ÄRENDENR: 2021/4367 **DATUM:** 2021-11-01

ÖPPEN ANTAGONISTISK HOTBILD FÖR ELFÖRSÖRJNINGEN

November 2021

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 transmissionsnät och elmarknaden för att möta samhällets behov av en säker, hållbar och ekonomisk elförsörjning. Därmed har Svenska kraftnät också en viktig roll i klimatpolitiken.

Rapporten är skriven av Enheten för verksamhets- och säkerhetsskydd på Svenska kraftnät.
Illustrationer och kartor har tagits fram av Svenska kraftnät.
Foto omslag: Svenska kraftnät
Pressbilder från: Svenska kraftnät

Org. Nr 202100-4284

SVENSKA KRAFTNÄT
Box 1200
172 24 Sundbyberg
Sturegatan 1

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

www.svk.se

Innehåll

1 Inledning 5

1.1 Syfte *5*
1.2 Målgrupp *5*

2 Antagonistiska aktörer 6

2.1 Statliga aktörer *6*
2.2 Icke statliga aktörer *7*

3 Omvärldsbevakning 8

3.1 Norden *8*
3.2 Europa *10*
3.3 Övriga världen *11*
3.4 Covid-19 ..... *12*

4 Terrorhotbedömning 14

4.1 Europa *14*
4.2 Sverige *14*

5 Hotbild för elförsörjningen 16

5.1 Mål inom elförsörjningen *16*

6 Antagonistiska hot mot elförsörjningen 18

6.1 Cyberhot *18*
6.2 Fysisk skadegörelse *20*
6.3 Informationsinsamling *21*
6.4 Uppköp av fastigheter och mark *23*
6.5 Leverantörskedjor och underentreprenörer *24*
6.6 Gråzon och hot mot Sveriges totalförsvar *26*

1 Inledning

Svenska kraftnät går igenom flera öppna källor för att analysera och sammanställa de hot som anses vara aktuella mot elförsörjningen. De öppna källorna innefattar bland annat publikationer från Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap, Försvarsmakten, Försvarets radioanstalt och andra länders årsredovisningar.

Antagonistiska hot uppstår då en aktör har både avsikt och förmåga att genomföra skadliga handlingar riktat mot den skyddsvärda verksamheten. Eftersom en aktörs avsikt kan förändras snabbt, är en hotbild kortsiktig och behöver uppdateras löpande.

I denna öppna hotbild för elförsörjningen presenteras olika typer av antagonister, omvärldsbevakning och terrorhotnivåbedömning samt slutligen de antagonistiska hot som anses mest relevanta för verksamheter i elförsörjningen.

1.1 Syfte

Syftet med följande hotbild är att uppdatera den antagonistiska hotbilden som ingår i den nationella risk- och förmågebedömningen för elförsörjningen som Svenska kraftnät tar fram, den kan även användas som en källa avseende antagonistiska hot till säkerhetsskyddsanalysen. Hotbilden ska ses som ett komplement till Säkerhetspolisens ”Hotbild mot säkerhetskänslig verksamhet” [1] som är mer generellt formulerad.

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

1.2 Målgrupp

Målgruppen för hotbilden är verksamheter i elförsörjningen. För att hotbilden ska vara tillgänglig för elförsörjningen är den öppen och den baseras på öppna källor.

Varje verksamhet måste sedan själva baserat på den öppna hotbilden ta fram sin dimensionerande hotbild för sin verksamhet.

[1] Säkerhetspolisen – Hotbild mot säkerhetskänslig verksamhet juni 2019

2 Antagonistiska aktörer

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

2.1 Statliga aktörer

Det finns ett 15-tal stater som utövar informationsinsamling och som ägnar sig åt underrättelseinhämtning i Sverige. Säkerhetspolisen nämner särskilt tre stater som intresserar sig för säkerhetskänslig verksamhet i Sverige: Ryssland, Kina och Iran. Det utesluter inte att fler stater också är intresserade.

Ryssland samlar in information och kartlägger säkerhetskänslig verksamhet och infrastruktur, 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. I december 2019 uttalade Kinas dåvarande ambassadör i Sverige att landet avser att begränsa utbytet och samarbetet inom handel och ekonomi med Sverige. Situationen 2021 är oförändrad, Kina har under denna tid även hunnit anklaga den svenska diplomaten i Kina för spionerі.

Iran bedriver främst flykting och industrispionage mot Sverige. Den iranska statens flyktingspionage i Sverige är riktat mot minoritetsgrupper som den iranska regimen uppfattar som ett hot.

Det har under det senaste året uppmärksammats att USA bedrev spionage mot de nordiska länderna med mål att kartlägga viktiga personer inom den politiska världen. Detta finns närmare beskrivet i 3.1 omvärldsbevakning.

Säkerhetspolisen bedömer att underrättelsehotet kommer att fortsätta vara högt de närmaste åren. Det kommer främst att rikta sig mot kommersiella mål, militära mål, teknik, forskning och utveckling och mot människor som sökt fristad i Sverige. Statliga antagonister kommer också fortsatt försöka att påverka svenska politiska ställningstaganden såväl som bilden i det egna landet av ett Sverige i förfall. Det finns också en fortsatt avsikt och förmåga att använda våld mot regimkritiker som tagit sin tillflykt till Sverige.

2.2 Icke statliga aktörer

Det finns även icke statliga antagonister. Säkerhetspolisen pekar ut tre områden: de våldsbejakande högerextremistiska, vänsterextremistiska, och islamistiska miljöerna. Dessa grupperingar fokuserar på systematiskt våld eller hot och trakasserier mot politiker, journalister och myndighetsföreträdare, allt med syfte att minska förtroendet mot politiker, journalister och myndigheter.

Inom samtliga tre extremistmiljöer ser Säkerhetspolisen individer som utgör ett hot på lång sikt mot Sverige genom att de ägnar sig åt olika typer av stödverksamhet, som till exempel finansiering av terrorverksamhet, radikalisering och rekrytering. Stödverksamheten ökar tillväxten och handlingsutrymmet för personer inom våldsbejakande extremistmiljöer, vilket i sin tur påverkar attentatshotet.

Icke statliga aktörer runt om i Europa har sporadiskt visat intresse för kärnkraftverk men i Sverige finns inga tecken på att elförsörjningen skulle vara ett mål. Ideologiskt drivna antagonister har intresserat sig för elförsörjningen. Förmågan hos både statliga och icke statliga antagonister kan variera mellan olika grupper och över tid.

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 och sabotage.

3 Omvärldsbevakning

3.1 Norden

De nordiska ländernas säkerhetstjänster har alla lyft upp de högerextrema extremisterna som en av de grupperingar som växt mest under åren. SKYPO (Finland) skriver i sin årsbok för 2021 [2]:

Hotet om högerextrem terrorism har ökat i vårt land. Skyddspolisen har identifierat högerextrema aktörer med förmåga och motivation att genomföra terrorattentat. Det har också upptäckts tecken på konkreta förberedelser.

Noterbart är att både Norge och Finland i sina årsböcker har presenterat att skyddet mot kritisk infrastruktur ska höjas. Den finska säkerhetspolisen (SKYPO) ser att den kritiska infrastrukturen och hoten mot den blir allt mer komplexa. Det går att skaffa sig kontroll över sådan infrastruktur exempelvis genom ägarförhållanden. Därför har SKYPO genom sina nya befogenheter fått bättre möjligheter att följa och förhindra spioneri och påverkan i anslutning till ekonomisk aktivitet.

I Sverige har det under de senaste åren varit många uppmärksammade fall av informationsinsamling avseende skyddsvärden. Flera av dessa presenteras i Säkerhetspolisens årsbok. Ett av de mer uppmärksammade fallen är rättegången där flera män dömdes till ett års fängelse vardera för att under flera års tid ha kartlagt militära skyddsobjekt runt om i landet. Om uppgifterna hade röjts och andra länder fått kännedom om försvarshemligheterna, hade det inneburit en kännbar skada för Sveriges säkerhet, anser en enig tingsrätt. Det hade exempelvis kunnat bidra till att ett annat land hade kunnat slå ut försvarsanläggningar i Sverige vid en krigssituation. Alla länder runt Sverige har noterat liknande typ av informationsinsamling.

[2] Skyddspolisens årsbok 2020: Den förändrade lägesbilden i fråga om extremhögern märks i terrorhotbedömningen

Slutligen är det värt att nämna är att alla länderna de senaste åren väckt åtal mot personer som anses ha en koppling till terrorism. I Danmark åtalades och dömdes en man till 12 år i fängelse och utvisning för planering av en terroristattack i Köpenhamn [3]. I Norge har flera personer blivit dömda för hjälp till terrororganisation. Under de senaste åren i Sverige har det väckts åtal och fallit domar mot personer som offentligt uppmanat, rekryterat och utbildat med avsikt att utföra terroristbrott. Det finns även svenska medborgare som har deltagit i terroristbrott utomlands.

NATO

Under maj 2021 framkom det att den amerikanska underrättelsetjänsten NSA med hjälp av Danmark spionerat på ledande politiker och höga tjänstemän i Sverige.

Avslöjandet bygger på information från nio olika källor som alla ska ha haft tillgång till hemligstämplad information från danska underrättelsetjänsten. Alla uppgifter ska vara bekräftade av flera av varandra oberoende källor. Majoriteten av källorna bekräftar för Danmarks Radio att svenska politiker och höga tjänstemän var ett mål för spionaget. Det ska inte, via källorna, ha varit möjligt att få svar på hur många svenska politiker eller tjänstemän det rör sig om eller deras namn. Det framkom att NSA även spionerat på toppolitiker i Tyskland, Frankrike och Norge.

Kort efter detta framkom det även att NSA har bedrivit spionage mot SAAB från en bas i Danmark. Flera källor har pekat ut det svenska Gripen programmet som mål för avlyssningen.

Sverige är inte en fullvärdig medlem i NATO men tillhör de länder som samarbetar inom ramen för Partnerskap För Fred (PFF). I och med partnerskapet deltar Sverige bland annat i de årliga militärövningarna. Syftet med dessa är att förbättra samarbetet mellan förband från olika länder, vilket är nödvändigt för att gemensamma fredsfrämjande insatser ska bli effektiva. Ryssland bedöms ha på sin agenda att förhindra att Sverige blir fullvärdiga medlemmar i NATO.

[3] PET – Annual report 2109

3.2 Europa

Storbritannien
Direktören för MI5 General Ken McCallum lyfte i sitt årliga tal (2021) vilka hot som finns mot Storbritannien och även tryckte på vikten av att öka sitt säkerhetsskydd på grund av utvecklingen i världen [4]. Likt de nordiska länderna lyfter även McCallum det ökade hotet från högerextrema grupper. Diskussionen kring statliga antagonisterna landar precis som för Sverige på Ryssland. Salisburyhändelsen[5] där två personer, varav en avhoppad KGB agent, utsattes för nervgift ökade spänningen mellan västmakterna och Ryssland återigen. Denna händelse ledde till den största utvisningen av diplomater under modern tid. Närmare ett nytt kallt krig har man inte varit konstaterade McCallum.

Ryssland
Ryssland är den statliga aktören med en antagonistisk avsikt som skulle kunna få störst konsekvenser för Sveriges säkerhet. Svensk teknologi och vetenskap är av säkerhetspolitiskt intresse för Ryssland, samt kartläggning av kritisk infrastruktur. Att öka kunskapen om Sveriges totalförsvarsplanering och militära förmåga är också av intresse [6].

Sverige är en del av Östersjöregionen som är militärt, ekonomiskt och säkerhetspolitiskt viktig för Ryssland. Därför är målet för Rysslands aktiviteter mot Sverige att verka för att Sverige ska vara alliansfritt och hållas utanför försvarsalliansen Nato.

Ryssland använder kontinuerligt en rad metoder under tröskeln för en väpnad konflikt. Det handlar om att få Sveriges och andra länders politiska, och ekonomiska samarbeten samt försvarssamarbeten att försvagas.

Ryska statskontrollerade medier förmedlar också en bild av Sverige som ett land i kaos och förfall, bland annat för att stärka den ryska regimens ställning hos den egna befolkningen.

Den ryska regimens politiska fortlevnad är högt prioriterad hos det ryska ledarskapet. Genom underrättelseofficerare med diplomatisk täckmantel rekryterar Ryssland agenter som spionerar mot Sverige. Var tredje rysk diplomat i Sverige bedöms vara underrättelseofficerare som verkar under just diplomatisk täckmantel[6].

4 Director General Ken McCallum gives annual threat update 2021 | MI5 - The Security Service
5 Två personer utsatta för okänt ämne utanför Salisbury - Nyheter (Ekot) | Sveriges Radio
6 Säkerhetspolisen – Hotbild mot säkerhetskänslig verksamhet Juni 2019

En mer detaljerad bild av Rysslands metoder återfinns i den Estländska årssammanfattningen [7].

Under rubrik 6.6 Gråzon och hot mot Sveriges totalförsvar beskrivs det några händelser som belyser dessa hot.

3.3 Övriga världen

Kina
Kinas deklarerade ambition är att öka sitt globala inflytande och nå en ställning som stormakt; militärt, ekonomiskt och politiskt. I takt med att den kinesiska ekonomin växer, ökar även den kinesiska statens behov av underrättelser i syfte att stödja dessa intressen.

Kina har både avsikt och förmåga att försvaga och begränsa Sveriges handlingskraft, i de fall svenskt agerande uppfattas som ett hot mot kinesiska intressen. Sverige ligger geografiskt långt från Kina, men tydligt inom den kinesiska intressesfären vad gäller Kinas långsiktiga militära, ekonomiska och politiska mål.

Kinas ekonomiska planer är tydligt kopplade till landets säkerhetspolitiska mål. Kina söker aktivt information om teknologi och kunskap som finns och utvecklas i Sverige. Det kan till exempel handla om industrispionage och strategiska uppköp av svenska energi- och teknikföretag för att uppnå Kinas femårsplaner. Kinesiskägda företag är enligt kinesisk lag skyldiga att dela med sig av teknologi och kunskap till landets civila och militära underrättelsetjänster. Detta har även uppmärksammats i den dom där förvaltningsrätten fastställde PTS begäran avseende att användande av Huwaei produkter i det svenska 5G nätet inte skulle tillåtas [8].

Det förekommer att den kinesiska staten nyttjar kinesiska medborgare vid svenska högskolor och universitet i syfte att inhämta teknik och kunskap som ökar den kinesiska militära förmågan samt förståelse för den svenska elsektorn. Det finns även ett kinesiskt intresse mot andra svenska sektorer, utöver industrispionage och strategiska uppköp.

Säkerhetspolisen har sett hur det kinesiska underrättelsehotet har breddats och fördjupats för att nu omfatta även cyberspionage, strategiska uppköp och påtryckningar eller hot mot bland annat svenska politiska beslutsfattare, forskare och offentliga personer. Likt ryska underrättelseofficerare agerar även kinesiska

[7] INTERNATIONAL SECURITY AND ESTONIA 2021
[8] Tillämpning av lagen om elektronisk kommunikation – Förvaltningsrätten Mål: 24231-20

underrättelseofficerare under diplomatisk täckmantel i Sverige. Även journalistisk täckmantel används av kinesisk underrättelsetjänst

Iran
För Iran handlar det till exempel om att kartlägga regimkritiker och mål i Sverige kopplade till oppositionella grupper som av Iran bedöms vara eller kunna vara regimdestabiliserande.

I en internationell kontext finns flera exempel på hur den iranska ledningens agerande utgjort fara för liv och hälsa för personer. Planering och förberedelser för detta har bedrivits i Sverige. Iran bedriver också industrispionage som främst riktas mot svensk högteknologisk industri och svenska produkter som kan användas i kärnvapenprogram. Iran lägger stora resurser på detta och en del av resurserna används i Sverige.

Beskrivningen av hoten från Ryssland, Kina och Iran är hämtade i delar eller i sin helhet från Säkerhetspolisens årsbok 2020.

Afghanistan
De amerikanska trupperna började dra sig tillbaka från Afghanistan under maj 2021, samtidigt så började talibanerna och deras allierade militanta grupper sin militära offensiv. Talibanerna vann snabbt mark och 21 juli stod halva Afghanistan under talibanernas kontroll. Den 30 augusti så drog sig de sista amerikanska trupperna sig tillbaka från Afghanistan och under september så presenterade talibanerna sin regering.

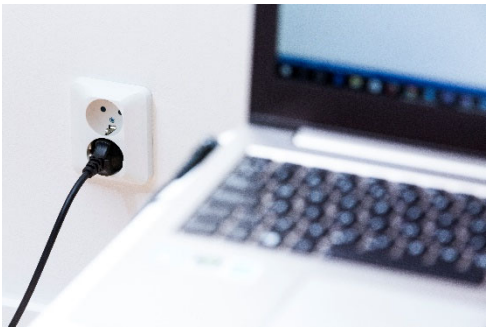
Säkerhetspolisen bedömer visserligen inte i dagsläget att det som nu skett i Afghanistan ökat attentatshotet på kort sikt i Sverige, men hur det påverkar hotet på lång sikt är det för tidigt att säga något om. De våldsbejakande extremistmiljöerna påverkas av sådana här händelser på flera olika sätt. Risken för terrorresor från Sverige till Afghanistan finns på lång sikt.

3.4 Covid-19

Covid-19 har präglat 2020 och större delen av 2021 och kommer med all trolighet att göra det ett tag framöver också. Man kan inte se varken ett ökat eller ett minskat antal terrorattacker under 2020. Däremot så kan man se att extremisterna utnyttjade pandemin för att bygga upp en mycket större närvaro på internet.

En ökning av intresset för att köpa säkerhetskänsliga företag som drabbats hårt av pandemin är också en trend som noterats. Läs mer om detta under 6.5 Leverantörskedjor och underentreprenörer.

Nedstängningarna på grund av pandemin och att färre platser för folksamlingar, såsom shoppingcentra, kyrkor, konsertlokaler och idrottsarenor funnits tycks ha lett till att användningen av sprängmedel vid terrorattacker minskat.



Med den ökade användningen av internet under pandemin har grupper och nätverk i sociala medier spelat en viktig roll för att sprida våldsam extremism. Efter insatser från meddelandeappar, såsom Telegram, för att blockera terrorgrupper, spreds jihadistpropagandan istället över flera, ofta mindre onlineplattformar. Högerextremister, särskilt unga, använde i högre utsträckning dataspel och spelplattformar för att sprida sin ideologi.

Både jihadister och högerextremister har försökt utnyttja coronapandemin för propagandasyften, medan vänsterextremister och anarkister integrerade kritik mot myndigheternas agerande i kampen mot pandemin i sina narrativ [9].

I Europa har en uppgång i cyberrelaterade brott rapporterats under pandemin. Den internationellt rapporterade uppgången i cyberrelaterade brott speglas inte i antalet inrapporterade brottsanmälningar i Sverige. Det går inte heller att belägga en uppgång i antalet inträffade incidenter, utifrån den rapportering som inkommit till MSB. Utifrån rapporteringen har varken antalet incidenter i stort eller antalet incidenter som orsakas av antagonistiska handlingar ökat under perioden.

Det finns dock ett stort mörkertal över cyberrelaterade brott i Sverige, och det har troligen ökat under pandemin [10].

[9] European Union Terrorism Situation and Trend report 2021 (TESAT)
[10] Säkerhetspolisen – Cybersäkerhet i Sverige – I skuggan av en pandemi

4 Terrorhotbedömning

4.1 Europa

Enligt Europols rapport 2021 om terrorförekomsten inom EU [11] skedde 57 försök till attacker i EU under 2020, jämfört med 55 under 2019. Siffran inbegriper lyckade, misslyckade och avvärjda försök. Av de 57 försöken var 10 attacker jihadistattacker i Österrike, Frankrike och Tyskland. Även om de bara utgör en sjättedel av alla attacker inom EU orsakade jihadistattackerna mer än hälften av alla dödsfall.

Totalt 14 etno-nationalistiska eller separatistiska attacker utfördes i antingen Frankrike eller Spanien, medan 24 attacker utfördes av vänsterextrema eller anarkistiska terrorgrupper eller individer, alla i Italien. I de flesta fallen riktade dessa attacker sig mot privata eller offentliga fastigheter, såsom finansinstitutioner eller myndighetsbyggnader.

År 2020 utsattes tre medlemsländer (Tyskland, Belgien och Frankrike) för totalt fyra terrorförsök utförda av högerextremister. Bara ett av dessa slutfördes.

Varje land bedömer terrorhotet separat, under rubriken nedan så finns den bedömning som just nu gäller för Sverige.

4.2 Sverige

Historiskt sett har Sverige varit relativt förskonat från terroristdåd jämfört med många andra länder. Sedan 1900 så har det skett ett tiotal dåd. Det har skett ett flertal attacker i modern tid, varav den senaste är en av de värsta. Fyra människor dödades på Drottninggatan i Stockholm. Bara vid ett tillfälle har fler människor dött i en terrorattack i Sverige - vid attentatet mot tidningen Norrskensflamman 1940 då fem personer omkom.

Terrorhotet mot Sverige 2021

Nationellt centrum för terrorhotbedömning (NCT) är en permanent arbetsgrupp med personal från Säkerhetspolisen, Försvarets radioanstalt (FRA) och Militära underrättelse- och säkerhetstjänsten (Must). Uppgiften är att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen på kort och lång sikt.

[11] Europol har sammanställt och bedömt terrorhotet för Europa i sin årliga TESAT rapport

Det sammantagna terrorhotet mot Sverige utgör ett förhöjt hot (3) på en femgradig skala [12]. Inom ramen för denna hotnivå ryms att terrorattentat kan ske under 2021[13].

I NCT:s rapport terrorhot mot Sverige 2021 står att läsa:

Den våldsbejakande högerextremistiska miljön och den våldsbejakande islamistiska miljön utgör de främsta terrorattentatshoten mot Sverige. Inom dessa extremistmiljöer kommer det under 2021 möjligen finnas ett fåtal personer som utvecklar avsikt och förmåga att utföra ett terrorattentat i Sverige. De flesta attentat i västvärlden har sedan ett antal år utförts av ensamagerande individer som på eget initiativ inspireras och utvecklar attentatsavsikt och därefter planerar samt genomför ett terrorattentat. Det är troligt att denna trend kommer fortsätta även under 2021. Om ett terrorattentat genomförs i Sverige under 2021 kommer det troligen utföras av en ensamagerande gärningsperson eller mindre grupp av likasinnade med hjälp av lättillgängliga medel

Sveriges grannländer
Det kan vara intressant att se över de svenska grannländernas bedömning av terrorhotsnivå då den överförbara hotnivån från Sveriges grannländer inte kan ignoreras vid landsgränserna.

Den danska säkerhetspolisen PET har bedömt terrornivån som significant, vilket betyder att det finns ett känt hot som har kapacitet, intention och där det även försiggår planering. Significant är den näst högsta nivån av fem nivåer [14].

Den norska säkerhetspolisen PST, har bedömt terrorhotet mot Norge som Moderat. Moderat är nivå 3 på en femgradig skala. Definitionen av nivå 3 är att en eller flera aktörer kan ha intention och vilja att genomföra terrordåd i Norge [15].

Den sista bedömningen görs av SKYPO den finska säkerhetspolisen. I Finland ligger terrorhotet på nivå 2 – förhöjt hot, av 4 [16]. Denna bedömning kan jämställas med den som är gjord i Norge.

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 [16].

[12] I Sverige används en femgradig skala för att ange hotnivå och nivåstegen är följande: inget identifierat hot (1), begränsat hot (2), förhöjt hot (3), högt hot (4) och mycket högt hot (5). Säkerhetspolischefen beslutar om hotnivån i Sverige.
[13] NCT Nationellt centrum för terrorhotbedömning – helårsbedömning 2021 - sammanfattning
[14] CTA Center for terroranalyse Assessment of the terrorist threat to Denmar k March 2021
[15] https://www.pst.no/temasider/trusselnivaer/#TerrortrusselenniversectionTitleAnch
[16] Terrorhotbedömning - Supo

5 Hotbild för elförsörjningen

Det moderna samhället är starkt beroende av en väl fungerande energiförsörjning. Störningar och avbrott i försörjningen av el, bränsle, gas och värme kan leda till allvarliga konsekvenser, såväl för människors liv och hälsa som för samhällets funktionalitet. Energiförsörjningen kan påverkas av en rad faktorer, på kort och lång sikt – väderförhållanden, olyckor, tekniska fel, ändrade marknadsmässiga förutsättningar, politiska beslut, klimatförändringar eller direkta attacker. Vårt samhälle bygger på integrerade system av vital infrastruktur, viket ger komplexa utmaningar i flera led. Elförsörjningen är en central komponent i samhället och störningar kan snabbt få konsekvenser inom andra verksamheter, såsom informations- och kommunikationsteknologi samt transportsystemet. Robusta försörjningssystem för energi med en god förmåga att hantera eventuella störningar som kan uppstå, bidrar till att verksamheter inom bland annat livsmedelsförsörjning, informationsteknologi, telefoni, radio och tv kan fungera.

Attacker kan riktas mot kraftsystemet i syfte att destabilisera samhällets funktionalitet och försämra totalförsvarsförmågan. I förlängningen kan en antagonist vilja utöva inflytande på Sveriges utrikes- och säkerhetspolitiska agerande. 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.

5.1 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 funktion att de ska vara tillgängliga dygnet runt, för flera aktörer och från flera geografiska platser.

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 informationsinsamling och kartläggning.

Ytterligare angreppsätt kan vara att antagonisten får in en vilande närvaro i när-/produktionsmiljön. Till skillnad från ett direkt cyberangrepp ska en sådan operation inte märkas alls. Ett exempel på detta är den attack som utfördes mot transmissionsnätet i Ukraina. Där lyckades antagonisten plantera in skadlig kod för att nästan ett år senare kunna ta över fjärrstyrning av elstationer samt ge falsk driftinformation.

Ett ytterligare mål kan vara att stjäla värdefulla komponenter och utrustning som förvaras på anläggningsplatserna.

6 Antagonistiska hot mot elförsörjningen

Baserat på den övergripande hotbilden som presenteras under rubriken 5. Hotbild för elförsörjning lyfts under detta kapitel sex antagonistiska hot som anses vara de mest relevanta.

6.1 Cyberhot

De cyberhot som riktas mot Sverige är mångfacetterade och kan kopplas till flera olika typer av hotaktörer. I huvudsak utgörs dessa av statliga aktörer och kriminella grupper.

Statliga aktörer genomför cyberangrepp mot Sverige i syfte att exempelvis inhämta information som kan gynna det egna landets utrikes- och säkerhetspolitiska intressen, eller i syfte att stärka det egna landets ekonomi och företag genom företagsspionerі. Cyberkriminalitet syftar i de allra flesta fall till att tjäna pengar och de ideologiskt motiverade aktörerna agerar i enlighet med sina egna formulerade agendor.

Cyberangrepp från statliga aktörer i syfte att inhämta underrättelser pågår ständigt mot svenska mål. De angriper bland annat verksamheter som hanterar känslig eller skyddsvärd information som rör Sveriges säkerhet.

Lösenordsattacker
Angripare har tillskansat sig lösenord sedan datorsystem kunde kopplas upp med modem på det sena 1980- talet. Dessa metoder fortsätter än idag att användas med stor framgång. Särskilt vanligt är det med lösenordsattacker mot publikt tillgängliga e-postservrar, databaser och tjänster för exempelvis fjärrstyrning (Remote Desktop Protocol, RDP) och Virtual private network (VPN-anslutningar). Phishingmail kan även ha som mål att anskaffa angriparen lösenord genom exempelvis falska inloggningssidor.

Angrepp via e-post
Att använda e-post för att genomföra angrepp kallas nätfiske (phishing) eller, i de fall angreppet är riktat mot en eller ett fåtal individer, riktat nätfiske (spearphishing). Syftet med denna metod är att få en användare att agera på ett sätt som hjälper angriparen. Detta sker genom att angriparen skickar e-postmeddelanden som ska verka legitima och på så sätt får användaren att klicka på en länk i meddelandet, öppna ett bifogat dokument eller tillåta innehåll i e-postmeddelandet, exempelvis en bild, att hämtas från internet. Gör användaren något av detta hjälper det angriparen på något sätt att uppnå sitt syfte.

Ransomware
Ransomware går även under benämningarna utpressningsprogram, utpressningsvirus, gisslanprogram och gisslanvirus. Detta är en typ av skadlig programvara vars syfte är att utpressning, genom att ta filer som gisslan via kryptering. För att kunna häva krypteringen eller återfå kontrollen över datorn kräver utpressningsprogrammet en lösensumma eller handling som gynnar antagonisten som ligger bakom programmet. längre fram i avsnittet presenteras ett tydligt exempel på när ransomware har använts.

Spearphising
Ett spearphishingangrepp inkluderar personliga detaljer som exempelvis ett namn eller referenser till något som är av intresse för mottagaren och skickas vanligtvis till ett begränsat antal mottagare. Detta kräver att hotaktören har kartlagt organisationen eller personen för att kunna utforma ett riktat angrepp. De kan även handla om att lura offret att lämna ifrån sig lösenord via förfalskade inloggningssidor. Den aktuella händelsen som presenteras är ett tydligt exempel på när ransomware har använts.

Hot mot elförsörjningen
Det en antagonist vill komma åt via ett cyberangrepp är information om anläggningar, it-system, sårbarheter i elförsörjningen och personer i kritiska funktioner som kan vara mål för informationsinsamling och kartläggning. Även tillgång till it-system som styr driften av anläggningar och system är mål för en antagonist. Viljan kan dels vara att använda sin nya förmåga direkt, dels att kunna bygga en dold närvaro genom ett brohuvud hos motståndaren.

De statliga aktörerna har stora resurser och intentioner att kunna påverka svensk elförsörjning genom cyberangrepp.

De icke statliga aktörerna har även de resurser och intention att komma åt information för att främst utöva utpressning mot den utsatta parten.

Aktuella händelser
En av de största cyberhändelserna 2021 var den it-attack som Coop blev utsatt för. Attacken kunde kopplas till att aktören hade angripit det amerikanska mjukföretaget Kaseya för att sedan attackera andra företag. Tusentals företag världen över antas vara drabbade av händelsen. För Coop betydde detta att runt 800 butiker var tvungna att stänga på grund av problem med betalningssystemet.

Mjukvaruföretaget Kaseya som säljer it-tjänster till mängder av kunder världen över ska ha utsatts för en omfattande ransomware-attack. En ransomwareattack kan exempelvis göras möjlig genom oförsiktighet av hantering av bilagor i e-post. Hackarna krävde 70 miljoner dollar för att häva attacken. Det är idag oklart exakt vilka som stod bakom attacken och om det fanns en statlig aktör som stödde aktionen.

En lärdom från denna händelse är att ha starka krypteringslösningar och redundanta lösningar på viktiga system. Personalens säkerhetskännedom kring dessa typer av attacker och hur de går till väga är en nyckelkomponent för att förhindra ransomware genom exempelvis e-post.

6.2 Fysisk skadegörelse

Explosivämnen har blivit åtråvärda för kriminella och stölder sker bland annat på byggarbetsplatser där sådana ämnen förvaras. Nationella bombskyddet ser en trend med kraftigare sprängladdningar och att sprängningar sker även i mindre städer.

Ideologiskt motiverade brott begås utifrån politiska skäl eller religiös övertygelse och kan vara kopplat till en konflikt, en sakfråga eller en situation som uppfattas som orättvis. Inom elförsörjningen så har historiskt sett kärnkraften varit utsatta för skadegörelse från denna typ av antagonister. Frågor kring upplåtelse av mark för uppförande av transmissionsnätsstationer och vindkraftverk har väckt missnöje och lett till skadegörelse.

Den vanligaste formen av fysisk skadegörelse på anläggningsområden är dock de som kommer av inbrott eller mindre skadegörelse.

Hot mot elförsörjningen

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 och stöld. Kriminella aktörer kan försöka stjäla material som är enkelt att sälja vidare så som maskiner eller koppar.

Aktuella händelser

Stölder och inbrott på anläggningar kopplade till elförsörjningen sker återkommande runt om i landet. Oftast som ovan nämnt för att få tillgång till material som är enkelt att sälja vidare. Skadegörelse för att visa missnöje förekommer också, och det kan inte uteslutas att den skadegörelsen kan drabba viktiga komponenter på ett anläggningsområde.

Ett starkt fysiskt skydd kring det som är skyddsvärt är det främsta skyddet mot denna typ av händelser. Brister i det fysiska skyddet ger aktörerna en möjlighet.

6.3 Informationsinsamling

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 eller, 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.

Informationsinsamling avseende Sveriges skyddsvärden pågår ständigt av både statliga och icke statliga aktörer.

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). En kartläggning av skyddsvärda tillgångar inom elförsörjningen kan blotta vilka kritiska beroenden som finns och var man skulle kunna planera en attack där den skulle göra störst skada.

De senaste åren har insiderproblematiken blivit mer framträdande. En insider kan definieras som en person som oftast frivilligt väljer att arbeta för ett annat lands underrättelsetjänst. Den statliga antagonisten tar kontakt och använder sig av den så kallade värvningstrappan (mer detaljerad information om denna återfinns bland annat i Säkerhetspolisen årsbok eller på deras hemsida). Det ska noteras att statliga antagonister kan lägga mycket pengar och lång tid på att värva en person som kan agera som insider för att på detta sätt kunna läcka information eller ge tillgång till system de annars inte hade kunnat få tillgång till.

Aktuella händelser

Tingsrätten har under senaste året dömt en man hemmahörande i Kristianstadstrakten till sex månaders fängelse för att på ett internetforum ha publicerat uppgifter om militära skyddsobjekt.

Det var under perioden september 2015 till juni 2016 som mannen publicerade hemliga uppgifter om elva försvarsanläggningar på internetforumet LS-tornet. Tingsrätten har kommit fram till att det skulle medföra betydande men för Sveriges säkerhet om andra länder fick del av uppgifterna. Brottet har bedömts

som grovt eftersom de hemliga uppgifterna rört förhållanden av stor betydelse för Sveriges försvar. Tingsrätten dömde mannen till sex månaders fängelse [17].

En annan händelse som är värd att lyfta är en 47-årig man som dömdes till tre års fängelse för att ha spionerat inom svensk fordonsindustri.

Mannen misstänks ha träffat en rysk diplomat under flera års tid för att överlämna uppgifter. Informationen ska ha kommit från mannen under tiden som han arbetade som konsult för Scania.

"*Tingsrätten har kommit fram till att mannen kopierat hemlig information från både Volvo och Scania och överfört denna på bl.a. USB-minnen som han sedan överlämnat till den ryske ambassadtjänstemannen samt att han varit fullt medveten om att de uppgifter han lämnat skulle komma Ryssland till del*", står det i tingsrättens dom.

Den 47-årige mannen är civilingenjör och har arbetat som konsult för Volvo personvagnar under 2016-2017 och från februari 2018 till dess han greps den 26 februari 2019 för Scania. Mannen dömdes till tre års fängelse.[18].

Det första fallet visar på vikten än en gång av ett starkt fysiskt skydd samt av att i den mån det är möjligt skydda uppgifter om var ens skyddsvärden finns placerade.

Fallet med mannen som läckte information inifrån verksamheten hade kanske kunnat förhindras, om tjänsten varit placerad i säkerhetsklass med lämplig säkerhetsprövning. Den säkerhetsprövningsintervju som ingår i säkerhetsprövningen kan ge ett tydligt underlag för om en person är lämplig att arbeta i en säkerhetskänslig verksamhet.

17 Fängelse för grov obehörig befattning med hemlig uppgift – Kristianstad tingsrätt Mål: B 2562-09
[18] Konsult döms till tre års fängelse för spioneri - Sveriges Domstolar Mål: B 18657,20

6.4 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. Det finns två aktörer som utmärker sig inom detta område och det är 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. I Finland finns det exempel på utländska köp av mark och fastigheter nära anläggningar som kan ha strategisk betydelse för samhället och totalförsvaret [19].

Hot mot elförsörjningen

För elförsörjningens del kan detta handla om att en statlig aktör, eller personer med kopplingar till en statlig antagonist, köper mark- eller sjöområden eller fastigheter nära 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 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.

Aktuella händelser

Fortifikationsverket försökte 2017 köpa tillbaka Marinvarvet i Fårösund av en privatperson, men man kom inte överens om priset. Fortifikationsverket bedömde marknadsvärdet då som nu till 20 miljoner kronor

Istället såldes anläggningen till företaget Artmax AB som ägs av en affärsman från Hong Kong, för en okänd summa pengar.
Artmax erbjöd sedan Fortifikationsverket att köpa hamnen för 62 miljoner kronor, vilket man tackade nej till.

Fastighets AB Bunge Kronhagen som nu sålt de tre fastigheterna Gotland Bunge Kronhagen till Fortifikationsverket där den kinesiska affärsmannens svenska företagssfär ingår.

Regeringen godkände affären, och Försvarsmakten har kunnat använda hamnen från och med den 30 april 2018 [20] .

19 SUPO – skyddspolisens årsbok 2020
20 Försvaret har köpt tillbaka ubåtshamnen i Fårösund | SVT Nyheter

I Sverige infördes från och med den 1 januari 2021 en komplettering till säkerhetsskyddslagstiftningen med nya bestämmelser som gäller överlåtelser av säkerhetskänslig verksamhet. Ett antal nya krav infördes som riktas mot den som vill sälja eller på annat sätt överlåta säkerhetskänslig verksamhet. Det betyder i praktiken att en säkerhetskänslig verksamhet får överlåtas och först om det bedöms som lämplig och har samrådts med ansvarig myndighet

6.5 Leverantörskedjor och underentreprenörer

Det privata näringslivet ansvarar alltmer för viktiga leveranser till säkerhetskänsliga verksamheter 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 kan planteras i kritiska komponenter som används inom elförsörjningen. Det går inte att utesluta att en kvalificerad angripare planterar avancerad skadlig kod i hårdvara som sedan köps in och används i samhällskritiska it-system, exempelvis i SCADA-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 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.

Hot mot elförsörjningen

Inom elförsörjningen finns ett stort beroende av entreprenörer och leverantörer för både byggnation, underhåll, reparationer och kritiska komponenter, även från utlandet. Det finns vissa leverantörer som tillhandahåller verksamhetskritiska tjänster/komponenter åt flera nordiska och europeiska systemoperatörer inom elförsörjningen. 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.

Aktuella händelser

Som nämnt tidigare i dokumentet så är Stockholms förvaltningsrätts dom avseende Post- och telestyrelsen (PTS) skäl för att förena tillstånd att använda radiosändare. Detta med villkor som förbjuder produkter från Huawei i centrala funktioner i svenska 5G-nät och som anger att befintliga produkter från Huawei ska vara avvecklade senast den 1 januari 2025. PTS har också haft skäl för villkoret att tillståndshavarna senast den 1 januari 2025 ska ha avvecklat beroenden av personal eller funktioner som är placerade i utlandet och, om nödvändigt, ersätta dessa med funktioner eller personal placerade i Sverige [21].

Förvaltningsrätten valde att döma till PTS fördel baserat på informationen om att Kina bedriver säkerhetshotande verksamhet mot Sverige. Den koppling Huawei har till den kinesiska staten och de underrättelselagar som finns gör att företag måste ge tillträde till och samarbete med den kinesiska underrättelsetjänsten. PTS anser att den kinesiska underrättelselagen innebär att den kinesiska staten kan utöva påtryckningar mot Huawei att vidta åtgärder mot Sverige och svenska 5G-nät.

Händelsen för med sig en lärdom även för elförsörjningen. Det är viktigt att för skyddsvärda system och komponenter vara noggrann i hela leverantörskedjan. Den säkerhetsskyddade upphandlingen med säkerhetsskyddsavtal (SUA) spelar stor roll för att visa på lämpligheten hos leverantörer.

[21] Tillämpning av lagen om elektronisk kommunikation – Förvaltningsrätten Mål: 24231-20

6.6 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 elnätet 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.

Aktuella händelser
Zapad 2021 är namnet på en storskalig rysk övning där det troliga övningsscenariot är att NATO samarbetar med ”terrorister” med mål att avsätta det ryssvänliga styret i Belarus.

Enligt ryska uppgifter deltar 200 000 soldater i övningen, men siffrorna får tas med en nypa salt då Ryssland kan överdriva antalet involverade i övningar. Övningen involverar både luft-, vatten- och markstridsövningar.

Flera länder deltar i övningen bland dessa återfinns Armenien, Belarus, Indien, Kazakstan, Kirgizstan, Mongoliet, Serbien, Sri Lanka och Tadzjikistan samt övervakas av observatörer från Kina, Myanmar, Pakistan, Uzbekistan och Vietnam.

Sverige har i och med övningen ökat sin närvaro på Gotland samt utökat sjöbevakningen. Försvarsmakten påpekar att bedömningen är att hotbilden fortfarande är oförändrad och att sannolikheten för väpnat angrepp på Sverige är låg.

Utöver denna storskaliga övning har Ryssland återkommande gånger kränkt svenskt territorium. Vid en av de senaste händelserna tog sig två ryska korvetter in på svenskt territorialvatten utanför Vinga, på Västkusten.

I MSB:s rapport Handlingskraft som kom ut i augusti 2021 beskrivs handlingsplanen för det svenska totalförsvaret [22]. I rapporten presenteras olika scenarier kopplade till elförsörjningen.

22 Handlingskraft – ”Handlingsplan för att främja och utveckla en sammanhängande planering för totalförsvaret 2021-2025

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 transmissionsnät 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