan att upprätthålla elförsörjningen i händelse av ansträngda situationer, om importbegränsningar uppstår.

I sammanhanget bör det noteras att ökade utmaningar uppstår avseende stabilitet i kraftsystemet och överföringsförmåga när sådana generatorer som bidrar med betydande kraftsystemsstabilitet avvecklas i södra Sverige (jfr riskkälla "1.2 Fortsatt decentralisering av det nationella elsystemet"). Minskad mängd och andel av planerbar elproduktion minskar marginalerna avseende effektillgången i det svenska elsystemet, men även avseende viktiga stödtjänster som behövs för att stabilisera och balansera elnätet (vilket planerbar elproduktion historiskt bidragit med, jfr Energimyndigheten: *Nationell riskberedningsplan för Sveriges elförsörjning, 2021*).

#### Exempel på åtgärder:

- > Utbyggnad av nätstrukturen på ett sätt som tillgodoser även framtida behov av trygg elförsörjning.
- > Ökad flexibilitet i både elförbrukning och elproduktion.
- > Utvecklad teknik avseende energilagring som möjliggör leverans av framtida systemtjänster, exempelvis vätgas och batterier.
- > Fler systemstabiliserande stödtjänster.
- > Upprätthåll resurser för planerbar elproduktion.

#### **1.16 Begränsningar i viktiga förmågor och resurser att hantera olika systemdrifttillstånd**

Att kunna hantera olika systemdrifttillstånd (med "systemdrifttillstånd" avses normaldrift, skärpt drift, nöddrift, nätsammanbrott och återuppbyggnad) kan påverkas negativt av eventuella begränsningar i nödvändiga förmågor och resurser. Nedan följer några exempel på sådana förmågor och resurser som upprätthåller viktig funktionalitet inom elförsörjningen:

- > Den kommande energiomställningen med förändrad produktionsmix innebär ett allt större behov av att kunna balansera ett mer volatilt kraftsystem, vilket bedöms medföra ett ökat behov av stödtjänster.
- > Eventuella brister i kraftsystemets tekniska förmågor, exempelvis avseende nödvändig reglerutrustning för spänningsreglering, kan också vara en potentiell utmaning.
- > Vid återuppbyggnad är förmågan att upprätthålla lokal/regional elförsörjning avhängig av den tekniska och organisatoriska förmågan att köra delsystem (ö-drift). Brister i förmågan kan exempelvis bero på att vissa produktionsanläggningar, dvs. kraftvärmeverk, som är nödvändiga för ö-driften, läggs ner pga. lönsamhets- och miljöskäl (jfr riskkälla "1.13 *Överlappande och divergerande bestämmelser och lagstadgade krav på aktörer inom elförsörjningen*").
- > En generell utmaning är att det kan vara svårt att genomföra storskaliga funktionsövningar inom elsektorn.



*Potentiella konsekvenser:* eventuella bristfälliga förmågor och resurser kan öka risken för att inte kunna hålla kraftsystemet inom driftsäkerhetsgränserna. Vid inträffade svåra påfrestningar inom elförsörjningen kan sådant försvåra att återgå till (normal)drift.

Exempel på åtgärder:

- > Säkerställ erforderliga tekniska förmågor och resurser som behövs för att hålla kraftsystemet inom driftsäkerhetsgränser.
- > Säkerställ viktiga resurser som möjliggör ö-driftsförmågan.
- > Säkerställ att samhällsviktiga verksamheter har egen lokal reservkraft.
- > Säkerställ sammanhållen planering (inkl. utbildning och övning) som krävs för återuppbyggnad av kraftsystemet på alla nivåer inom elförsörjningen, men även med andra berörda aktörer.
- > Säkerställ teknisk förmåga att återstarta elanläggningar vid nätsammanbrott.

***1.17 Störningar i kritiska beroenden, andra sektorer, kritiska försörjningskedjor eller tjänster som elförsörjningen är beroende av***

Störningar i kritiska beroenden eller kritiska försörjningskedjor, eller tjänster som aktörer inom elförsörjningen är beroende av kan orsaka störningar inom den egna verksamheten.

Sådana kritiska beroenden är exempelvis elförsörjningen. Vid elavbrott är tillgången till lokal reservkraft (inkl. drivmedel) eller avbrottsfri kraft kritisk. Störningar i försörjningen av drivmedel till reservkraft kan i sin tur bero på olika anledningar, globala eller lokala.

Vidare finns beroenden av sådan utrustning, produkter och komponenter, som behövs för att kunna upprätthålla, bygga ut och vid behov, reparera den kritiska infrastrukturen inom elförsörjningen – som i vissa fall tillhandahålls av ett fåtal leverantörer som dominerar på marknaden.

Exempel på sektorer och tjänster där störningar eller avbrott kan leda till negativa konsekvenser inom elförsörjningen:

- > Tele- och datakommunikationer
- > Transporter för kritisk materiel och personal inom elförsörjningen (väg-, järnväg-, flyg- och sjötransporter)
- > Vattenförsörjning (till exempel för att kyla ned viss infrastruktur)
- > Väderprognostjänster (för störningsanalyser och produktionsplaner)

Exempel på åtgärder:

I den utsträckning det är möjligt både tekniskt och ekonomiskt:

- > Säkerställ den egna verksamhetens kritiska beroenden genom kontinuitetshantering som även omfattar externa beroenden.
- > Säkerställ verksamhetens förmåga till redundant försörjning (t.ex. vatten, ventilation, värme, lagerhållning av drivmedel m.m.).

Brister i organisatoriska frågor, t.ex. bristfällig teknisk dokumentation av den infrastruktur som upprätthåller kritiska försörjningskedjor, eller bristfälliga kontinuitets- och nödsituationsplaner kan också vara en orsak till eller försvåra hanteringen av störningar.

*Potentiella konsekvenser:* avbrott och störningar i den ordinarie (kritiska) verksamheten och dess infrastruktur, men även i sådan verksamhet som behövs vid krissituationer och svåra påfrestningar.

Eventuella konsekvenser kan även påverkas av bristfällig förmåga hos en leverantör/aktör att tillhandahålla en kritisk tjänst eller vara.

---

Svenska kraftnät är systemansvarig myndighet, med uppgift att på ett affärsmässigt sätt förvalta, driva och utveckla ett kostnadseffektivt, driftsäkert och miljöanpassat kraftöverförings-system. Det omfattar ledningar för 400 kV och 220 kV med stationer och utlandsförbindelser. Svenska kraftnät utvecklar transmissionsnätet och elmarknaden för att möta samhällets behov av en säker, hållbar och ekonomisk elförsörjning. Därmed har Svenska kraftnät också en viktig roll i klimatomställningen.

SVENSKA KRAFTNÄT  
Box 1200  
172 24 Sundbyberg  
Sturegatan 1

Tel: 010-475 80 00  
Fax: 010-475 89 50  
[www.svk.se](http://www.svk.se)

