SAMMANFATTNING

Risk- och sårbarhetsanalys för år 2020

SVENSKA KRAFTNÄT

Svenska kraftnät

Svenska kraftnät är ett statligt affärsverk med uppgift att förvalta Sveriges transmissionsnät för el, som omfattar ledningar för 400 kV och 220 kV med stationer och utlandsförbindelser. Vi har också systemansvaret för el. Vi 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 klimatpolitiken.

Foto
Tomas Ärlemo

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

Rapporten baseras på Affärsverket svenska kraftnäts sammanfattande redovisning av risk- och sårbarhetsanalysen för år 2020 (Svk 2019/2886) till regeringskansliet och Myndigheten för samhällsskydd och beredskap (MSB).

1. För en robust elförsörjning

Elförsörjningen är en nationellt samhällsviktig verksamhet och en förutsättning för samhällets funktionalitet. Därför ska de mest nödvändiga funktionerna i den samhällsviktiga verksamheten kunna upprätthållas, såväl vid krissituationer som inför och under krig.

Arbetet med risk- och sårbarhetsanalys syftar till att öka medvetenheten och kunskapen om den mångfald av hot, risker och sårbarheter som föreligger. Därmed utgör risk- och sårbarhetsanalysen en grund för att förstärka förmågan att förebygga, motstå och hanterar störningar inom elförsörjningen som kan medföra svåra påfrestningar på samhället.[1]

Kraftsystemet är en grundförutsättning för Sveriges totalförsvarsförmåga. Robusthet, redundans och reparationsförmåga för flera funktioner inom elförsörjningen behöver fortsatt förstärkas, för att säkerställa förmågan även under störda förhållanden.

Den pågående Coronapandemin har ytterligare tydliggjort den samhällsviktiga verksamhetens beroenden av såväl personella och materiella resurser som förmågan till samverkan inom elförsörjningen. Att säkerställa kontinuiteten i den samhällsviktiga verksamheten, det vill säga att kunna bedriva kritisk verksamhet på en acceptabel nivå oavsett typ av störning eller avbrott som verksamheten utsätts för, är av central betydelse för en robust elförsörjning.

[1] 1 Jfr Elberedskapslagen (1997:288) och Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

2. Nationell risk- och förmågebedömning för elförsörjningen

Svenska kraftnät ska, som särskilt ansvarig myndighet för krisberedskapen, analysera hot och risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra förmågan till verksamhet inom området. I analysen ska särskilt beaktas:

- situationer som uppstår hastigt, oväntat och utan förvarning, eller en situation där det finns ett hot eller en risk att ett sådant läge kan uppstå,
- situationer som kräver brådskande beslut och samverkan med andra aktörer,
- att de mest nödvändiga funktionerna kan upprätthållas i samhällsviktig verksamhet, samt
- förmågan att hantera mycket allvarliga situationer inom myndighetens ansvarsområde.

Analysen ska värderas och resultatet sammanställas i en risk- och sårbarhetsanalys. Svenska kraftnät, förutom att analysera hot, risker och sårbarheter inom sitt eget ansvarsområde, upprättar en nationell risk- och sårbarhetsanalys för elsektorn (produktion av, distribution av och handel med el) enligt elberedskapslagen. Dessa båda aspekter sammanställs i en samlad risk- och sårbarhetsanalys.

3. Identifiering av samhällsviktig verksamhet inom elförsörjningen och dess kritiska beroenden

Elförsörjningen består av aktörer som producerar, distribuerar och handlar med el och är en av de samhällsviktiga verksamheter som är helt avgörande för samhällets funktionalitet. Ett elavbrott påverkar bland annat elektroniska kommunikationer, transporter, kommunalteknisk försörjning, vård- och omsorg, energiförsörjning och finansiella tjänster. Flera samhällsviktiga verksamheter avstannar omedelbart vid ett elavbrott om de saknar reservkraft.

Med samhällsviktig verksamhet avses en verksamhet som uppfyller minst ett av följande villkor:

- Ett bortfall av eller en svår störning i verksamheten kan ensamt eller tillsammans med motsvarande händelser i andra verksamheter leda till att en allvarlig kris inträffar i samhället.
- Verksamheten är nödvändig eller mycket väsentlig för att en redan inträffad kris i samhället ska kunna hanteras så att skadeverkningarna blir så små som möjligt.[2]

Inom elförsörjningen bedöms den samhällsviktiga verksamheten omfatta sådana operativa funktioner som säkerställer både transmission, distribution, produktion och handel av el, både i normalfall men även vid krissituationer och svåra störningar.

En viktig utgångspunkt för riskanalysen är att identifiera den samhällsviktiga verksamheten inom elförsörjningen, vad den består av, med särskilt fokus på de verksamhetsdelar, inklusive arbetsprocesser och –aktiviteter inom den egna verksamheten, som bedöms som kritiska ur ett krisberedskaps- och kontinuitetsperspektiv.

Identifiering av kritisk verksamhet utgör alltså en strategisk utgångspunkt för arbete med risk- och sårbarhetsanalysen och en nödvändig grund för kontinuitetshantering. Kritiska verksamheter ska fungera i normalläge men även i kris och krig, dvs. under störda förhållanden. Därför är det av yttersta vikt att de identifierade verksamheterna har en förmåga att förebygga, motstå och hantera olika slags hot och risker (all-hazards) samt en fungerande kontinuitetshantering.

[2] Jfr Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser MSBFS 2016:7. MSB har den 27 oktober 2020 uppdaterat definitionen av samhällsviktig verksamhet, vilken betonar vikten av att upprätthålla eller säkerställa samhällsfunktioner som är nödvändiga för samhällets grundläggande behov. Den uppdaterade definitionen börjar gälla under hösten 2021.

Genom att ha fastställt de kritiska verksamheterna kan man arbeta med kontinuitetshantering på ett systematiskt sätt.[3] I nästa steg identifierats dess kritiska beroenden (resurser).

Som ett led i arbetet identifieras acceptabla avbrottsnivåer[4] för verksamhetens kritiska beroenden (resurser), även där det finns kritiska beroenden av andra aktörer.

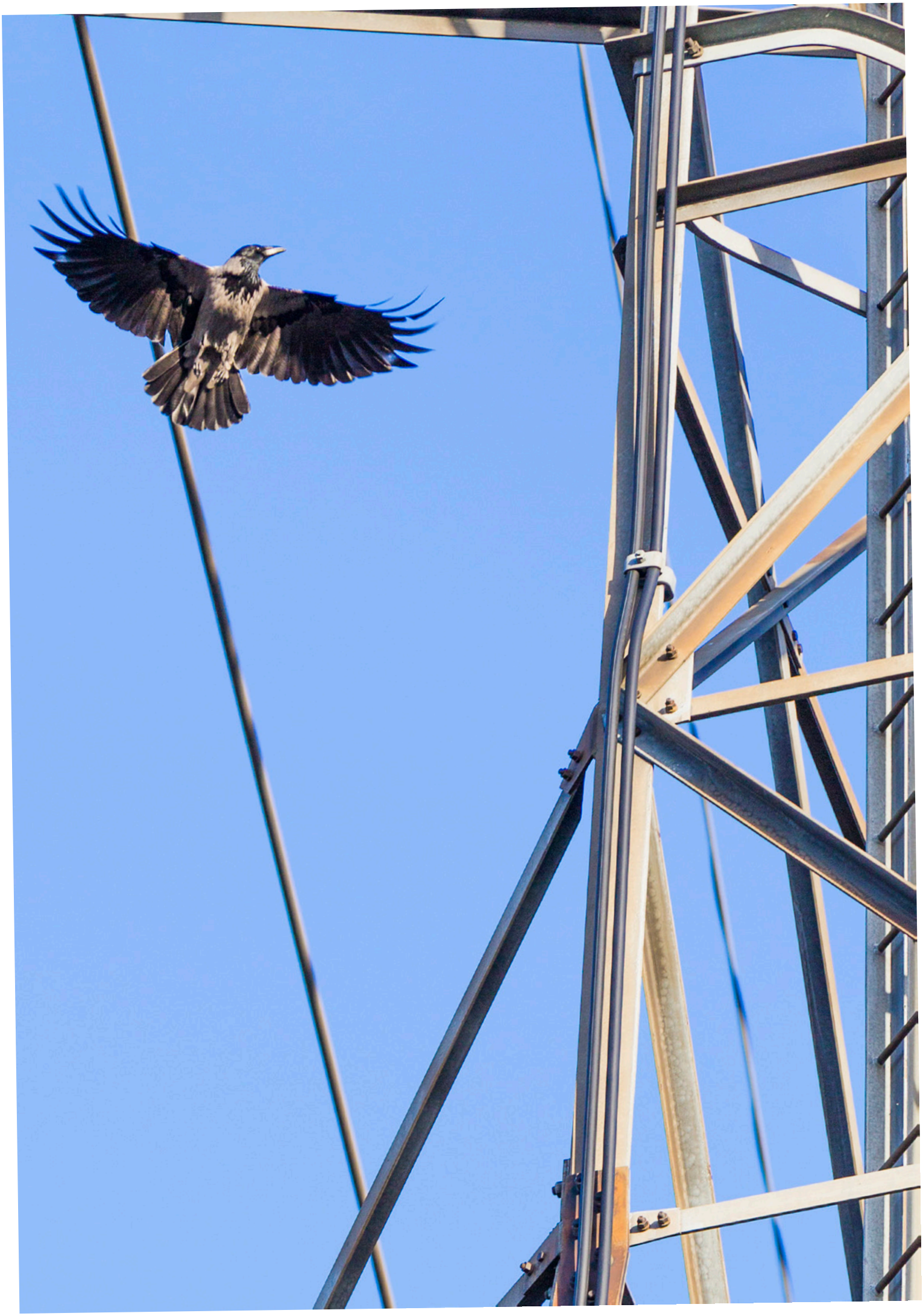
Kritiska beroenden inom elförsörjningen kan sammanfattas som följande:

- Elektroniska kommunikationer
- Teknisk infrastruktur (inklusive IT-infrastruktur)
- Kritisk materiel, omfattande även kritiska leverantörskedjor
- Framkomlighet (för transport av materiel och personal, till exempel vid reparationsarbete)
- Personella resurser
- Samverkan med andra företag inom elsektorn, till exempel för att kunna kalla fältpersonal från andra företag till reparationsarbete (även stöd från aktörer i samhället, till exempel räddningstjänst, polis, Försvarsmakten och frivilligorganisationer)
- Beredskapsorganisation, dvs. en fungerande kris- och krigsorganisation/storstörningsorganisation. Tillgång till reservdriftställe som medger teknisk drift om ordinarie driftsställe och IT- system faller bort.
- Information - tillgång till störningsinformation och en aktuell och riktig lägesbild för att kunna hantera en störningssituation.

Värt att notera är att de kritiska beroendena listade ovan i vissa fall är kritiska för den dagliga driften, i vissa fall är kritiska för att kunna upprätthålla verksamheten i en kris eller krigssituation.

[3] Konkret innebär kontinuitetshantering att motstå störningar och avbrott, att bedriva kritisk verksamhet på en acceptabel nivå oavsett vilken typ av störning eller avbrott som verksamheten utsätt för, att motverka eller lindra konsekvenser av skador vid avbrott samt att snabbt kunna återfå normal funktionalitet efter ett avbrott.

[4] Med acceptabel avbrottstid menas den tid som har beslutats i förväg på hur långa avbrott som kan accepteras, dvs. vilken förmåga/tolerabel nivå som är acceptabel att bedriva verksamheten vid störning.



4. Hot, risker och sårbarheter inom elförsörjningen

Analysen beskriver den aktuella antagonistiska hotbilden för elsektorn[5] samt ett axplock av risker och utmaningar i samhällsutvecklingen som bedöms ha bäring på krisberedskapen inom elförsörjningen – redan i dag eller på längre sikt. Även tidigare risk- och sårbarhetsanalyser samt arbetet med EU:s elkrisscenarier[6] utgör ett viktigt ingångsvärde i det fortsatta arbetet med den nationella risk- och sårbarhetsanalysen för elsektorn.

Att analysens tyngdpunkt ligger på vissa utvalda fokusområden innebär dock inte att endast dessa områden är av relevans för den aktuella risk- och sårbarhetsanalysen, utan det är viktigt att kontinuerligt genomföra hot- och riskanalyser för den egna verksamheten, även sådana utanför fokusområden för denna analys.

Analysen innehåller inga bedömningar av hur troliga händelseutvecklingar kan vara, utan syftar främst till att ge en orientering i det över tid aktuella hot- och risklandskapet inom elförsörjningen.

Vad kan anses påverka säkerheten och beredskapen inom elförsörjningen? Frågan kan också besvaras utifrån den förmåga som ska upprätthållas, exempelvis inom:

- Reparationsberedskap (avseende reparationsmateriel och utförande personal - både utifrån kompetens/kunskap och utifrån tillräcklig bemanning. Transporter är en viktig del av reparationsberedskapen.)
- Ödrift och dödnätsstart (vid svåra störningar inom elförsörjningen)
- Störningsreserver - t.ex. gasturbiner (vid svåra påfrestningar inom elproduktion)
- Säkra och robusta kommunikationer
- Säker och robust IT-infrastruktur
- Fullgod informationssäkerhet
- Fullgott fortifikatoriskt och fysiskt skydd (avseende anläggningar, ledningsplatser och övriga lokaler)

En principiell utmaning är att aktörer inom elförsörjningen själva inte kan påverka vissa händelser samt yttre hot som samhällsutvecklingen kan medföra. Därför är det viktigt att känna till sådant som kan utgöra hot, risker och utmaningar för verksamheten - och förhålla sig till det. I detta ingår en ständig balansgång mellan samhällsutvecklingen i stort, säkerhetsskyddet och beredskapsförmågan inom elförsörjningen.

[5] Med ett antagonistiskt hot avses en aktör som har avsikt och förmåga att skada elförsörjningen på en nivå som får konsekvenser för Sveriges säkerhet.

[6] Enligt EU Kommissionens förordning (EU 2019/941) om riskberedskap inom elsektorn. Arbetet samordnas med den behöriga myndigheten i Sverige, Statens Energimyndighet.

4.1. Antagonistisk hotanalys

Följande hotbild omfattar kända hot och den ska inte uppfattas som heltäckande för alla hot mot elförsörjningen som kan förekomma. [7]

Sammanfattning

Främmande makts informationsinsamling och kartläggning är fortsatt det största hotet mot Sveriges elförsörjning. Säkerhetspolisens första hotbild specifikt för säkerhetskänslig verksamhet publicerades i juni 2019 och nämner Ryssland och Kina som stater med intresse för sådan verksamhet. Hotet från terrorism och organiserad kriminalitet är lågt men kan inte uteslutas. Bedömningarna i Svenska kraftnäts nationella risk- och sårbarhetsanalys 2018 består alltså. Angreppssätten är också i stort sätt de samma, bland annat phishing-mejl, kontaktförsök via sociala medier och rekrytering av anställda eller entreprenörer inom elsektorn. Säkerhetspolisen lyfter också fram att leverantörskedjor och upphandlingar kan nyttjas av antagonister för att nå sina mål.

4.1.1 Hot

Fysisk skadegörelse

Under 2019 har sprängdåd i Sverige ökat till det dubbla jämfört med 2018. Sprängningarna utförs huvudsakligen av och mot kriminella nätverk. Nationella bombskyddet ser en trend med kraftigare sprängladdningar och att sprängningar sker även i mindre städer. Explosivämnen har blivit åtråvärda för kriminella och stölder sker bland annat på byggarbetsplatser där sådana ämnen förvaras. Explosivämnen har även upphittats utomhus i naturen i bebyggt område.

Andra former av fysisk skadegörelse kan också förekomma.

Hot mot elförsörjningen:

Fysisk infrastruktur inom elförsörjningen kan drabbas indirekt av en sprängning i närheten av anläggningen. Inbrott kan ske för att komma över explosivämnen, tändhattar och annan utrustning för bombtillverkning.

Phishing-mejl och andra cyberhot

Mejl i syfte att lura mottagagaren, s.k. phishing, att gynna angriparen på något sätt (ofta ekonomiskt) är vanligt förekommande idag. Angriparen kan även ha som syfte att få åtkomst till inloggningsuppgifter och IT-system. De falska mejlen blir alltmer sofistikerade. Avsändaren kan se ut att vara en välkänd person, t.ex. en högt uppsatt chef eller en leverantör som man normalt har kontakter med. Innehållet utformas så att det är

[7] Detta delkapitel baseras på Svenska kraftnäts hotbild för elsektorn (januari 2020), Svk 2020/287. Hotbilden ska ses som ett komplement till Säkerhetspolisens ”Hotbild mot säkerhetskänslig verksamhet” som är mer generellt formulerad.

svårare att upptäcka att det inte är från den påstådda avsändaren, t.ex. genom att vara språkligt korrekt.

Det finns en rad andra cyberhot (dvs. hot via Internet) som är vanligt förekommande. Informationsinhämtning kan ske genom inspelning (avlyssning) eller avbildning genom fjärrstyrning av elektronisk utrustning som mobiltelefoner och datorer men även smartklockor och liknande. Kapning av konton, lösenord och identiteter ger antagonister möjligheter att sprida vilseledande information under en trovärdig täckmantel.

Hot mot elförsörjningen:

Som alla andra sektorer i samhället kan även elsektorn drabbas av phishing-mejl och andra cyberhot. Informationsinsamling, spridning av falsk information och åtkomst till inloggningsuppgifter för IT-system kan ha allt från försumbar påverkan till förödande effekter för elförsörjningen, beroende på hur höga kunskaper och andra skydd mot cyberhot som finns i den drabbade organisationen.

Informationsinsamling genom affärskontakter och sociala medier

Genom kontakter med anställda kan information samlas in om en verksamhet och de anställda själva. Informationsinsamling kan ske på en rad olika sätt, t.ex. vid affärsmöten, konferenser, genom LinkedIn och andra sociala medier. Säkerhetspolisen pekar på att Kina men även Ryssland och andra stater har en aktiv informationsinsamling om säkerhetskänslig verksamhet i Sverige.

Hot mot elförsörjningen:

Genom kontakter med personal inom elförsörjningen kan en antagonist få tillgång till information (uppgifter) av betydelse för elförsörjningen, inklusive om annan personal med nyckelfunktioner, tillgång till IT-system (t.ex. genom inloggningsuppgifter) och möjlighet att påverka hur personal agerar (t.ex. under kriser).

Uppköp av fastigheter och mark

Uppköp av mark- och sjöområden eller fastigheter i närheten av objekt som är strategiska för Sveriges säkerhet, kan genomföras i syfte att komma åt säkerhetskänslig verksamhet. Säkerhetspolisen nämner två stater som intresserar sig för säkerhetskänslig verksamhet i Sverige: Ryssland och Kina. Strategiska köp av fastigheter och mark, genomförda av dessa aktörer, eller med kopplingar till dessa aktörer, är därför av intresse i sammanhanget. Uppköp av fastigheter, mark- och sjöområden kan också användas som ett strategiskt instrument i hybridkrigföring, där verksamhet under det förberedande skedet har en stor betydelse.[8] I Finland finns det exempel på utländska köp av mark och fastigheter nära anläggningar som kan ha strategisk betydelse för samhället

[8] Se finska Säkerhetskommitténs bedömning: < https://svenska.yle.fi/artikel/2016/02/15/ryska-markaffarer-ett-hot-sakerhetskommitten-listade-hybridkrigsfenomen >, inhämtat december 2019

och totalförsvaret. Finland har också en ny lag om tillstånd för fastighetsköp för köpare utanför EU- och EES-området som trätt i kraft 2020.[9]

Hot mot elförsörjningen:

För elförsörjningens del kan detta handla om att en främmande makt, eller personer med kopplingar till en främmande makt, köper mark- eller sjöområden eller fastigheter nära till viktiga elanläggningar, broar eller vägar (som krävs för att transportera både personal och materiel till anläggningar). Syftet kan vara att kunna blockera vägar till anläggningar, avlyssna eller sabotera dessa. Det kan även röra sig om sådana områden som ligger nära viktiga kommunikationsnoder för elförsörjningen. Här handlar de främsta hoten om avlyssning och möjligheten att störa viktig kommunikationstrafik för elsystemet.

Leverantörskedjor och underentreprenörer

Det privata näringslivet ansvarar alltmer för säkerhetskänsliga verksamheters viktiga leveranser och globaliseringen innebär att verksamheternas leverantörer kan finnas i flera länder. Därför är det viktigt att verksamhetsutövare inom säkerhetskänslig verksamhet är medvetna om potentiella risker som utkontraktering av verksamhetskritiska delar till en tredje part kan medföra.

Ett hot är att spionutrustning planteras i kritiska komponenter som används inom elförsörjningen. Det går inte att utesluta att en kvalificerad angripare planterar avancerad skadlig kod i hårdvara hos leverantörer som sedan köps in och används i samhällskritiska IT-system, exempelvis i SCADA[10]-system.

Leverantörskedjor möjliggör flera angreppssätt för en angripare. Ju längre leverantörskedja, dvs. ju fler bolag som finns i kedjan, desto fler potentiella angreppspunkter finns för angriparen. En antagonist kan också, i syfte att komma åt den säkerhetskänsliga verksamheten, bli en leverantör av kritisk utrustning.

Även utländskt delägande i företag eller strategiska investeringar (av utländska aktörer) i företag som driver säkerhetskänslig verksamhet kan utgöra ett hot, om syftet är att angripa eller utöva påtryckningar mot den säkerhetskänsliga verksamheten. Genom delägandeskap/strategiska investeringar kan man få tillgång till känsliga uppgifter om den säkerhetskänsliga verksamheten och därigenom en möjlighet att påverka hur verksamheten styrs. Även här hänvisas till den bedömning som Säkerhetspolisen gör angående Ryssland och Kina som intresserar sig för säkerhetskänslig verksamhet i Sverige (och andra europeiska länder). Globaliseringen har medfört att det inte är ovanligt att företag i olika länder är sammankopplade genom ägarskap. Ett exempel från elsektorn är det statliga kinesiska företaget State Grid Corporation of China som äger den grekiska

[9] < https://www.defmin.fi/sv/aktuellt/tillstand_for_fastighetskop_for_kopare_utanfor_eu-_och_ees-omradet>, inhämtat december 2019

[10] industriellt kontroll- och styrsystem

nationella systemoperatören (TSO) till hälften och är delägare i en portugisisk TSO. Samma företag har 2018 försökt köpa in sig i tyska TSO:n 50Hertz.[11] I Sverige visade företaget intresse för att köpa ABB Power Grid (som har verksamhet Ludvika) när den var till salu.[12]

Hot mot elförsörjningen:

Inom elförsörjningen finns ett stort beroende av entreprenörer och leverantörer för byggnation, underhåll, reparationer och kritiska komponenter, även från utlandet. Det finns vissa leverantörer som tillhandahåller verksamhetskritiska tjänster/komponenter åt flera nordiska och europeiska systemoperatörer för el. Vid ett eventuellt angrepp mot dessa leverantörer, eller mot tjänster som dessa leverantörer tillhandahåller, finns en risk för en kaskadeffekt i de verksamheter som anlitar samma leverantör. Antagonisters insteg i leverantörskedjor och delägarskap i företag som är leverantörer och entreprenörer till elsektorn kan inte uteslutas.

Gråzon och hot mot Sveriges totalförsvar

Med gråzon menas ett tillstånd av osäkerhet som varken kan beskrivas som fred eller regelrätt krig men där antagonistiska handlingar riktas mot Sverige från en annan stat, mer eller mindre öppet. Under gråzon kan ryktesspridning, motsägelsefull information, kriminell verksamhet, sabotage samt nätverks- och påverkansoperationer förekomma.

Hot mot elförsörjningen:

Attacker kan riktas mot elnätets infrastruktur och IT-infrastruktur i syfte att destabilisera samhällets funktionalitet och försämra totalförsvarsförmågan. I förlängningen kan en antagonist vilja utöva inflytande på Sveriges utrikes- och säkerhetspolitiska agerande. I händelse av att Sverige blir utsatt för väpnad konflikt bedöms sabotage mot elförsörjningen utgöra ett led i hybridkrigsföring. Sabotage kan ske både genom cyberangrepp och genom fysiskt sabotage. Sabotage i mindre omfattning kan genomföras i fredstid i syfte att testa elförsörjningens förmåga att förebygga och hantera angrepp.

[11] Reuters, ”China's State Grid seals purchase of stake in Greek power grid”, 2016. The Asset, ”State Grid renews attempt to buy into German electricity transmission grid”, 2018. Second Opinion, ”Laddat när Kina vill köpa energiföretag”, 2018.
[12] Dalabygden, ”Ludvika förbereder sig få kinesiska herrar”, 2018.

4.1.2 Antagonistiska aktörer

Allmänt

Antagonister som orsakar eller utför angrepp mot elförsörjningen kan, då de är kända, delas in i olika typer av antagonister. Några typer beskrivs nedan. Det är inte heller ovanligt att antagonister förblir helt okända och inte kan hänföras till någon typ.

Främmande stat

Säkerhetspolisen nämner två stater som intresserar sig för säkerhetskänslig verksamhet i Sverige: Ryssland och Kina. Det utesluter inte att fler stater också är intresserade. Ryssland samlar in information och kartlägger säkerhetskänslig verksamhet, vilket kan ingå i att hålla Sverige i en gråzon och vara förberedelser för att kunna angripa Sverige.

Kina visar framförallt intresse för forskning, teknologi och innovationer som landet vill tillägna sig för att främja sin egen industri. Under 2019 har relationerna mellan Sverige och Kina försämrats. I december 2019 uttalade Kinas dåvarande ambassadör i Sverige att Kina avser att begränsa utbytet och samarbetet inom handel och ekonomi med Sverige. Det betyder inte att risken för industriellt spionage i Sverige minskar.

Statliga aktörer har stora resurser, bred kompetens och arbetar långsiktigt för att nå sina mål avseende information om Sverige, inklusive säkerhetskänslig verksamhet.

Övriga antagonister

Terrorister i Europa har sporadiskt visat intresse för kärnkraftverk men i Sverige finns inga tecken på att dessa delar av elförsörjningen skulle vara ett mål (enligt öppna källor).

Det troligaste hotet från terrorister eller kriminella är skador på elförsörjningen som en konsekvens av angrepp riktade mot ett annat närstående mål, antingen fysiskt/geografiskt eller i cyberrymden.

Ensamagerande antagonister kan förekomma. Motiven för deras agerande varierar. Det kan bland annat vara missnöje med att mark används för elförsörjningens infrastruktur (t.ex. ledningar och ledningsstolpar) vilket kan yttra sig som fysisk skadegörelse.

Mål inom elförsörjningen

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. IT-system är kritiska för elförsörjningen samtidigt som de kan vara svåra att skydda eftersom det ligger i deras funktionalitet att de ska vara tillgängliga dygnet runt, för flera aktörer och från flera geografiska platser. Attackerna 2015 och 2016 mot elförsörjningen i

Ukraina visar att cyberangrepp är möjligt och att konsekvenserna då kan bli omfattande.

Information i form av data i elförsörjningens IT-system kan vara det egentliga målet för en antagonist men även information om anläggningar, IT-system, sårbarheter i elförsörjningen och personer i kritiska funktioner kan vara mål för informationsinhämtning och kartläggning.

4.2. Risker och utmaningar i samhällsutvecklingen

Här nedan följer ett urval av sådana aktuella risker och utmaningar kopplade till samhällsutvecklingen som bedöms ha bäring på krisberedskapen inom elförsörjningen.[13]

Att utveckla elsystemet innebär ofta långa ledtider vilket ytterligare stärker behovet av att analysera möjliga framtida utveckling. Det finns flera tänkbara händelseutvecklingar som kan komma att påverka elförsörjningens robusthet negativt, med konsekvenser som exempelvis kapacitets- eller elenergibrist, olyckor och tekniska fel.

Exempelvis kan konsekvenser av extremt väder/klimatförändringar leda till störningar i den normala driften, både på kort och också lång sikt. Hur omfattande konsekvenserna kan bli beror bland annat på infrastrukturens robusthet, förebyggande arbete samt huruvida reparationsberedskapen är dimensionerad för att möta konsekvenserna av extremt väder/klimatförändringar. Om viktiga anläggningar, som ingår i förmågan att upprätthålla kraftsystemet, påverkas av extremt väder/klimatförändringar kan beredskapsförmågan påverkas negativt. Detta bör beaktas i arbetet med dimensionering avseende till exempel infrastruktur, reparationsberedskap, organisation och ledning, samband och kommunikation.

4.2.1 Kompetensförsörjning och bemanning

Utmaningar kopplade till kompetensförsörjning och bemanning är fortsatt aktuella. Elförsörjningen är en högteknologisk sektor, där man är beroende av en rad olika tekniska spetskompetenser. Även kompetens inom juridik, miljötillstånd och markåtkomst är viktig för att kunna utveckla elsystemet miljörättsligt, rättssäkert och effektivt. Dessutom håller det svenska transmissionsnätet på att byggas ut och upprustas, vilket innebär ett ökat behov av utförande personal.

Inom elförsörjningen finns generellt också ett stort leverantörsberoende. Även ”outsourcing” bedöms fortsatt öka, dvs. att verksamhetsutövaren lägger ut tjänster, processer eller system på en extern leverantör/utförare. Det kan vara en utmaning att hitta leverantörer med rätt kunskap och kompetens, särskilt inom landets gränser. Dessutom nyttjas samma resurser av flera aktörer inom elsektorn, vilket vid större störningar inom elförsörjningen kan komma att leda till resursbrist.

Många av de leverantörer som anlitas inom elförsörjningen är utländska och det finns ett allt större beroende av utländska leverantörer från utanför EU, även för att tillhandahålla kritiska komponenter. En del utländska leverantörer innehar

[13] Delkapitlet baseras delvis på Totalförsvaret forskningsinstitutets (FOI) Litteraturstudie om framtidens elförsörjning och elberedskap (2018). Beskrivningar i rapporten är baserade på strategiska framtidsanalyser och bedömningar genomförda av ett flertal myndigheter, forskningsinstitut mm. Jfr även Svenska kraftnäts omvärldsanalys 2020, Svk 2020/2156, 2020-08-18. I analysen identifieras och beskrivs följande megatrender: 1) Klimatförändringar, ökad elanvändning och bredare hållbarhetsfokus, 2) Tek-nologiska genombrott och ökad digitalisering, 3) Urbanisering och ett större mer mobil medelklass, 4) Ökad fokus på samhälls-säkerhet och sårbarhet, 5) Globalisering och individualisering

specialistkompetens som inte finns i Sverige, vilket kan innebära en risk vid omfattande samhällsstörningar, där rörlighet av varor och tjänster internationellt påverkas.

På grund av det stora konsult- och leverantörsberoende som finns inom elförsörjningen riskerar viktiga funktioner stå utan resurser vid en storstörningssituation eller höjd beredskap då entreprenörer och leverantörer vanligtvis inte ingår i verksamhetens beredskapsorganisation. Dessutom gäller inte alltid avtal med entreprenörer och leverantörer vid force majeure/höjd beredskap. I en gråzonssituation där krigslagar ännu inte trätt i kraft kan detta blir problematiskt, men även i krig.

Utvecklingen under de senaste årtiondena har dessutom medfört en generell trend att redundans avseende viktiga funktioner inom den egna organisationen minskar, vilket kan medföra svårigheter kring kompetensförsörjning samt långvarig bemanning av elanläggningar i händelse av kris. Den pågående Coronapandemin har aktualiserat risken med plötslig, omfattande personalfrånvaro och belyst beroendet av kritisk personal inom elförsörjningen.

Teknikutvecklingen, inklusive automatisering av arbetsuppgifter, ställer också krav på ny kompetens. Kunskapen om viktiga system (avseende både IT, OT och tekniska system) riskerar att minska hos driftpersonalen när automatiserade lösningar/AI ersätter ordinarie personal. Den dagliga användningen av digitala hjälpsystem och en samtidig förlust via ökande pensionsavgångar av personer med erfarenhet av robusta, manuella hjälpsystem, ökar risken för störningar i verksamheten om de automatiserade lösningarna slutar fungera och/eller måste ersättas av manuell hantering. Detta i sin tur kan medföra svårigheter för att kunna felavhjälpa och reparera. En sådan situation kan bli mycket svår i kris och krig, inte minst om verksamheten är kritiskt beroende av externa leverantörer och entreprenörer.

4.2.2. Internationalisering av det svenska elsystemet och geopolitiska utmaningar

Det svenska elsystemet sammankopplas allt mer med det nordiska och europeiska synkrona elsystemet, exempelvis så kommer det nordiska balanseringskonceptet (elhandel) knyta samman styrning av elnätet i hela norden. Detta innebär en hel del möjligheter men även vissa utmaningar, exempelvis minskad planeringsfrihet och minskade möjligheter till för Sverige anpassade lösningar. I sammanhanget bör det noteras att det i vissa avseenden ställs högre säkerhetskrav på verksamhetsutövare inom säkerhetskänslig verksamhet i den svenska säkerhetsskyddslagstiftningen än i motsvarande lagstiftningar i andra nordiska länder. Detta kan innebära vissa utmaningar i det nordiska samarbetet.

Ett alltmer sammankopplat nordiskt/europeiskt elsystem medför att information om det svenska elsystemet skickas bland annat till ENTSO-E[14] och nordiskt RSC[15] för att fullgöra de europeiska samarbetsavtalen. Denna utveckling kan innebära en minskad nationell kontroll över information om den svenska elförsörjningen och i slutändan kan det vara svårt att kontrollera till exempel vilka personer och/eller organisationer som får ta del av informationen. Mängden aggregerad information om nordiska och europeiska förhållanden kan också möjliggöra en ”större målyta” för angriparen (se även ”Gråzon och hot mot Sveriges totalförsvar” i tidigare avsnitt).

På grund av ökad sammankoppling av olika nationella elsystem är en regional kaskadeffekt inte omöjlig, med andra ord: att flera länder kan drabbas av en händelse som har sitt ursprung i ett land/i en enskild region. En variant av detta är ”överförd hotbild” mot den svenska elförsörjningen, där den svenska elförsörjningen drabbas även om angriparen haft ett annat land som huvudmål.

Omvärldsutveckling och geopolitiska intressen är också av vikt att beakta i sammanhanget. Exempelvis kan de baltiska staternas integrering i EU:s kraftsystem 2025 (och samtidiga frikoppling från det östeuropeiska systemet) nämnas, då den kommer att medföra en ändring i den energipolitiska spelplanen i Europa. Detta kan i sin tur ha en inverkan på de säkerhetspolitiska spänningar som i dagsläget finns mellan de baltiska staterna och några av dess grannländer.[16]

[14] Den europeiska samarbetsorganisationen för systemoperatörer (European Network of Transmission System Operators for Electricity)

[15] Regional Security Coordination

[16] Svenska kraftnäts omvärldsanalys 2020, s. 22

4.2.3 Ödrift

Vid omfattande störningar eller fel i transmissions- eller på regionnät i såväl fredstida kriser som i krig är förmågan till ödrift (regional försörjning utan elektrisk förbindelse med transmissionsnätet) av yttersta vikt.

Ödrift kan ha tillgång till olika produktionskällor exempelvis gasturbiner, dieselaggregat och kraftvärmeverk där bränslet kan bestå av biobränsle eller avfall. Gasturbiner och andra reservkraftverk är viktiga komponenter för att hantera en störning och få elsystemet i balans. Gasturbiner ska även kunna bidra med elproduktion i en ödriftsituation och är i vissa fall avgörande för dödnätsstart vid en storstörning. Analysen nedan avgränsas till ödriftsförmåga och kraftvärmeverkens roll i detta.

Kraftvärmeverken har en viktig roll att spela för ödriften. Dessa anläggningar ligger ofta i närheten av områden där förbrukningen är som störst. Kraftvärmeverken utgör en stor andel av sådana elproduktionskällor som kan användas i ödrift. Nedläggning, minskad nybyggnation och omvandlande av kraftvärmeverk till enbart fjärrvärmeproduktion begränsar möjligheten till ödrift, särskilt i närheten av större städer. Verksamhetsutövarna får allt svårare att finna lönsamhet när det gäller elproduktion i kraftvärmeverk på grund av låga elpriser och höga reinvesteringskostnader. Detta medför att äldre oljeeldade anläggningar läggs ned då de inte uppnår nationella och europeiska miljökrav samt lönsamhetskrav.

Det bör därför utredas mer huruvida förnybar elproduktion kan användas i ödrift. Dessvärre är vindkraftverken ofta placerade allt för långt bort från ödriftområden för att vara brukbara i ödriften. Vindkraften är väderberoende och bidrar inte med tillräckligt stabilitet i elsystemet, vilket behövs för att uppnå driftsäkerhet under såväl normal drift som under ansträngda förhållanden.

Kraftvärmeverken spelar också en viktig roll för elförsörjningen i flera städer under normal drift.[17]Kraftvärmeproduktionen har därmed en avhjälpande effekt på kapacitetsfrågan i tätorterna. Minskad produktion försämrar situationen ur ett effekttillräcklighetsperspektiv. Kraftvärmen spelar även en viktig roll för leveranssäkerheten då den i regel producerar mycket el när behovet är högt.[18]

Ödriftsförmågan är en hörnpelare i den svenska elberedskapen, därför kan de ovan beskrivna utmaningarna få omfattande konsekvenser för samhällets elförsörjning vid kris och krig.

[17] Jfr Svenska kraftnät: ”Kraftbalansen på den svenska elmarknaden, rapport 2020”, Svk 2020/334, 2020-05-29 s.27-29

[18] Notera att detta dock inte gäller de allra kallaste dagarna då värmeproduktionen behöver öka på bekostnad av elproduktionen. I skrivande stund pågår en analys på Svenska kraftnät angående effekt- och produktionstillgänglighet i hela Sverige. Se Regleringsbrev för budgetåret 2020 avseende Affärsverket svenska kraftnät, "Återrapportering” avseende försörjningstrygghet och leveranssäkerhet.

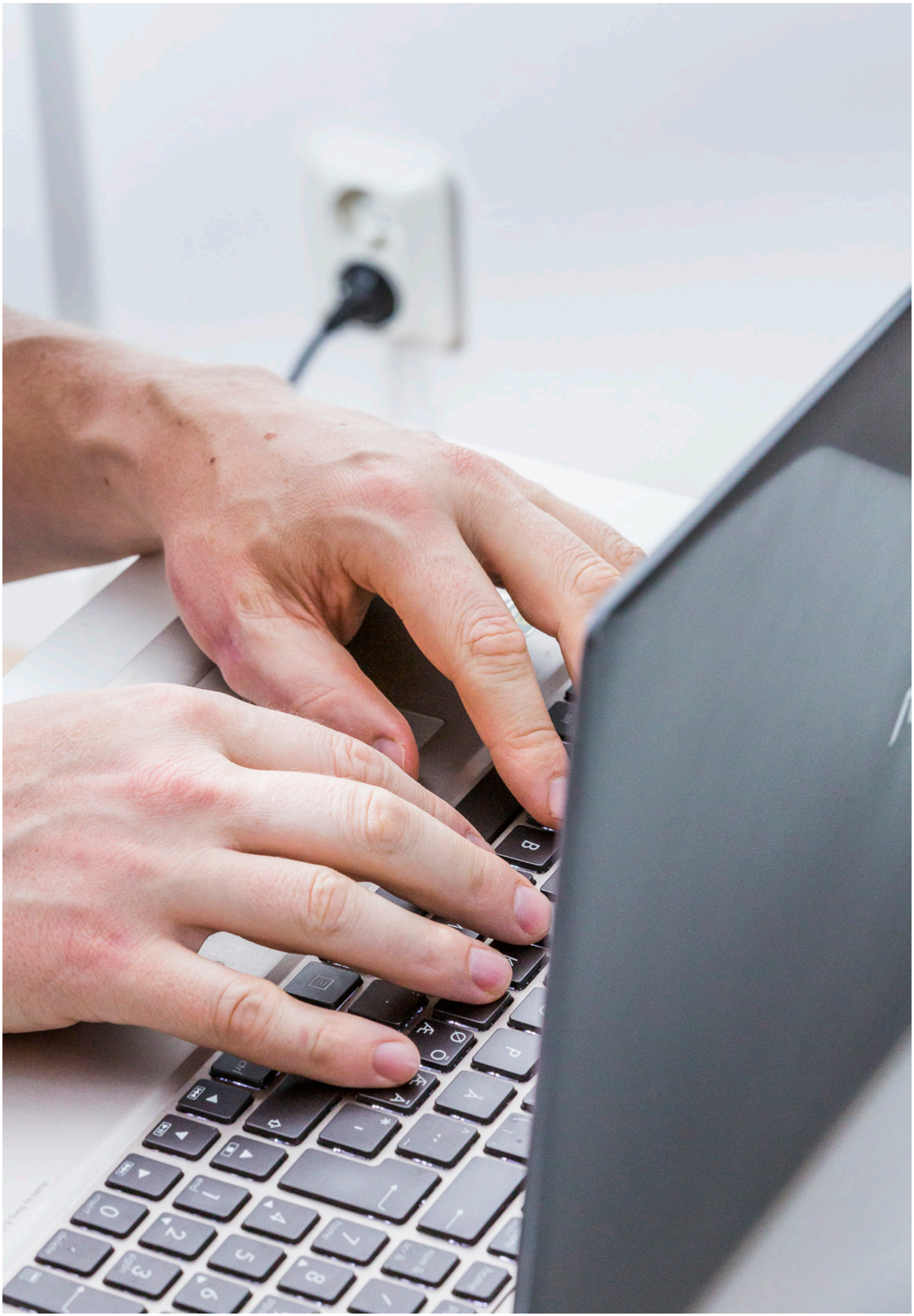
Detta är ett strukturellt problem, som bör utredas på en högre strategisk nivå än på en enskild anläggnings- eller verksamhetsnivå. Då trenden med nedläggning av lokala kraftvärmeverk går relativt fort, medan att återställa en nedlagd anläggning tar lång tid (om det ens är tekniskt och tillståndsmässigt möjligt), bör åtgärder vidtas omgående på nationell nivå. Det är en nödvändig förutsättning att viktiga resurser, som kräver långsiktig planering, säkerställs i förebyggande syfte. I detta fall handlar det om att kraftvärmeverken finns kvar och hålls i brukbart skick, under en övergångsperiod till det nya energilandskapet.

4.2.4 Tematisk fördjupning: fjärrstyrning av viktiga anläggningar inom elförsörjningen

Teknikutveckling och automatiserade lösningar möjliggör fjärrstyrning av kraftsystemet genom fjärråtkomst till elanläggningar. Detta innebär att elanläggningar normalt inte behöver bemannas för att kunna manövrera och styra apparater som är kritiska för att kunna upprätthålla kraftsystemet, vilket ger en effektiv samt drift- och personalsäker lösning för styrningen. Den pågående teknikutvecklingen och vissa elmarknadskrav innebär även att ännu fler funktioner som fjärrstyrs centralt för kraftsystemet kan och kommer att automatiseras ytterligare.

Utöver de möjligheter som fjärrstyrning medför så kan den även ge upphov till nya sårbarheter som är viktiga att analysera ur ett riskperspektiv. Sådana nya sårbarheter behöver inte nödvändigtvis ligga i kommunikationen i sig, men kan vara ett resultat av att man blir allt mer beroende av att kommunikationen hela tiden fungerar. I de fall fjärrstyrning integreras med en IT-miljö så ökas kommunikationssystemens exponering mot olika typer av cyberhot. Därför är det viktigt att beakta antagonistiska hot och även avväga eventuella konsekvenser av antagonistiska angrepp på framtagna tekniska lösningar och vid dimensionering av infrastrukturen.

Vid störningar i fjärrstyrning kan man bemanna de drabbade anläggningarna för att lokalt manövrera dessa, genom att bevarade tekniska förmågor till lokal styrförmåga kan utnyttjas av personal med kompetens att bemanna och direkt styra de berörda anläggningarna.



5. Förstärkt förmåga genom åtgärder

De identifierade och analyserade hoten, riskerna och sårbarheterna är ett viktigt underlag för arbete med åtgärder.

Den pågående Coronapandemin har påverkat kompetenshöjande insatser inom elsektorn. Exempelvis har inplanerade utbildnings- och övningsinsatser i flera fall inom beredskap och informationssäkerhet fått ställas in under 2020. Samtidigt har elsektorns aktörer arbetat praktiskt med kris- och kontinuitetshantering under Coronapandemin för att säkerställa kontinuiteten i den samhällsviktiga verksamheten, elförsörjningen, även vid påfrestningar i samhället.

Det är fortsatt viktigt att arbeta med robust- och säkerhetshöjande åtgärder inom elförsörjningen, för att kunna hantera olika slags händelser och möta eventuella kommande utmaningar. Kontinuitetshantering utgör grunden för att säkerställa krisberedskapsförmågan, oavsett vad som händer. Genom att analysera behov av åtgärder ur flera perspektiv; krisberedskap, säkerhetsskydd, kontinuitet och totalförsvar, kan synergieffekter uppnås i arbetet – för en förstärkt förmåga att upprätthålla samhällsviktig verksamhet.

Svenska kraftnät är ett statligt affärsverk med uppgift att förvalta Sveriges stamnät för el, som omfattar ledningar för 400 kV och 220 kV med stationer och utlandsförbindelser. Vi har också systemansvaret för el. Vi utvecklar stamnätet och elmarknaden för att möta samhällets behov av en säker, hållbar och ekonomisk elförsörjning. Därmed har Svenska kraftnät också en viktig roll i klimatpolitiken.

SVENSKA KRAFTNÄT
Box 1200
172 24 Sundbyberg
Sturegatan 1

Tel 010-475 80 00
Fax 010-475 89 50

www.svk.se

SVENSKA KRAFTNÄT