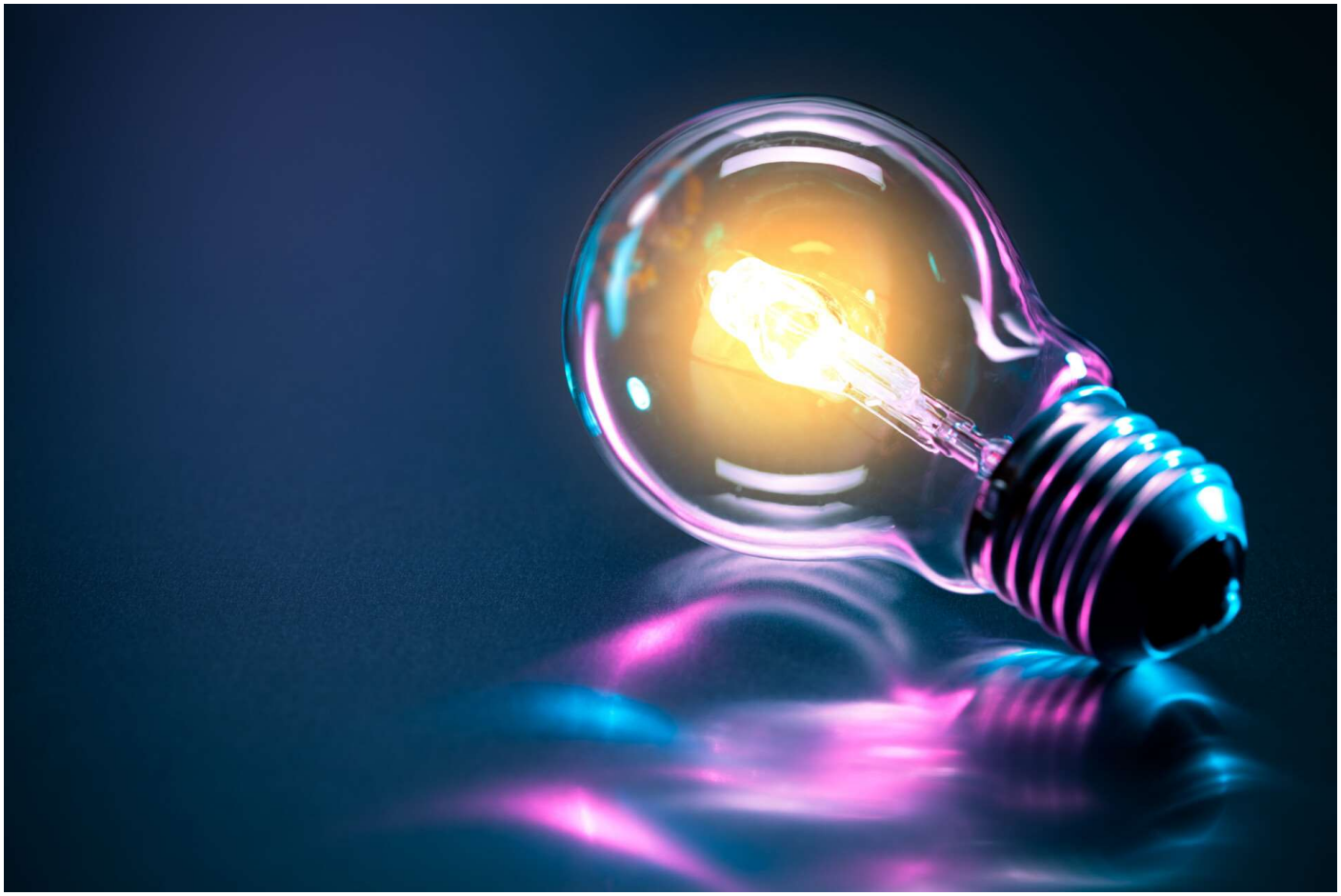
**Ärende nr:** Svk 2024/2196 **Datum:** 2024-05-15

# Öppen antagonistisk hotbild för svensk elförsörjning



SVENSKA KRAFTNÄT

# 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 1.0**
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

# Sammanfattning

Svenska kraftnät bedömer att de hot som svensk elförsörjning möter i grunden är av samma art idag som för några år sedan. Samtidigt är vissa av dem – som cyberhotet – i ständig förändring och det försämrade säkerhetsläget har gjort att vissa hot är än mer aktuella än tidigare. Dessutom har hotbilden fått större uppmärksamhet efter invasionen av Ukraina, vilket har lett till ökad medvetenhet om de hot som finns samt att större fokus riktas mot säkerhetsarbetet inom elförsörjningen, och vilka åtgärder som krävs för att öka säkerheten inom sektorn.

Den samlade bedömningen från underrättelsemyndigheterna är att hotbilden har blivit både mer allvarlig och mer komplex. Säkerhetspolisen påtalar också att läget kan försämras, och att det krävs beredskap för en sådan utveckling.

Enligt Säkerhetspolisen bedriver främmande makt systematiskt säkerhetshotande verksamhet mot Sverige inom ett stort antal områden, och myndigheten framhåller att Ryssland, Kina och Iran agerar allt mer offensivt för att nå sina mål.

Svenska kraftnät delar de svenska underrättelsemyndigheternas bedömning – de största hoten mot svensk elförsörjning kommer från Ryssland, Kina och Iran. Säkerhetspolisen lyfter särskilt det civila försvaret som ett målval för Rysslands informationsinhämtning, och då specifikt svensk energiförsörjning.

De främsta antagonistiska hoten som Svenska kraftnät ser gentemot svensk elförsörjning är, utan inbördes rangordning:

- Cyberhot
- Fysisk skadegörelse och sabotage
- Informationsinsamling
- Uppköp av fastigheter och mark
- Utkontraktering och osäkra leverantörskedjor
- Gråzonsproblematik och väpnat angrepp

Mål inom elförsörjningen för en antagonistisk aktör kan vara fysisk infrastruktur, it-infrastruktur, it-system, information (uppgifter) och personal. En angripare kan också välja att komma åt dessa mål genom leverantörer av varor eller tjänster som dessa mål är beroende av, exempelvis genom upphandlingar.

Genom denna öppna antagonistiska hotbild delar Svenska kraftnät en generell hotbild för elförsörjningen som helhet. Målet är att bidra till att utveckla säkerhets- och beredskapsarbetet inom svensk elförsörjning. Varje verksamhet behöver göra en egen analys av hotbilden mot den egna verksamheten och hur den påverkas av exempelvis kriget i Ukraina, det ökade terrorhotet eller Sveriges inträde i Nato.

En aktörs avsikt kan snabbt förändras, vilket gör att hotbilder är en färskvara. Svenska kraftnät uppmanar därför organisationer verksamma inom elförsörjningen att bevaka uttalanden från myndigheterna inom underrättelseområdet, exempelvis Säkerhetspolisen och FRA.

Verksamhetsutövare inom elförsörjningen bör också vara vaksamma på lägesbilden för sin egen verksamhet. Fokus behöver ligga på vad som utgör vardag, den så kallade normalbilden, och vad som avviker från denna. I det senare fallet bör man överväga att informera Säkerhetspolisen om det rör säkerhetskänslig verksamhet eller säkerhetsskyddsklassificerade uppgifter samt polisanmäla händelsen om den kan utgöra ett brott. Är det en anmälningspliktig händelse ska den alltid anmälas till Säkerhetspolisen. Information och anmälningar är avgörande för att Säkerhetspolisen ska kunna upprätthålla och förbättra sin lägesbild gällande hoten mot Sverige, inklusive mot elförsörjningen.

# Innehåll

# 1 Inledning

Svenska kraftnäts öppna antagonistiska hotbild presenterar hotbilden mot svensk elförsörjning i fredstid och gråzon. Svenska kraftnät har i framtagandet sammanställt flera öppna källor i syfte att dokumentera och analysera de hot som anses vara aktuella mot elförsörjningen. De öppna källorna innefattar främst publikationer från Säkerhetspolisen, Försvarets radioanstalt (FRA) och Nationellt centrum för terrorhotbedömning (NCT).

Rapporten är en uppdatering av den öppna antagonistiska hotbild som Svenska kraftnät publicerade 2021.[1] Vissa delar är i princip desamma, men flera delar är helt eller delvis uppdaterade eller omskrivna för att spegla de senaste årens händelser i omvärlden och för att hänvisa till mer aktuella källor.

Främsta förändringen är att Svenska kraftnät med den här revideringen lägger större tonvikt vid den komplexa hotbilden, och att olika antagonistiska aktörer i högre utsträckning tar hjälp av varandra. Att avgöra vem som bär ansvaret för olika händelser blir därmed svårare. Det ställer också högre krav på verksamhetsskyddet (som skyddar den egna verksamheten) som också därmed blir en än mer självklar förutsättning för ett fungerande säkerhetsskydd (skyddet för Sveriges säkerhet).

## 1.1 Syfte

Syftet med denna öppna antagonistiska hotbild är att dela en öppen och generell hotbild för elförsörjningen som helhet. Målet med detta är att bidra till att utveckla säkerhets- och beredskapsarbetet inom svensk elförsörjning. Den öppna antagonistiska hotbilden utgör underlag till Svenska kraftnäts risk- och sårbarhetsanalys som görs enligt 7 § förordning (2022:524) om statliga myndigheters beredskap.

## 1.2 Källor

I denna öppna hotbild för elförsörjningen beskrivs olika typer av antagonister, främst utifrån Säkerhetspolisens årsbok 2023/2024, FRA:s årsrapport 2023 samt Militära underrättelse- och säkerhetstjänstens (Must) årsöversikt 2023. För terrorhotnivåbedömningen används senaste rapporten från NCT från februari 2024. Ytterligare källor är bland annat Europol, Nationellt cybersäkerhetscentrum och Myndigheten för samhällsskydd och beredskap (MSB). Svenska kraftnät uppmanar alla aktörer inom elförsörjningen att ta del

[1] Svenska kraftnät (2021), *Öppen antagonistisk hotbild för elförsörjningen*, Svk2021/4367.

av dessa öppna underlag i sin helhet. Vidare har Svenska kraftnäts interna hotbild och hotbildsanalys bidragit i framtagandet. I slutet av rapporten finns en lista med de mest relevanta källorna.

## 1.3 Avgränsningar

Följande hotbild omfattar kända antagonistiska hot och ska inte uppfattas som heltäckande för alla hot mot elförsörjningen som kan förekomma. Den är inte heller avgränsad till att enbart röra säkerhetskänslig verksamhet, det vill säga vad som omfattas utifrån säkerhetsskyddslagen, även om det är utgångspunkten för Svenska kraftnäts arbete med hotbilden.

Hotbilden är generell för elförsörjningen. Den behöver anpassas för varje enskild aktörs verksamhet, vid behov i kombination med Säkerhetspolisens Dimensionerande antagonistiska förmågor (DAF)[2].

Svenska kraftnäts öppna antagonistiska hotbild omfattar inte hot under höjd beredskap och krig, då hotbilden kan innefatta ytterligare hot.

De nordiska och baltiska motsvarigheterna till de svenska underrättelsemyndigheterna publicerar också årsrapporter som är värda att läsa, men denna rapport omfattar inte en genomgång av dessa rapporter. Exempel på dessa rapporter återfinns i referenslistan.

## 1.4 Målgrupp

Målgruppen för den här hotbilden är aktörer inom elförsörjningen, men den kan även användas av exempelvis ägare av dammanläggningar. För att hotbilden ska vara tillgänglig för elförsörjningen är den öppen och baseras på öppna källor.

[2] För mer information om DAF, se https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/sakerhetsskyddsanalys/sakerhetshot-och-daf.html, 2024-03-20.

# 2 Hoten mot Sverige

## 2.1 Omvärldsläget

Alla svenska underrättelsemyndigheter beskriver i sina senaste årsöversikter det ökade militära hotet från Ryssland och kriget i Ukraina samt det ökade terrorhotet där Säkerhetspolisen i augusti 2023 höjde hotnivån.[3] Till detta läggs kriget i Gaza, den tekniska utvecklingen med främst AI och ett ökat fokus på rymden och Arktis. Från den 7 mars 2024 är Sverige även medlem av Nato.

Den samlade bedömningen från underrättelsemyndigheterna är att hotbilden har blivit både mer allvarlig och mer komplex. Säkerhetspolisen påtalar också att läget kan försämras, och att det krävs beredskap för en sådan utveckling.

Enligt Säkerhetspolisen bedriver främmande makt systematiskt säkerhetshotande verksamhet mot Sverige inom ett stort antal områden, och myndigheten framhåller att Ryssland, Kina och Iran agerar allt mer offensivt för att nå sina mål.

Svenska kraftnät noterar att cyberhotet inte lyfts fram lika tydligt i de senaste årsöversikterna, och tolkar det som att cyberhotet nu är en del av en ny normalbild för Sverige avseende det ständigt närvarande hotet från organiserad brottslighet och främmande makt. Detta bekräftas också av MSB:s årsrapport om it-incidentrapportering 2023, där en allt större andel av de rapporterade incidenterna orsakas av angrepp snarare än icke-antagonistiska händelser.[4]

### 2.1.1 Nato-medlemskap

I samband med Rysslands fullskaliga invasion av Ukraina 2022 ansökte Sverige, tillsammans med Finland, om medlemskap i Nato. Sverige blev fullvärdig medlem i Nato den 7 mars 2024. Ryssland meddelade i samband med Sveriges anslutning till Nato att de kommer vidta repressalier i form av politiska och militärtekniska åtgärder, något som skedde mot Finland i samband med deras inträde i Nato. Detta bestod bland annat av att Ryssland konstruerade migrantkriser vid gränsen mot Finland, sabotage mot undervatteninfrastruktur samt cyberattacker.[5] Ryssland har även uttalat att de

[3] De flesta är publicerade under våren 2024, se avsnitt 1.2 Källor.
[4] MSB (2024), *EU förändrar cybersäkerhetsområdet : årsrapport it-incidentrapportering 2023*, MSB2341, https://rib.msb.se/filer/pdf/30618.pdf, 2024-03-20.
[5] Brusman, Filip; Ågran Svedberg, Regina. *Finska Säpo-chefen: ”Ökade hot efter medlemskapet”*. 2024-03-08. https://www.svt.se/nyheter/inrikes/finska-sapo-chefen-okade-hot-efter-medlemskapet (Hämtad 2024-03-08)

ska stärka gränsen mot Finland och Baltikum i samband med att Finland och Sverige gått med i Nato.

Erfarenheter från finska Cybersäkerhetscentret (NCSC-FI) efter Finlands inträde i Nato visar att ransomware-attacker mot finländska organisationer har fyrdubblats sedan landet lämnade in ansökan om medlemskap. Ökningen av cyberincidenter tros vara kopplad till geopolitiska faktorer, men ledde dock inte till några offentligt synliga störningar.[6] Det svenska Nato-inträdet skulle kunna innebära en liknande utveckling i Sverige.

## 2.2 Antagonistiska aktörer

Antagonistiska aktörer delas ofta lite förenklat in i olika typer utifrån vilka motiv de har. Främmande makt är andra stater, som i princip motiveras av att befästa eller utöka sin makt. Våldsbejakande extremister drivs istället av ideologiska motiv, medan organiserad brottslighet söker ekonomisk vinning. Därutöver förekommer en blandning av dessa motiv, eller att antagonistiska aktörer använder varandra för att uppnå sina mål. Några antagonistiska aktörer beskrivs nedan. Nedanstående underlag är sammanställt utifrån Säkerhetspolisens årsbok 2023-2024[7] om inget annat anges.

### 2.2.1 Främmande makt

Såväl Säkerhetspolisen som FRA nämner särskilt tre stater som intresserar sig för säkerhetskänslig verksamhet i Sverige: Ryssland, Kina och Iran. Alla dessa tre stater bedriver enligt Säkerhetspolisen underrättelseverksamhet och säkerhetshotande verksamhet i och mot Sverige.[8] Detta utesluter inte att fler stater också är intresserade och bedriver motsvarande verksamhet.

***Ryssland*** är enligt Säkerhetspolisen den enskilt största hotaktören mot Sveriges säkerhet. Kriget i Ukraina har inneburit att det säkerhetspolitiska läget i Sveriges närområde har försämrats. Ryssland har en alltmer aggressiv hållning gentemot sina grannländer, vilket påverkar Sveriges närområde, i synnerhet Östersjöområdet.

---

[6] The Record (2023). *Finland sees fourfold spike in ransomware attacks since joining NATO, senior cyber official says*, https://therecord.media/finland-sees-fourfold-spike-in-rasomware-attacks-nato , först publicerad 2023-08-03.
7 Säkerhetspolisen (2024), *Säkerhetspolisen 2023-2024*, https://sakerhetspolisen.se/download/18.5cb30b118d1e95affec37/1708502268494/L%C3%A4gesbild%202023-2024.pdf, 2024-03-19.
[8] FRA (2024) *FRA Årsrapport 2023*, https://fra.se/download/18.27dd4df418cca16de4a2c0/1709120525079/FRA_arsrapport_2023_uppslag.pdf, 2024-03-19.

Rysslands underrättelseverksamhet i Sverige kompletteras även av att man bedriver påverkanskampanjer där man bland annat utnyttjar händelser man själv inte skapat, men väljer att dra nytta av.

Ryssland samlar in information och kartlägger säkerhetskänslig verksamhet och infrastruktur, vilket kan ingå i förberedelser för att kunna angripa Sverige i ett gråzonsläge.

***Kina*** arbetar långsiktigt och fokuserar enligt Säkerhetspolisen främst på att inhämta information om och påverka svenskt beslutsfattande, liksom att inhämta information om svensk forskning och utveckling. Till detta kommer även strategiska investeringar och uppköp där exempelvis FOI har uppmärksammat kinesiskt ägande av vindkraftsparker i Sverige.[9]

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 samband med ett beslut från Post- och telestyrelsen (PTS) om att inte tillåta Huawei-produkter i det svenska 5G-nätet, ett beslut som senare fastställdes i en dom i förvaltningsrätten[10].

Säkerhetspolisen har särskilt varnat för den strategiska underrättelseinhämtning som Kina ägnar sig åt på cyberområdet och som är riktad mot svenska intressen. Till viss del rör det sig om att hämta in kunskap om kritisk infrastruktur.

Kunskap om sårbarheter är särskilt intressant. Sedan hösten 2021 insamlar och hemlighåller kinesiska myndigheter med lagstöd dessutom en stor mängd nyupptäckta IT-sårbarheter, vilket lett till en markant nedgång av antalet publicerade IT-sårbarheter. Även västerländska tillverkare av IT-utrustning som är verksamma i Kina har krav på sig att medverka i detta.[11]

Amerikanska myndigheter har även varnat för att Kina på flera håll planterat dold programvara i -it-utrustning tillhörande amerikansk, kritisk infrastruktur.[12]

---

[9] Oscar Almén (2023) *Kinesiska investeringar i Sverige: en kartläggning*, FOI-R--5474--SE
[10] Förvaltningsrätten i Stockholm (2021), *Förbudet mot produkter från Huawei i svenska 5G-nät står fast*, Mål 24231-20 2378-21, https://www.domstol.se/nyheter/2021/06/forbudet-mot-produkter-fran-huawei-i-svenska-5g-nat-star-fast/, först publicerad 2021-06-22.
[11] Atlantic Council (2023), *Sleight of hand: How China weaponizes software vulnerabilities*, https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/, först publicerad 2023-09-23.
[12] Cyberstructure & Infrastructure Security Agency (2024), *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a, först publicerad 2024-02-07.

Säkerhetspolisen varnar även för att framför allt Kina använder it-system i Sverige, både hyrda servrar och hackade privatdatorer, som plattformar för cyberangrepp mot andra länder.

***Iran*** bedriver historiskt sett främst flykting- och industrispionage mot Sverige. Den iranska statens flyktingspionage i Sverige är i huvudsak riktat mot minoritetsgrupper som den iranska regimen uppfattar som ett hot. Enligt Säkerhetspolisen kan den iranska säkerhetstjänsten försöka utnyttja kopplingar till hemländerna för att förmå individer att bedriva underrättelseverksamhet mot svenska intressen, inklusive säkerhetskänslig verksamhet. Även på cyberområdet är den iranska regimen en kvalificerad hotaktör som enligt Säkerhetspolisen kan agera opportunistiskt om tillfälle ges.

### 2.2.2 Våldsbejakande extremism

Aktörer inom våldsbejakande extremism har ideologiska motiv, och använder våld eller hot om våld för att uppnå dessa motiv. Säkerhetspolisen pekar i regel ut tre grupperingar: våldsbejakande vänsterextremism, våldsbejakande högerextremism och våldsbejakande islamism.[13]

I augusti 2023 beslutade Säkerhetspolisen att höja terrorhotnivån i Sverige till nivå fyra på en femgradig skala, vilket innebär ett högt hot för terrorattentat.[14]

Hotet kommer i dagsläget enligt Nationellt centrum för terrorhotbedömning (NCT)[15] främst från ensamagerande individer inom våldsbejakande islamism eller våldsbejakande högerextremism, samt från individer med vad Säkerhetspolisen uttrycker som en mer blandad extremistisk ideologi, med inslag av konspirationsteorier och antistatliga budskap.[16]

Inom våldsbejakande extremism finns även våldsbejakande vänsterextremism. Denna typ av våldsbejakande extremism är inte omnämnd i varken NCT:s eller Säkerhetspolisens årsrapporter från våren 2024, men det innebär inte att de är irrelevanta för hotbilden mot svensk elförsörjning.

---

[13] https://sakerhetspolisen.se/hoten-mot-sverige/terrorism-och-extremism/valdsbejakande-extremism.html, Hämtad 2024-04-04.
[14] https://www.sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2023-08-17-hojning-av-terrorhotnivan-till-hogt-hot.html, 2024-03-19.
[15] Nationellt center för terrorhotbedömning (NCT) är en permanent arbetsgrupp med medarbetare från Säkerhetspolisen, Must och FRA som gör strategiska bedömningar av terrorhotet mot Sverige och svenska intressen utomlands.
[16] Nationellt centrum för terrorhotbedömning (2024), *Helårsbedömning 2024 – sammanfattning*, https://www.sakerhetspolisen.se/download/18.5cb30b118d1e95affe641/1707750097566/NCT%20Helarsbedomning%202024.pdf, 2024-03-19.

### 2.2.3 Organiserad brottslighet

Ett antal myndigheter[17] publicerar årliga lägesbilder gällande organiserad brottslighet. Det myndighetsgemensamma underrättelsearbetet som utgör grunden för dessa lägesbilder inriktas mot *strategiska personer, utsatta områden samt mot aktörs- eller fenomenbaserad organiserad brottslighet av allvarlig eller omfattande karaktär. Myndigheterna ska särskilt beakta möjligheterna att stödja samhällets samlade åtgärder för att motverka våldsbejakande extremism, terrorism, penningtvätt och brott mot välfärdssystemet*. I dessa myndigheters samarbete definieras organiserad brottslighet som minst två personer som varaktigt över tid begår allvarliga brott i samarbete i syfte att uppnå ekonomisk vinning.[18]

Den organiserade brottsligheten har historiskt sett handlat om exempelvis gängkriminalitet, narkotikahandel, bedrägerier och ekonomisk brottslighet. Numera handlar det också i allt större utsträckning om bland annat olika former av cyberkriminalitet, välfärdsbrottslighet (där kriminella utnyttjar samhällets välfärdssystem) samt avancerade internationella upplägg i den kriminella ekonomin. Den organiserade brottsligheten är enligt den gemensamma lägesbilden omfattande, multikriminell och mångfacetterad.

I den gemensamma lägesbilden lyfter myndigheterna särskilt hotet kring så kallad otillåten påverkan. Det definieras som *olika brottsliga och icke brottsliga tillvägagångssätt som syftar till att påverka det politiska beslutsfattandet, yttrandefriheten, rättsprocessen, att direkt eller indirekt påverka myndighetsutövning samt beslutsfattare inom det privata näringslivet*. I detta inkluderar myndigheterna även infiltration. Otillåten påverkan beskrivs som en pyramid enligt nedan.

[17] Arbetsförmedlingen, Ekobrottsmyndigheten, Försäkringskassan, Kriminalvården, Kronofogdemyndigheten, Kustbevakningen, Migrationsverket, Skatteverket, Säkerhetspolisen, Polismyndigheten, Tullverket och Åklagarmyndigheten.
[18] Arbetsförmedlingen et al. (2023), *Myndighetsgemensam lägesbild organiserad brottslighet 2023*, https://polisen.se/siteassets/dokument/organiserad_brottslighet/mgl-2023.pdf , 2024-03-20.


**Figur 1.** Otillåten påverkan. Hämtad från *Myndighetsgemensam lägesbild organiserad brottslighet 2023* (Arbetsförmedlingen).

Cyberkriminella aktörer drivs huvudsakligen av ekonomiska incitament och söker därmed största möjliga avkastning. Ofta föregås deras cyberattacker av gedigen kartläggning och förberedelser som anpassats efter måltavlans sårbarheter.[19]

### 2.2.4 Vem ligger bakom olika händelser?

När något händer är det sällan som man inledningsvis vet om det rör sig om ett attentat eller en olycka, än mindre vem som ligger bakom ett attentat. Ett vanligt tillvägagångssätt för främmande makt är enligt Säkerhetspolisen att använda sig av andra typer av antagonister för att utföra antagonistiska handlingar, i syfte att inte avslöja att de själva ligger bakom handlingen.

Statliga aktörer har generellt sett en hög uthållighet, i kombination med betydande resurser och kunskap. Denna typ av aktör kombinerar ofta flera olika syften och hotområden i sitt agerande för att sabotera, störa och förleda.[20]

Efter den ryska invasionen av Ukraina har Ryssland enligt Säkerhetspolisen i högre utsträckning börjat använda sig av ombud för underrättelseinhämtning. Detta främst eftersom det blivit svårare för Ryssland att använda sig av så kallade inresande, eller underrättelseofficerare som agerat under diplomatisk täckmantel.

[19] Nationellt centrum för cybersäkerhet (2022), *Cybersäkerhet i Sverige 2022 Del 1: Hot, metoder, brister och beroenden*, https://www.ncsc.se/siteassets/publikationer/ncsc-rappor-1-cybersakerhet-i-sverige-2022-hot-metoder-brister-och-beroenden.pdf, hämtad 2024-04-05
[20] Ibid.

NCT nämner specifikt att främmande makt kommer att kunna använda sig av icke-statliga aktörer som ombud för våldsutövning, eller på andra sätt utöva våld under täckmantel. NCT pekar särskilt ut Iran och Ryssland som användare av sådana metoder.[21]

I den senaste myndighetsgemensamma lägesbilden gällande organiserad brottslighet ges följande exempel på statsunderstödd kriminalitet: vapensmuggling, sanktionsbrott, skeninvandring, människoexploatering, påverkanskampanjer, samt att agera bulvan för köp av taktiskt eller strategiskt intressanta tillgångar (som exempelvis fastigheter i närheten av skyddsobjekt) eller köp av tjänster för cyberangrepp.[22]

Hacktivism har de senaste åren utvecklats från cyberkriminella kollektiv, till att övervägande bestå av statligt mobiliserade grupper som är mer organiserade, strukturerade och sofistikerade med målsättningen att förmedla ideologiska och politiska budskap.[23]

Inom cyberområdet har det under ett antal år varit ett etablerat förfarande att främmande makt använder sig av cyberkriminella för att dölja syftet med olika typer av attacker. Dels kan detta åstadkommas med hjälp av hackergruppers ideologiska hemvist, och dels genom betalning.

Ett exempel på det förra är enligt Europol den våg av överbelastningsattacker som skett efter Rysslands invasion av Ukraina mot olika europeiska mål. Attackerna har enligt Europol koordinerats av pro-ryska hackergrupper.[24]

Överbelastningsattackerna som utfördes av hackare som betecknat sig tillhöra grupperingen ”Anonymous Sudan” är ett exempel på vad som skulle kunna vara statsunderstödd kriminalitet eller hacktivism. Attackerna genomfördes mot svenska hemsidor och myndigheter som ett svar på koranbränningarna. Anonymous Sudan kan kopplas till ryska hacktivistgrupper, som stöttar den ryska geopolitiska agendan. Det som utmärker Anonymous Sudan och dess tillvägagångssätt är att man använt servrar i IBM:s molntjänst i Tyskland, vilket är en betaltjänst, snarare än kapade enheter. Detta tyder på att

[21] Nationellt centrum för terrorhotbedömning (2024), *Helårsbedömning 2024 – sammanfattning*, https://www.sakerhetspolisen.se/download/18.5cb30b118d1e95affe641/1707750097566/NCT%20Helarsbedomning%202024.pdf, 2024-03-19.
[22] Arbetsförmedlingen et al. (2023), *Myndighetsgemensam lägesbild organiserad brottslighet 2023*, https://polisen.se/siteassets/dokument/organiserad_brottslighet/mgl-2023.pdf , 2024-03-20.
[23] Wired (2022), Hacktivism Is Back and Messier Than Ever, https://www.wired.com/story/hacktivism-russia-ukraine-ddos/, först publicerad 2022-12-27.
[24] Europol (2023), *Internet Organised Crime Threat Assessment (IOCTA) 2023*, https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf, 2024-03-19.

Anonymous Sudan förfogar över finansiella medel som kännetecknar en nationalstat och som ”vanliga” aktivister och hackare saknar.[25][26]

Metoden att betala för attacker benämns ”crime-as-a-service”, där beställaren betalar en eller flera utförare. Flera mellanhänder kan också förekomma, då utföraren kan ha ”underleverantörer” för att genomföra olika delar eller olika typer av attacker.[27]

[25] Truesec (2023), *Anonymus Sudan – Threat Intelligence Report, daterad 2023-02-23, https://files.truesec.com/hubfs/Reports/Anonymous%20Sudan%20-%20Publish%201.2%20-%20a%20Truesec%20Report.pdf

[26] SVT (2023), Hackergruppen ”Anonymous Sudan” fick 61 servrar nedtagna: ”Stoppat dem temporärt”, Hackergruppen ”Anonymous Sudan” fick 61 servrar nedtagna: ”Stoppat dem temporärt” | SVT Nyheter, först publicerad 2023-02-23.

[27] Europol (2023), Europol spotlight – Cyber attacks – The apex of crime-as-a-service, https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf , 2024-03-19.

# 3 Hotbild för elförsörjningen

Svenska kraftnät bedömer att de hot som svensk elförsörjning möter i grunden är av samma art idag som för några år sedan. Samtidigt är vissa av dem – som cyberhotet – i ständig förändring och det försämrade säkerhetsläget har gjort att vissa hot är än mer aktuella än tidigare. Dessutom har hotbilden fått större uppmärksamhet efter invasionen av Ukraina, vilket har lett till ökad medvetenhet om de hot som finns samt att större fokus riktas mot säkerhetsarbetet inom elförsörjningen, och vilka åtgärder som krävs för att öka säkerheten inom sektorn.

Varje verksamhet behöver göra en egen analys av hotbilden mot den egna verksamheten och hur den påverkas av exempelvis kriget i Ukraina, det ökade terrorhotet eller Sveriges inträde i Nato.

## 3.1 Vilka hotar Sveriges elförsörjning, och hur?

Svenska kraftnät delar de svenska underrättelsemyndigheternas bedömning – de största hoten mot svensk elförsörjning kommer från Ryssland, Kina och Iran. Säkerhetspolisen lyfter särskilt det civila försvaret som ett målval för Rysslands informationsinhämtning, och då specifikt svensk energiförsörjning.

De främsta antagonistiska hoten som Svenska kraftnät ser gentemot svensk elförsörjning är, utan inbördes rangordning:

- Cyberhot
- Fysisk skadegörelse och sabotage
- Informationsinsamling
- Uppköp av fastigheter och mark
- Utkontraktering och osäkra leverantörskedjor
- Gråzonsproblematik och väpnat angrepp

Vilka hotaktörer som använder vilka metoder är inte alltid lätt att avgöra, då de kan ta hjälp av varandra, se kapitel 2.2.4 om vem som ligger bakom olika händelser. Utifrån hur underrättelsemyndigheterna resonerar är det främst organiserad brottslighet som använder olika former av cyberhot och fysiska sabotage, liksom att de utnyttjar utkontraktering och leverantörskedjor. Det sistnämnda utnyttjas systematiskt inom cyberbrottslighet. Åtminstone på cybersidan är det vanligt att främmande makt använder organiserad brottslighet som täckmantel, men det kan förekomma inom alla typer av brottslighet. Övriga tre hot i listan ovan härrör mer direkt till främmande makt.

Attacker från våldsbejakande extremism har elförsörjningen i Sverige hittills varit förskonad från. De attacker vi hittills sett i Sverige har riktats mot Sverige och svenskar i allmänhet, eller enskilda personer eller grupper, inte specifika mål inom svensk elförsörjning. Det utesluter inte att elförsörjningen drabbas av skadegörelse och sabotage utifrån missnöje, exempelvis inom ramen för elnätsutbyggnad.

Det närmaste elförsörjningen kommit ovanstående är att det förekommer olika typer av protestgrupper som motsätter sig elnätets utbyggnad. Det motståndet sker vanligtvis inom lagens och demokratins ramar och Svenska kraftnät bedömer att det inte är våldsbejakande. Det är dock tänkbart att det kan utnyttjas av främmande makt genom exempelvis påverkanskampanjer för att störa och fördröja planerade byggprojekt.

## 3.2 Mål inom elförsörjningen

Mål inom elförsörjningen för en antagonistisk aktör kan vara fysisk infrastruktur, it-infrastruktur, it-system, information (uppgifter) och personal. En angripare kan också välja att komma åt dessa mål genom leverantörer av varor eller tjänster som dessa mål är beroende av, exempelvis genom upphandlingar.

Fysisk infrastruktur eller it-infrastruktur kan angripas fysiskt eller via it-system, till exempel genom en cyberattack. It-system kan vara kritiska för elförsörjningen utifrån att informationen i dem ska vara korrekt och tillgänglig för att elförsörjningen ska kunna upprätthållas. Flera av dessa system är konstruerade och driftsatta innan dagens it-säkerhetskrav trädde i kraft. Nya säkerhetsåtgärder kan därför behöva tillföras systemen efter att de tagits i drift, vilket ofta är svårare än att ha säkerhetskrav med i arbetet när nya system tas fram och driftsätts.

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 it-system som utgör styrsystem för elnät eller elproduktion. Till skillnad från ett direkt cyberangrepp är syftet att en sådan operation inte ska 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 anläggningar i elnätet samt ge falsk

driftinformation.[28] Här går den tekniska utvecklingen snabbt framåt, där angripare i allt större utsträckning kommer kunna använda AI för att utveckla sin förmåga till allt mer avancerade attacker.[29]

Ett ytterligare mål kan vara att stjäla eller förstöra komponenter och utrustning som förvaras på anläggningsplatserna. Syftet kan vara ekonomisk vinning, men lika gärna att försöka sabotera arbetet, då reserv- eller byggmateriel kan vara en bristvara och ta lång tid att ersätta.

Utbyggnaden av det svenska elnätet innebär stora ekonomiska värden i omfattande upphandlingar, på en marknad med stor efterfrågan och där leverantörerna i dagsläget väljer vilka affärer som bäst passar deras verksamhet utifrån kapacitet och över tid.[30] Hög konkurrens om leverantörer snarare än uppdragen kan locka mindre seriösa budgivare då dessa ser en chans att vinna större kontrakt med lägre bud. Upphandlingar av större byggprojekt kan därmed utgöra en måltavla för organiserad brottslighet, i syfte att få del av dessa ekonomiska värden. Givet att främmande makt i högre utsträckning har börjat använda sig av ombud innebär det i förlängningen att upphandlingar av större byggprojekt kan komma att utnyttjas av främmande makt som en möjlighet att påverka svensk elförsörjning och inhämta information om det svenska elnätet.

Slutligen kan en antagonist välja att försöka utnyttja personalen (anställda eller konsulter) som arbetar inom elförsörjningen genom en så kallad insider. Det kan ske antingen genom att den som utnyttjas tvingas till det (utpressning) eller går med på det frivilligt, medvetet eller omedvetet.

## 3.3 Avsikt, förmåga och normalbild

Svenska kraftnät vill särskilt påpeka att hotbilden kan se olika ut beroende på vilken funktion eller vilket skyddsvärde som avses. Olika antagonistiska aktörer kan ha olika motiv och metoder beroende på vilka mål de riktar in sig på och vilka syften de vill uppnå.

En aktörs avsikt kan snabbt förändras, vilket gör att hotbilder är en färskvara. Svenska kraftnät uppmanar därför organisationer verksamma inom elförsörjningen att bevaka uttalanden från myndigheterna inom

[28] Wired (2016), *Inside the cunning, unprecedented hack om Ukarine's power grid*, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, först publicerad 2016-03-03.
[29] Europol (2023), *ChatGPT The impact of Large Language Models on Law Enforcement*, https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf , först publicerad 2023-03-27.
[30] Svenska kraftnät (2024), *Omvärldsanalys 2024*, Svk2024/738.

underrättelseområdet, exempelvis Säkerhetspolisen och FRA. Verksamhetsutövare inom elförsörjningen bör också vara vaksamma på lägesbilden för sin egen verksamhet. Fokus behöver ligga på vad som utgör vardag, den så kallade normalbilden, och vad som avviker från denna. I det senare fallet bör man överväga att informera Säkerhetspolisen om det rör säkerhetskänslig verksamhet eller säkerhetsskyddsklassificerade uppgifter samt polisanmäla händelsen om den kan utgöra ett brott. Är det en anmälningspliktig händelse enligt 2 kap 4 § säkerhetsskyddsförordningen (2021:955) ska den anmälas till Säkerhetspolisen.[31] Information och anmälningar till Säkerhetspolisen är avgörande för att Säkerhetspolisen ska kunna upprätthålla och förbättra sin lägesbild gällande hoten mot Sverige, inklusive mot elförsörjningen.

De antagonistiska aktörernas förmåga varierar, och som nämnts i tidigare kapitel samarbetar också dessa aktörer. Här ansvarar Säkerhetspolisen för att styra dimensioneringen av det fysiska skyddet för säkerhetskänslig verksamhet och för skyddet av säkerhetsskyddsklassificerade uppgifter genom sin publikation *Dimensionerande antagonistiska förmågor* (DAF). Publikationen är sekretessbelagd och delges de verksamheter som har säkerhetskänslig verksamhet, utifrån den grad av skada som ett angrepp mot verksamheten kan få, se nivåerna i 2 kap 5 § säkerhetsskyddslagen (2018:585) samt i 2 kap 5 § Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1).[32]

[31] För mer information, se https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/anmalan-vid-sakerhetshotande-handelser.html, 2024-04-30.
[32] För mer information, se https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/sakerhetsskyddsanalys/sakerhetshot-och-daf.html, 2024-03-19.

# 4 Antagonistiska hot mot elförsörjningen

Detta kapitel baseras på den övergripande hotbilden som presenterats under föregående kapitel. Hotbilden för elförsörjningen specificeras i detta kapitel till sex antagonistiska hot som anses vara de mest relevanta.

## 4.1 Cyberhot

I takt med ett alltmer digitaliserat samhälle ökar antalet cyberangrepp, globalt och i Sverige. Det främsta hotet bedöms komma från främmande makt och organiserad brottslighet, särskilt med anledning av det försämrade säkerhetspolitiska läget i vårt närområde och Sveriges inträde i Nato.

Hotaktörer inom cyberområdet har idag generellt en hög förmåga att skräddarsy och skapa komplexa cyberattacker, där samhällskritisk infrastruktur i allt högre utsträckning utgör en måltavla.[33]

För att komma åt system försöker hotaktörer identifiera och angripa den svagaste länken, vilket ofta kan utgöras av anställda såväl som dåligt skyddade tekniska system En indikation på den tekniska utvecklingen hos hotaktörer är AI-drivna attacker där angripare framöver väntas kunna använda AI och maskininlärning för att automatisera och förbättra sin kapacitet, vilket gör attackerna mer sofistikerade och anpassningsbara.[34]

Energisektorn och kritisk infrastruktur utsätts allt oftare för riktade cyberattacker. Ransomware och överbelastningsattacker (DDoS) är vanligt förekommande cyberhot mot svenska myndighetsidor, kommuner och företag.[35]

En vanlig möjliggörare för ransomware är social engineering-attacker i form av nätfiske (phishing), eller i de fall angreppet är riktat mot en eller ett fåtal individer, riktat nätfiske (spearphishing). Nätfiske som metod har utvecklats

[33] Nationellt centrum för cybersäkerhet (2022), *Cybersäkerhet i Sverige 2022 Del 1: Hot, metoder, brister och beroenden*, https://www.ncsc.se/siteassets/publikationer/ncsc-rappor-1-cybersakerhet-i-sverige-2022-hot-metoder-brister-och-beroenden.pdf, hämtad 2024-04-05
[34] Europol (2023), *ChatGPT The impact of Large Language Models on Law Enforcement*, https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf, först publicerad 2023-03-27.
[35] Regeringskansliet (2024), *Regeringen samlade berörda myndigheter med anledning av storskalig cyberattack*, https://www.regeringen.se/pressmeddelanden/2024/01/regeringen-samlade-berorda-myndigheter-med-anledning-av-storskalig-cyberattackregeringen-samlade-berorda-myndigheter-med-anledning-av-storskalig-cyberattack/, först publicerad 2023-03-27.

och blivit alltmer specialiserad för att få användaren att agera på det sätt som gynnar angriparen.[36] Målsättningen kan variera, men vanligtvis handlar det om att lura användaren att exponera sitt lösenord eller få användaren att omedvetet ladda ner skadlig kod.[37]

Relativt nytt i samband med it-intrång är också att angripare i allt större grad överger metoden att placera skadlig kod i ett angripet system och istället utnyttjar befintlig programkod där, ett fenomen som numera benämns LOTL (eng. living off the land).[38] Tillvägagångssättet minskar angriparens spår i det angripna systemet och minskar därmed också risken för upptäckt.[39]

### 4.1.1 Hot mot elförsörjningen

Givet resurserna, kunskapen och intentionerna som både statliga- och icke-statliga aktörer besitter, kan en antagonist påverka svensk elförsörjning genom cyberangrepp.

Åtkomst till it-system som styr exempelvis driften av anläggningar och system, liksom information om dessa system, är potentiella mål för en antagonist. Det kan dels handla om direkt tillgång och exploatering, dels om dold tillgång och en mer långsiktig exploatering.[40]

Erfarenheterna från Rysslands invasionskrig i Ukraina visar att såväl cyberangrepp som fysiska (kinetiska) attacker regelbundet riktas mot elnätet, särskilt vintertid. Prioriterade mål inom elförsörjningen är delar som är svåra eller tar tid att återställa.[41]

Den snabba teknikutvecklingen i kombination med elnätens alltmer distribuerade karaktär innebär att befintliga hotaktörer snart kan få tillgång till

---

[36] ENISA (2023), *ENISA Threat Landscape 2023*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023, hämtad 2024-04-05.
[37] För mer information om olika attackmetoder, se Nationellt centrum för cybersäkerhet (2022), *Cybersäkerhet i Sverige 2022 Del 1: Hot, metoder, brister och beroenden*, https://www.ncsc.se/siteassets/publikationer/ncsc-rappor-1-cybersakerhet-i-sverige-2022-hot-metoder-brister-och-beroenden.pdf, hämtad 2024-04-05
[38] För mer information om LOTL, se *Joint Guidance, Identifying and Mitigating Living Off the Land Techniques*, framtagen av amerikanska, kanadensiska, australiensiska, nyazeeländska och brittiska myndigheter inom cybersäkerhet. https://www.cisa.gov/sites/default/files/2024-02/Joint-Guidance-Identifying-and-Mitigating-LOTL_V3508c.pdf, 2024-03-27.
[39] Cybersecurity & Infrastructure Security Agency (2023), *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection*, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a, först publicerad 2023-05-24.
[40] RISE (2023), *Förslag på åtgärder för att möta cyberhot mot elsystemet*, Centrum för cybersäkerhet, RISE Rapport 2023: mars, https://www.ri.se/sites/default/files/2023-12/CfCs_Rapport_Cyberhot-mot-elsystemet-1.pdf
[41] MSB (2023), *Erfarenheter från Ukraina – Initiala lärdomar för det civila försvaret – Delredovisning av regeringsuppdrag Fö2023/01325*, MSB2265 – november 2023, https://rib.msb.se/filer/pdf/30493.pdf.

helt nya, slagkraftiga angreppssätt. Ökad uppmärksamhet riktas idag mot it-säkerheten inom nya energislag och snabbt växande nischer som energilagring, elektriska fordon och balanseringstjänster. [42] [43] Angrepp kan till exempel ske mot otillräckligt skyddad teknik i stora mängder elfordon, fordonsladdare, värmepumpar, elmätare eller olika typer av kommersiella styrsystem hos privatanvändare. [44]

### 4.1.2 Aktuella händelser

Det finns ett flertal framträdande cyberhändelser som fått stor påverkan på företag och organisationer, inte minst inom energisektorn.

Vid flertalet tillfällen under 2023 har det rapporterats om GNSS-störningar (störning av satellitnavigering och tidshållning) i Östersjöområdet. [45] [46] Sådana störningar kan påverka tidssynkronisering och takthållning, något som krävs både inom it-verksamhet och för frekvenshållning och mätändamål i elförsörjningen. Störningarna har i flera fall haft sitt ursprung i den ryska enklaven Kaliningrad, och bland annat noterats av flygtrafik i Östersjöområdet. Även Finland har återkommande uppmärksammat liknande störningar. [47] [48]

ABB bekräftade i maj 2023 att företaget utsatts för en cyberattack där viss data stulits. Dock förblev både kundsystem och produktion tillgängliga utan avbrott.[49][50]

Kraftproduktionsföretaget Holding Slovenske Elektrarne (HSE) utsattes i november för en ransomware-attack som påverkade deras system, men inte

[42] J Johnson et al (2022), *Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses*, Energies 2022, 15(11), 3931; https://doi.org/10.3390/en15113931
[43] K Rohde (2019), *Cyber Security of DC Fast Charging: Potential Impacts to the Electric Grid*, Idaho National Labs, januari 2019, https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_8929.pdf
[44]RISE (2023), *Förslag på åtgärder för att möta cyberhot mot elsystemet*, Centrum för cybersäkerhet, RISE Rapport 2023: mars, https://www.ri.se/sites/default/files/2023-12/CfCs_Rapport_Cyberhot-mot-elsystemet-1.pdf
[45] GPSJam.org, https://gpsjam.org/
[46] ”Sverige drabbat av stor GPS-störning”, SVT Nyheter, 2024-01-03, https://www.svt.se/nyheter/inrikes/sverige-drabbat-i-storsta-gps-sabotaget-i-ostersjon
[47] “Finland sees five-fold increase in GPS disturbance reports during 2023”, YLE, 2024-03-08, https://yle.fi/a/74-20078262
[48] “Situational picture of disturbances in satellite navigation in Finland”, Traficom, 2023-07-12, https://www.traficom.fi/en/news/situational-picture-disturbances-satellite-navigation-finland
[49] Bleeping Computer (2023), US govt contractor ABB confirms ransomware attack, data theft, https://www.bleepingcomputer.com/news/security/us-govt-contractor-abb-confirms-ransomware-attack-data-theft/, först publicerad 2023-05-26.
[50] ABB (2023), ABB informerar om IT-säkerhetsincident, https://new.abb.com/news/sv/detail/103412/abb-informerar-om-it-sakerhetsincident, först publicerad 2023-05-23.

själva kraftproduktionen.[51] I december kom rapporter om att Serbiens statligt kontrollerade elbolag *Elektroprivreda Srbije* (EPS) utsatts för en liknande cyberattack.[52]

## 4.2 Fysisk skadegörelse och sabotage

Sabotage är en form av fysisk skadegörelse som syftar till att försämra förmågan hos den angripna verksamheten att upprätthålla sin funktionalitet. För elförsörjningen kan det handla om förstörelse av fysiska delar i elnätet eller dess it-infrastruktur, eller stölder av exempelvis explosivämnen, metaller, verktyg eller maskiner.

Ytterligare bakomliggande syften kan vara att testa förmågan till upptäckt och hantering av sabotage. I sådana fall kan det handla om misstänkta fordon eller okända personer som rör sig runt skyddsobjekt, eller mindre skadegörelse.

Andra hot kan vara sabotage i förberedande syfte, till exempel att beredskaps- och reservdelsresurser förstörs eller sätts ur spel, i syfte att försvåra återställning av funktionalitet inom elförsörjningen.

Andra former av hot kan vara attacker med farliga ämnen mot kontorsverksamhet, vilket även här kan vara ett sätt för en angripare att testa en verksamhets beredskap i form av förmåga till upptäckt och hantering.

Elförsörjningens anläggningar, eller byggarbetsplatser för sådana, innehåller också stöldbegärlig egendom, vilket gör att inbrott förekommer. Även kopparkabel utanför anläggningarna kan vara stöldbegärliga, trots att det för tjuven kan vara förenat med livsfara att genomföra stölden. Även här kan ett bakomliggande syfte vara att försvåra för verksamheten att återuppta arbetet, inte bara att stjäla värdefull materiel.

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 måltavla för denna typ av antagonister, exempelvis när aktivister gjorde olaga intrång på området för Oskarshamns kärnkraftverk.[53]

[51] Dark Reading (2023), Slovenian Electrical Utility HSE Suffers Ransomware Attack, https://www.darkreading.com/cyberattacks-data-breaches/slovenia-power-provider-hse-suffers-ransomware-attack, först publicerad 2023-11-28.
[52] Balkan Green Energy News (2023), Serbia's power utility EPS under unprecedented hacker attack, https://balkangreenenergynews.com/serbias-power-utility-eps-under-unprecedented-hacker-attack/, först publicerad 2023-12-19.
[53] SVT (2015), *19 fälls för intrång på kärnkraftverk*, https://www.svt.se/nyheter/nyhetstecken/19-falls-for-intrang-pa-karnkraftverk, först publicerad 2015-11-06.

Frågor kring upplåtelse av mark för uppförande av kraftledningar har väckt missnöje och lett till skadegörelse.

### 4.2.1 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.

### 4.2.2 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.

I september 2022 sprängdes flera hål i gasledningarna NordStream 1 och 2 i Östersjön.[54] Efter det har flera händelser uppmärksammats där det uppstått skador på undervattensinfrastruktur i Östersjön. En del av den infrastrukturen utgörs av undervattenskablar för elförsörjningen. Senast i oktober 2023 drabbades en undervattensledning för gas i Finska viken (BalticConnector) av en läcka.[55]

## 4.3 Informationsinsamling

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

Informationsinhämtning kan även ske genom spaning via drönare, otillåten fotografering och intrång. Därutöver finns också annan så kallad teknisk inhämtning, via exempelvis dataintrång och signalspaning. Det senare kan

[54] Säkerhetspolisen (2024), *Förundersökning om grovt sabotage läggs ned*, https://sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2024-02-07-forundersokning-om-grovt-sabotage-laggs-ned.html, först publicerad 2024-02-07.
[55] Dagens Nyheter (2023), *Tätare samarbete mot kabelsabotage i Östersjön*, https://www.dn.se/sverige/tatare-samarbete-mot-kabelsabotage-i-ostersjon/, först publicerad 2023-10-13.

handla om avlyssning av utrymmen eller teknisk utrustning såsom datorer eller mobiltelefoner.

AI kan föra med sig nya möjligheter för en hotaktör att lura, vilseleda och locka anställda eller leverantörer att dela med sig av information om svensk elförsörjning.

Informationsinsamling avseende Sveriges skyddsvärden pågår ständigt av både främmande makt och andra hotaktörer.

### 4.3.1 Hot mot elförsörjningen

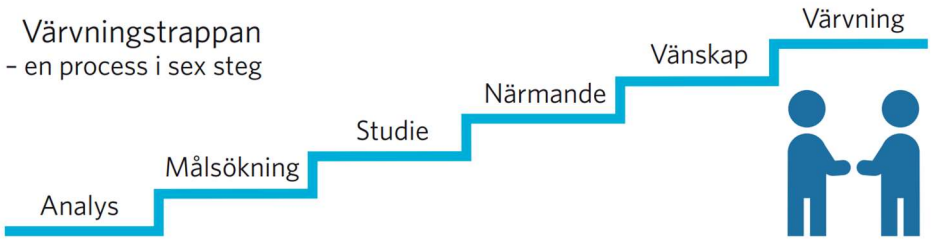
Genom kontakter med personal inom elförsörjningen kan en antagonist få tillgång till information (uppgifter) av betydelse för elförsörjningen (inklusive om annan personal med nyckelfunktioner), tillgång till it-system (t.ex. genom inloggningsuppgifter) och möjlighet att påverka hur personal agerar (t.ex. under kriser). En kartläggning av skyddsvärda tillgångar inom elförsörjningen kan blotta vilka kritiska beroenden som finns och var en attack skulle göra störst skada.

Kartläggning och informationsinhämtning kan ske genom olika former av avlyssning, med eller utan tekniska hjälpmedel. Metoderna är många, och består exempelvis av intrång i enskilda personers mobiltelefoner[56] och avlyssning av fysiska och digitala mötesrum.[57]

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. Representanter eller andra ombud för främmande makt tar kontakt och använder sig av den så kallade värvningstrappan. Främmande makt kan lägga omfattande resurser 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.

[56] Nationellt centrum för cybersäkerhet (2022), *Cybersäkerhet i Sverige 2022 Del 1: Hot, metoder, brister och beroenden*, https://www.ncsc.se/siteassets/publikationer/ncsc-rappor-1-cybersakerhet-i-sverige-2022-hot-metoder-brister-och-beroenden.pdf, hämtad 2024-04-05

[57] Säkerhetspolisen (2023) *Vägledning i säkerhetsskydd – Avlyssningsskyddade utrymmen*, https://sakerhetspolisen.se/download/18.3baf70bf187108c7cf04c4/1683121211992/Avlyssningsskyddade%20utrymmen_anpassad.pdf, hämtad 2024-04-16.




**Figur 2.** Värvningstrappan (Svenska kraftnät, 2023)

### 4.3.2 Aktuella händelser

De senaste åren har ett antal mål avgjorts i olika instanser gällande grov obehörig befattning med hemlig uppgift, utifrån ett internetforum där enskilda personer samlat och delat uppgifter om militära skyddsobjekt.[58][59]

Det mest uppmärksammade fallet gällande informationsinsamling på senare år gäller de två bröder som i november 2022 åtalades för grovt spionieri. Den äldre brodern åtalades även för grovt obehörig befattning med hemlig uppgift. Den äldre brodern dömdes till livstids fängelse, den yngre till fängelse i nio år och tio månader.[60] [61] [62]

Det har under våren 2024 rapporterats om misstänkt kartläggning av reservkraftverk och kommuners uthållighet vid strömavbrott, genom begäran om utlämning av allmän handling till merparten av landets kommuner[63].

I januari 2022 observerades drönare vid flera tillfällen över kärnkraftverken i Oskarshamn, Ringhals och Forsmark. Händelserna polisanmäldes, och utredningen övertogs av Säkerhetspolisen.[64] I mars 2022 meddelade

---

[58] Säkerhetspolisen (2024), *Åtal för obehörig befattning med hemlig uppgift*, https://sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2024-02-28-atal-for-grov-obehorig-befattning-med-hemlig-uppgift.html, hämtad 2024-04-16.
[59] Åklagarmyndigheten (2021), *En person åtalas för att ha spridit uppgifter om militära anläggningar*, https://www.aklagare.se/nyheter-press/pressmeddelanden/2021/februari/en-person-atalas-for-att-ha-spridit-uppgifter-om-militara-anlaggningar/, först publicerad 2021-02-05.
[60] Stockholms tingsrätt (2023), *Två bröder döms för grovt spionieri*, https://www.domstol.se/stockholms-tingsratt/nyheter/2023/01/tva-broder-doms-for-grovt-spionieri/, först publicerad 2023-01-19.
[61] Svea hovrätt (2023), *Svea hovrätt meddelar dom i mål om grovt spionieri*, https://www.domstol.se/nyheter/2023/05/svea-hovratt-meddelar-dom-i-mal-om-grovt-spionieri/, först publicerad 2023-05-25.
[62] Högsta domstolen (2023), *Högsta domstolen meddelar inte prövningstillstånd i mål om grovt spionieri*, https://www.domstol.se/hogsta-domstolen/nyheter/2023/09/hogsta-domstolen-meddelar-inte-provningstillstand-i-mal-om-grovt-spionieri/, först publicerad 2023-09-19.
[63] Larm om misstänkt kartläggning av landets elberedskap | SVT Nyheter (2024-02-27)
[64] Säkerhetspolisen (2022), *Förundersökning tas över kring drönare vid kärnkraftverk*, https://www.sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2022-01-19-forundersokning-tas-over-kring-dronare-vid-karnkraftverk.html, först publicerad 2022-01-19.

Åklagarmyndigheten att förundersökningen lagts ner då man inte lyckas styrka vem eller vilka som låg bakom. Utredningen kom dock fram till att flygningarna gjorts med fyra till nio drönare av ”professionell typ”.[65]

## 4.4 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. Ryssland och Kina utmärker sig inom detta område. 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 [66]. Norge har infört lagstiftning för att skydda sig mot denna typ av köp. [67]

Lagen (2023:560) om granskning av utländska direktinvesteringar trädde i kraft den 1 december 2023. Lagen gäller för investeringar i skyddsvärd verksamhet som bedrivs av ett aktiebolag, europabolag, handelsbolag, ekonomisk föreningar eller stiftelser som har säte i Sverige. Lagen gäller också för investeringar i sådan skyddsvärd verksamhet som bedrivs i Sverige i ett enkelt bolag eller som enskild näringsverksamhet.[68]

Lagen omfattar inte förvärv av fast egendom, men en utredning om ny reglering för detta pågår.[69]

### 4.4.1 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

[65] Omni (2022), *Utredning om drönare vid kärnkraftverk läggs ned*, https://omni.se/utredning-om-dronare-vid-karnkraftverk-laggs-ned/a/wOm6P4, först publicerad 2022-03-10.
[66] Skyddspolisen (2020), SUPO 2020 Årsbok, https://supo.fi/documents/38197657/40760239/Supo+%C3%85rsbok+2020.pdf/061873d5-3bbe-bc88-36c3-9ad3e355581b/Supo+%C3%85rsbok+2020.pdf?t=1646741973003, hämtad 2024-04-16.
[67] Lov om nasjonal sikkerhet (sikkerhetsloven), LOV-2018-06-01-24, Kapittel 9. Sikkerhetsgraderte anskaffelser mv., https://lovdata.no/dokument/NL/lov/2018-06-01-24/KAPITTEL_9#KAPITTEL_9, hämtad 2024-04-16.
[68] 2§ lagen (2023:560) om granskning av utländska direktinvesteringar.
[69] Dir. 2022:121 och Dir. 2023:172.

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.

### 4.4.2 Aktuella händelser

Under 2023 uppmärksammades att en rysk medborgare med affärsintressen i Ryssland låg bakom köpet av en fastighet i närheten av Muskö. På Muskö finns en örlogsbas samt flera hamnar i bergrum. Området kring Muskö var fram till 1990-talet helt avstängt för utländska medborgare, men idag finns inga sådana begränsningar i Sverige.[70]

## 4.5 Utkontraktering och osäkra leverantörskedjor

Det privata näringslivet ansvarar i stor utsträckning för viktiga leveranser till säkerhetskänsliga verksamheter. Globaliseringen innebär att dessa verksamheters leverantörer ofta finns utanför Sveriges gränser.

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.

### 4.5.1 Hot mot elförsörjningen

Inom elförsörjningen finns ett stort beroende av entreprenörer och leverantörer för både byggnation, underhåll, reparationer och kritiska

[70] Expressen (2023), *Ryske affärsmannen äger tomt – vid Musköbasen*, https://www.expressen.se/nyheter/ryske-affarsmannen-ager-tomt-vid-muskobasen/ Först publicerad 2023-01-04.

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. Detta gäller såväl leverantörer av hård- och mjukvara som konsulttjänster.

Ett exempel på ett hot via hårdvara eller mjukvara 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. Till detta har även så kallade LOTL[71]-tekniker tillkommit där befintlig programvara används som ingång för en attack, se avsnitt 4.1.

### 4.5.2 Aktuella händelser

Ransomware-gruppen Clop utnyttjade en nolldagarssårbarhet i företaget MOVEit:s filöverföringsplattform som används av flera tusen myndigheter och företag.[72] Bland de drabbade återfinns bl.a. Schneider Electric och Siemens Energy som är stora leverantörer av industriella kontrollsystem (ICS). Clop har genom sårbarheten lyckats utpressa hundratals organisationer genom att kompromettera en enda miljö. Omfattningen av attacken påvisade flera brister hos de drabbade, men även komplexiteten kring att säkra hela leverantörskedjan.[73]

I början av 2024 drabbades ett av it-leverantören TietoEvrys datacenter av en ransomware-attack som fick stor påverkan på svenska företag och myndigheter. Gruppen Akira tros ligga bakom attacken, som utförts genom att utnyttja en sårbarhet i Ciscos produkter.[74] Händelsen visar på många myndigheters och organisationers bristande beredskap för plötsligt bortfall,

[71] Living-off-the-Land (LOTL)
[72] CERT-SE (2023), Kritisk sårbarhet i MOVEit Transfer, https://www.cert.se/2023/06/kritisk-sarbarhet-i-moveit-transfer, först publicerad 2023-06-01.
[73] Emsisoft (2023), Unpacking the MOVEit Breach: Statistics and Analysis, https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/, först publicerad 2023-07-23.
[74] Computer Sweden (2024), Cyberattack mot Tietoevry slår hårt – många drabbade, https://computersweden.se/article/1296140/cyberattack-mot-tietoevry-slar-hart-manga-drabbade.html, först publicerad 2024-01-22.

samt riskerna med att samla flera verksamheter som nyttjar samma leverantörer.[75]

## 4.6 Gråzonsproblematik och väpnat angrepp

Med gråzonsproblematik 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.[76] Otydlig lagstiftning och konstitutionella begränsningar kan skapa möjligheter för antagonistiska handlingar. En sådan möjlighet är att dra nytta av gränsdragningar mellan myndigheters ansvar, exempelvis Polismyndigheten (ansvarar för landets inre säkerhet) och Försvarsmakten (ansvarar för landets yttre säkerhet). Motståndaren kan alltså angripa landet med något som tycks vara kriminell verksamhet men som egentligen har en djupare dimension. Under gråzon kan ryktesspridning, motsägelsefull information, agerande genom ombud, sabotage samt nätverks- och påverkansoperationer förekomma.

Väpnat angrepp är när en stat använder militära våldsmedel mot en annan stat. I modern krigföring kan även angrepp ske genom dolda och förnekbara aktiviteter, cyberattacker och påverkansoperationer. Antagonistiska handlingar i gråzon kan utgöra förberedelser till väpnat angrepp.

Det säkerhetspolitiska läget i Sveriges närområde har försämrats allvarligt sedan Rysslands militära anfall mot Ukraina 2022[77]. Läget beskrivs som det allvarligaste sedan andra världskrigets slut[78]. Kriget har medfört spänningar och splittring i världen där väst och demokratiska länder tenderar att hamna på en sida och Ryssland, Kina och andra auktoritära stater på den andra[79]. Ryssland fortsätter försöka reducera Västs inflytande till ett minimum i Rysslands självupplevda intressesfär samt säkerställa att grannländer är allierade med Ryssland, eller åtminstone neutrala, alternativt försvagade eller helt underställda rysk kontroll[80]. Risken finns att kriget i Ukraina kan spridas

[75] Regeringskansliet (2024), *Regeringen samlade berörda myndigheter med anledning av storskalig cyberattack*, https://www.regeringen.se/pressmeddelanden/2024/01/regeringen-samlade-berorda-myndigheter-med-anledning-av-storskalig-cyberattackregeringen-samlade-berorda-myndigheter-med-anledning-av-storskalig-cyberattack/, först publicerad 2023-03-27.
[76] För fördjupad läsning se FOI:s rapport *Gråzonslägen i krig och fred*, FOI-R--5447—SE, Juni 2023, https://www.foi.se/rest-api/report/FOI-R--5447--SE.
[77] MUST årsöversikt 2023, Försvarsmakten; Säkerhetspolisens årsbok 2023-2024, Säkerhetspolisen; FRA årsrapport 2023, Försvarets radioanstalt
[78] Försvarsberedningen (2023), *Kraftsamling, Inriktningen av totalförsvaret och utformningen av det civila försvaret*, .Ds. 2023:34. https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2023/12/ds-202334-kraftsamling/.
[79]MUST (2024) *Must årsöversikt 2023*, https://www.forsvarsmakten.se/siteassets/2-om-forsvarsmakten/dokument/musts-arsoversikter/must-arsoversikt-2023.pdf.
[80] Ibid

vidare eller eskalera ytterligare. En eskalering kan innebära angrepp mot andra stater och ett väpnat angrepp mot Sverige kan inte uteslutas[81].

### 4.6.1 Hot mot elförsörjningen

Attacker kan riktas mot den svenska elförsörjningen i syfte att destabilisera samhällets funktionalitet och försämra försvarsförmågan. I händelse av att Sverige blir utsatt för väpnat angrepp bedöms elförsörjningen kunna utgöra en måltavla för motståndarens krigföring. Elförsörjningen kan attackeras militärt med fjärrstridsmedel eller från marken, luften eller sjön. Vidare kan sabotage ske både genom cyberangrepp och genom fysiskt sabotage.

Sabotage kan även genomföras i fredstid som krigsförberedelser, i syfte att pröva elförsörjningen och dess förmåga att förebygga och hantera angrepp. I detta sammanhang kan aktören välja att agera inom ramen för gråzonsproblematik.

En jämförelse kan göras med kriget i Ukraina. I krigets inledning var inte elförsörjningen ett specifikt mål för Ryssland utan det var först hösten 2022 som riktade attacker mot ukrainsk elinfrastruktur påbörjades. Attackerna har skett med både missiler och drönare. Såväl produktionsanläggningar, transmissionsnät och distributionsnät har skadats svårt och det har medfört avbrott i eldistributionen och svåra konsekvenser för det ukrainska samhället och befolkningen som följd.

### 4.6.2 Aktuella händelser

Att avgöra om antagonistiska attacker utförs av främmande makt utifrån ett gråzonsläge är ibland mycket svårt, vilket också ligger i sakens natur då en angripare oftast vill dölja att man ligger bakom attacken. Resonemang kring detta återfinns i kapitel 2.2.4.

Cyberattacker mot svensk offentlig och privat verksamhet (se 4.5.2.) och skadegörelse på undervattensinfrastruktur i Östersjön (se 4.2.2.) kan vara exempel på agerande inom ramen för gråzonsproblematik.

[81] Försvarsberedningen (2023), *Kraftsamling, Inriktningen av totalförsvaret och utformningen av det civila försvaret*, .Ds. 2023:34. https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2023/12/ds-202334-kraftsamling/

# Referenser i urval

För ytterligare källor se respektive fotnot.

## Samlingssidor för svenska underrättelsemyndigheters årsöversikter

Säkerhetspolisens årsberättelse - Säkerhetspolisen (sakerhetspolisen.se)

Årsrapporter - FRA

MUST: Rapporter - Försvarsmakten (forsvarsmakten.se)

Nationellt centrum för terrorhotbedömning - Säkerhetspolisen (sakerhetspolisen.se)

## Samlingssidor för nordiska och baltiska underrättelsemyndigheters årsöversikter

Estland: Annual reviews | Kaitsepolitseiamet (kapo.ee)

Finland: Årsbok | Supo

Norge: Risiko 2024 - Nasjonal sikkerhetsmyndighet (nsm.no)

Danmark: Publications | | Danish Security and Intelligence Service (pet.dk)

## Svenska myndigheter i övrigt

Arbetsförmedlingen et al. (2023), *Myndighetsgemensam lägesbild organiserad brottslighet 2023*, https://polisen.se/siteassets/dokument/organiserad_brottslighet/mgl-2023.pdf

FOI (2023) *Gråzonslägen i krig och fred*, FOI-R--5447—SE, Juni 2023, https://www.foi.se/rest-api/report/FOI-R--5447--SE.

MSB (2023), *Erfarenheter från Ukraina – Initiala lärdomar för det civila försvaret – Delredovisning av regeringsuppdrag Fö2023/01325*, MSB2265 – november 2023, https://rib.msb.se/filer/pdf/30493.pdf

MSB (2024), *EU förändrar cybersäkerhetsområdet : årsrapport it-incidentrapportering 2023*, MSB2341, https://rib.msb.se/filer/pdf/30618.pdf.

Nationellt centrum för cybersäkerhet (2022), *Cybersäkerhet i Sverige 2022 Del 1: Hot, metoder, brister och beroenden*, https://www.ncsc.se/siteassets/publikationer/ncsc-rappor-1-cybersakerhet-i-sverige-2022-hot-metoder-brister-och-beroenden.pdf

Nationellt centrum för terrorhotbedömning (2024), *Helårsbedömning 2024 – sammanfattning*, https://www.sakerhetspolisen.se/download/18.5cb30b118d1e95affe641/1707750097566/NCT%20Helarsbedomning%202024.pdf

RISE (2023), *Förslag på åtgärder för att möta cyberhot mot elsystemet*, Centrum för cybersäkerhet, RISE Rapport 2023: mars, https://www.ri.se/sites/default/files/2023-12/CfCs_Rapport_Cyberhot-mot-elsystemet-1.pdf

Svenska kraftnät (2024), *Omvärldsanalys 2024*, Svk2024/738.

Säkerhetspolisen (2023) *Vägledning i säkerhetsskydd – Avlyssningsskyddade utrymmen*, https://sakerhetspolisen.se/download/18.3baf70bf187108c7cf04c4/1683121211992/Avlyssningsskyddade%20utrymmen_anpassad.pdf,

## Utländska myndigheter

Cybersecurity & Infrastructure Security Agency (2023), *People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection*, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

Cybersecurity & Infrastructure Security Agency et al. (2024), *Joint Guidance, Identifying and Mitigating Living Off the Land Techniques*, https://www.cisa.gov/sites/default/files/2024-02/Joint-Guidance-Identifying-and-Mitigating-LOTL_V3508c.pdf

ENISA (2023), *ENISA Threat Landscape 2023*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Europol (2023), *Internet Organised Crime Threat Assessment (IOCTA) 2023*, https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf

Europol (2023), *Europol spotlight – Cyber attacks – The apex of crime-as-a-service,* https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf

Europol (2023), *ChatGPT The impact of Large Language Models on Law Enforcement*,

https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf

Skyddspolisen (2020), *SUPO 2020 Årsbok*, https://supo.fi/documents/38197657/40760239/Supo+%C3%85rsbok+2020.pdf/061873d5-3bbe-bc88-36c3-9ad3e355581b/Supo+%C3%85rsbok+2020.pdf?t=1646741973003

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

SVENSKA KRAFTNÄT