Energimyndigheten

2026

Övningspaket för att stärka energisektorns förmåga inför kriser och krig

Drivmedel

Övningspaket Hybrida hot

Innehåll

Därför övar vi!		**3**
Gemensamma övningsbestämmelser		**4**
Instruktion för genomförande		**5**
Scenario: Grundläget		**6**
Moment	**Påverkansoperationer**	**7**
	Cyberangrepp	**8**
	Fysiska sabotage	**9**
	Underrättelseinhämtning	**10**
	Samordnade störningar	**11**
Reflektion och utvärdering		**12**

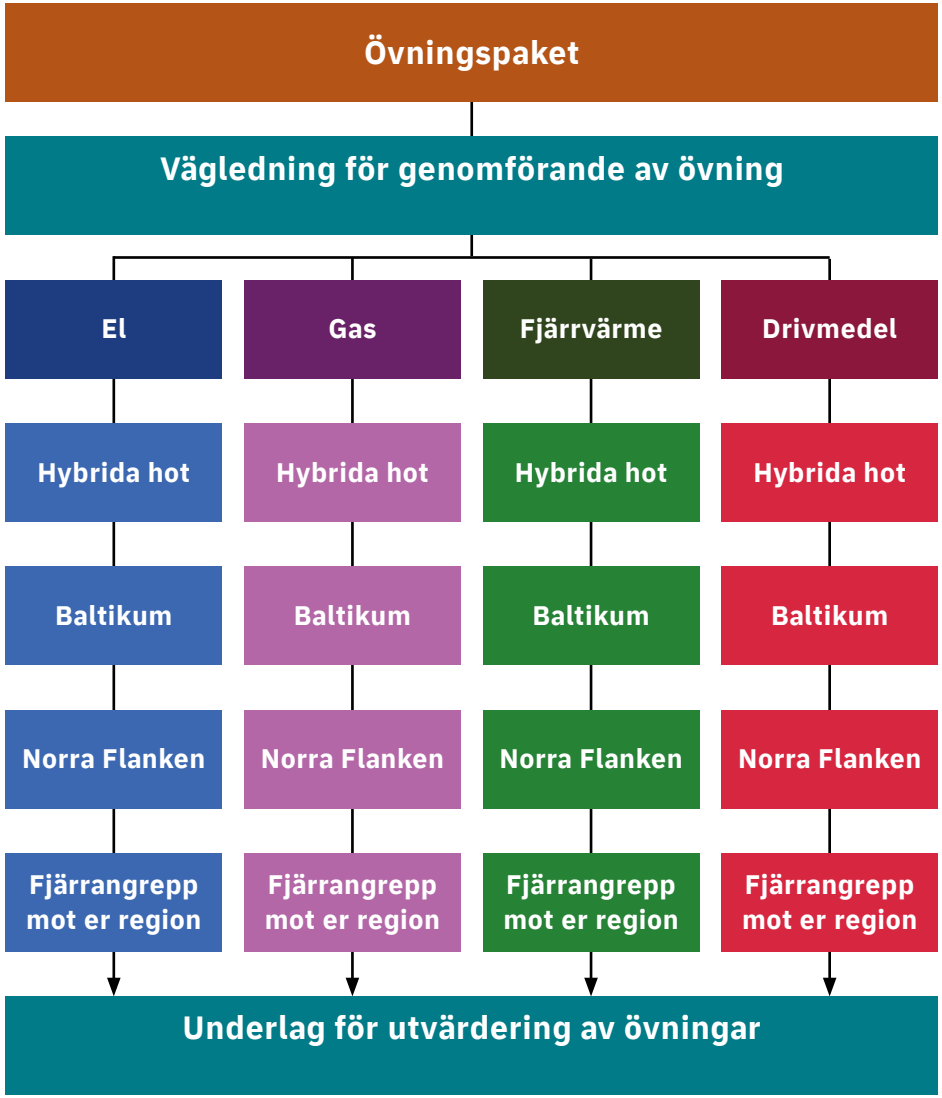
Därför övar vi!

Energiförsörjningen har en avgörande betydelse för samhällets funktionalitet och för att skydda liv, hälsa och samhällets motståndskraft vid olika typer av samhällskriser. Energiförsörjningen måste fungera både i vardagen, under fredstida samhällskriser och krig.

Alla energibolag har en viktig roll. Övning är ett effektivt sätt att stärka den mentala förberedelsen inför olika typer av störningar och underlätta identifiering av förebyggande åtgärder som gör det möjligt att upprätthålla verksamheten även under störda förhållanden.

I takt med den ökade digitaliseringen skapas nya sårbarheter och nya hot. Samtidigt medför klimat-förändringarna att tidigare kända hot kan få mer omfattande konsekvenser och bli mer frekventa.

De senaste åren har även det säkerhetspolitiska läget försämrats i Sveriges närområde. Sammantaget innebär det att vikten av att stärka motståndskraften för olika typer av störningar i energiförsörjningen får ökad betydelse.



Gemensamma övningsbestämmelser

För att ha en enad utgångspunkt inför övningen är det viktigt att diskutera och enas om vilka förhållningsregler som ska gälla under dagen.

Syfte och mål

- Vad vill ni uppnå med dagens övning?
- Vilka förmågor eller frågeställningar ska ha särskilt fokus?

Exempel:

”Vi ska öka vår förståelse för vår roll inom totalförsvaret” eller ”Vi ska öva prioritering av resurser under störda förhållanden.”

Förhållningssätt

- Hur vill ni att deltagarna ska agera under övningen?
- Hur säkerställer ni ett öppet och konstruktivt deltagande?

Exempel:

“Alla ska ges möjlighet att komma till tals” eller “Vi är lösningsorienterade om scenariot innehåller oklarheter.”

Övrigt

- Finns det andra praktiska eller gemensamma spelregler som ni vill komma överens om?

Exempel:

“Mobiltelefoner på ljudlöst” eller “Frågor och förtydliganden uppmuntras under hela övningen.”

Informationssäkerhet

- Säkerställ att ni använder ändamålsenliga lokaler och hjälpmedel utifrån hur skyddsvärd information som ska avhandlas.
- Bevaka löpande under övningen om det finns risk för att skyddsvärd information röjs till obehörig och pausa i så fall den diskussionen.
- På Energimyndighetens, Säkerhetspolisens och Försvarshögskolans hemsidor finner du mer information om säkerhetsskydd och informationssäkerhet.

Instruktion för genomförande

1 Läs grundscenariot

- Läs igenom scenariots Grundläget.

2 Genomför momenten

- Gå igenom momenten ett i taget.
- Varje moment beskriver en möjlig händelseutveckling som utmanar verksamhetens förmåga.
- Ni kan genomföra hela scenariot eller välja de moment som är mest relevanta utifrån era behov och den tid ni har tillgänglig.

3 Diskutera frågorna

- Till varje moment finns diskussionsfrågor inom tre perspektiv:
- Reaktivt – Hur hanterar ni situationen här och nu?
- Proaktivt – Vilka förberedelser, planer och förmågor bör finnas på plats?
- Ett samlat totalförsvar – Hur påverkas ert ansvar och ert bidrag till totalförsvaret?

4 Utvärdera

- Anteckna löpande åtgärder som identifieras under diskussionerna och säkerställ att dessa följ upp efter övningen.

Mer information om utvärdering efter övningen återfinns i Underlag för utvärdering av övning

Kom ihåg!

- Anpassa scenarier, moment och frågor utifrån er organisation, era beroenden och era förutsättningar.
- Det är inte nödvändigt att besvara alla frågor. Fokusera på de diskussioner som ger mest värde för verksamheten.
- Frågor märkta med ”Utveckla scenariot och anpassa till er verksamhet” kräver att ni kompletterar scenariot med detaljer som speglar den egna verksamhetens förutsättningar, beroenden och geografiska förhållanden. Detta är i praktiken relevant för hela övningen, men är särskilt viktigt för dessa frågor och de efterföljande frågorna inom momentet.

Scenario
Grundläget

Det är januari och sträng kyla råder i stora delar av Sverige.
Energibehovet är högt.

Under de senaste dagarna har flera allvarliga incidenter inträffat runt om i landet. Media rapporterar löpande om angrepp mot civila mål, bland annat gasinfrastruktur, teleanläggningar, transportrelaterade system och andra IT-miljöer. Vissa händelser har inneburit explosioner och fysisk skadegörelse, medan andra har bestått av riktade cyberangrepp mot styr- och övervakningssystem.

Störningarna har orsakat avbrott i gasleveranser, påverkat flöden och skapat en snabbt växande oro i samhället. Flera centrala samhällsfunktioner är påverkade. Produktionen och distributionen av el och drivmedel störs samtidigt i betydande omfattning, vilket skärper kraven på en stabil gasförsörjning till prioriterade användare. Den operativa hanteringen försvåras dessutom av en fortsatt ofullständig lägesbild.

Angriparen eller angriparna är i nuläget okända. Myndigheterna kan ännu inte fastställa om händelserna är samordnade, men tidssambanden och angreppens karaktär tyder på en möjlig systematik.

Det säkerhetspolitiska läget i Europa är fortsatt allvarligt. Rysslands fullskaliga invasion av Ukraina pågår och relationen mellan Ryssland och väst är mycket ansträngd. Flera stater använder hybrida metoder såsom cyberangrepp, sabotage och informationspåverkan.

Moment 1:
Påverkansoperationer

Förmågor som övas
- Kriskommunikation
- Hantera otillbörlig informationspåverkan
- Skydda förtroende för gasförsörjning

Momentbeskrivning
Under en period med hög belastning i gasförsörjningssystemet sprids uppgifter i sociala medier om att gasförsörjningen i Sverige riskerar att inte kunna upprätthållas. Informationen riktas delvis mot ert bolag och påstår att ni döljer brister och gör orättvisa prioriteringar.

Samtidigt publiceras ett läckt dokument som kopplas till er verksamhet. Dokumentet innehåller delvis felaktig information men uppfattas som trovärdigt.

Detta leder till ökad oro hos kunder och media. Förtroendet för er förmåga att upprätthålla gasleveranser påverkas och trycket på att snabbt ge tydliga besked ökar.

Diskussionsfrågor:

Reaktiva
- Vad är det som händer och hur påverkar det er just nu? Utveckla scenariot och anpassa till er verksamhet.
- Vad behöver vi göra direkt för att bemöta informationen?
- Hur säkerställer vi att korrekt information når kunder och media?
- Hur hanterar vi oro hos kunder och hot mot personal?
- Vilka aktörer behöver vi samverka med?

Proaktiva
- Hur väl förstår ni hur och varför hotaktörer använder otillbörlig informationspåverkan, och vilka exempel kan ni ge på hur denna förståelse påverkar ert arbete?
- Finns det rutiner för att möta falsk och vilseledande information, t.ex. i beredskapsplaner eller motsvarande? Om inte, vad kan ni förbereda för att möta falsk och vilseledande information?
- Vilka rutiner har ni för kriskommunikation?

Ett samlat totalförsvar
- Hur bidrar ni till att upprätthålla förtroendet för gasförsörjningen i samhället?
- Hur stödjer ni myndigheter med korrekt information?

Moment 2:
Cyberangrepp

Förmågor som övas
- Hantera IT/OT-angrepp
- Upprätthålla drift under störning
- Isolera och begränsa påverkan

Momentbeskrivning
Era styr- och övervakningssystem för gasförsörjning, exempelvis gasflöden, tryckreglering eller anläggningsstyrning, utsätts för ett cyberangrepp via en komprometterad fjärranslutning. Obehöriga kommandon skickas till flera anläggningar, såsom reglerstationer, lagringsanläggningar eller andra styrbara komponenter, och system visar felaktiga eller motstridiga flödes- och tryckvärden, och vissa funktioner går inte längre att styra som normalt.

Samtidigt manipuleras mätvärden och systemdata, vilket gör det svårt att avgöra vad som faktiskt sker i anläggningarna.

Detta påverkar er förmåga att övervaka och styra verksamheten. Risken ökar för felaktiga driftbeslut, vilket kan leda till obalanser i flöden, tryckproblem och störningar i leveranser.

Diskussionsfrågor:

Reaktiva
- Vad vet ni om intrånget och hur påverkar det era drift- och övervakningssystem? Utveckla scenariot och anpassa till er verksamhet.
- Vilka omedelbara åtgärder vidtar ni?
- Hur isolerar ni angripna system för att stoppa spridning?
- Vilka prioriteringar behöver ni göra för att undvika följdeffekter?
- Vilka aktörer behöver ni samverka med och hur sker den samverkan?

Proaktiva
- Finns denna typ av IT/OT-hot med i era beredskapsplaner?
- Vilka manuella eller alternativa driftlösningar har ni? Hur länge kan ni använda dessa?
- Hur ser era rutiner ut för att upptäcka och hantera intrång?
- Vilka förebyggande åtgärder kan ni vidta för att minska risken för den här typen av hot?
- Hur ser era rutiner ut för incidenthantering?

Ett samlat totalförsvar
- Hur bidrar era åtgärder till att begränsa de negativa effekterna i samhället?

Moment 3:
Fysiska sabotage

Förmågor som övas
- Hantera fysisk skada i gasinfrastruktur
- Prioritera återställning
- Skydda anläggningar

Momentbeskrivning
En explosion inträffar vid en av era större gasanläggningar, exempelvis en reglerstation, lagringsanläggning, importpunkt eller annan kritisk komponent. Kritisk utrustning skadas och anläggningen slås delvis ut.

Detta leder till att ett stort antal kunder och samhällsviktiga verksamheter får minskade eller uteblivna gasleveranser i ett läge med sträng kyla.

Händelsen påverkar er leveransförmåga direkt och skapar behov av snabba prioriteringar i återställningsarbetet.

Diskussionsfrågor:

Reaktiva
- Vilka anläggningar, komponenter eller driftfunktioner har skadats eller påverkats? Utveckla scenariot och anpassa till er verksamhet.
- Vilka omedelbara respektive följdverkningar kan det få?
- Vilka anläggningar, flöden eller driftfunktioner ska återställas först?
- Hur säkerställer ni att fler anläggningar eller funktioner inte påverkas?
- Hur organiserar ni det tekniska arbetet och insatserna på plats?

Proaktiva
- Hur prioriterar ni mellan olika kundgrupper?
- Har ni tillräcklig kapacitet att hantera flera skador samtidigt?
- Vilka ytterligare skyddsåtgärder för er gasinfrastruktur behöver införas?

Ett samlat totalförsvar
- Har ni tydliga principer för att prioritera återställning till samhällsviktig och militär verksamhet?

Moment 4:
Underrättelseinhämtning

Förmågor som övas

- Upptäcka säkerhetshot
- Skydda känslig information
- Rapportera säkerhetshot

Momentbeskrivning

Flera händelser inträffar som tyder på att någon kartlägger er gasinfrastruktur och drift. En medarbetare kontaktas med detaljerade frågor om tekniska lösningar kopplade till gasförsörjning. Samtidigt upptäcks ovanliga nedladdningar av driftinformation från interna system.

En drönare observeras i närheten av en av era anläggningar.

Händelserna var för sig är oklara, men sammantaget tyder de på riktad informationsinhämtning. Detta innebär en ökad risk för framtida angrepp mot er verksamhet.

Diskussionsfrågor:

Reaktiva

- Hur skulle tecken på att någon kartlägger eran verksamhet kunna se ut?
- Vilka åtgärder vidtar ni direkt för att skydda informationen?
- Hur samlar ni in information från påverkade delar av verksamheten till en gemensam lägesbild?
- Hur och till vem rapporterar ni detta? Vilka samverkar ni med?

Proaktiva

- Hur arbetar ni systematiskt med att upptäcka denna typ av avvikelser?
- Hur arbetar ni med säkerhetsskydd?
- Hur skyddad är er känsliga information idag?
- Hur utbildad är er personal i säkerhetsskydd?
- Har ni tydliga rutiner för rapportering och samverkan kring denna typ av händelse?

Ett samlat totalförsvar

- Hur bidrar ni till att motverka underrättelsehot?

Moment 5:
Samordnade störningar

Förmågor som övas
- Leda hantering av samordnade störningar
- Samordna interna och externa aktörer
- Prioritera åtgärder under tidspress

Momentbeskrivning
Ert bolag drabbas av ett cyberintrång i driftmiljön och ett fysiskt sabotage mot en anläggning.

Intrånget påverkar styrning och övervakning av gasflöden och anläggningar, medan sabotaget slår ut fysisk kapacitet i gasinfrastruktur, exempelvis vid en reglerstation, lagringsanläggning eller importpunkt. Kombinationen innebär att både styrning, övervakning och fysisk kapacitet i gasinfrastrukturen är nedsatt samtidigt.

Detta leder till omfattande störningar i gasförsörjningen och påverkar både kunder och samhällsviktig verksamhet. Situationen kräver snabba beslut under hög osäkerhet.

Diskussionsfrågor:

Reaktiva
- Hur etablerar ni ledning i denna situation?
- Vilka åtgärder ska prioriteras först?
- Hur samordnar ni arbetet internt?
- Vilka externa aktörer behöver ni samverka med?
- Hur prioriterar ni mellan olika samhällsviktiga behov?

Proaktiva
- Hur ser er krisledningsstruktur ut?
- Vilka prioriteringsprinciper har ni vid flera samtidiga störningar?
- Hur säkerställer ni effektiv samverkan med andra aktörer?
- Vilka beroenden behöver ni beakta i samverkan?
- Hur utbildade och övade är ni i att hantera komplexa händelser?

Ett samlat totalförsvar
- Hur bidrar era prioriteringar till totalförsvarets behov?

Reflektion och utvärdering

- Hur känns det nu?
- Vilka är våra styrkor?
- Vilka är våra förbättringsområden?
- Vad tar vi med oss i vår organisation framåt?

Tips!
Se och inspireras av det framtagna underlaget för utvärderingen.

Energimyndigheten

Materialet har tagits fram av 4C Strategies
på uppdrag av Energimyndigheten

Statens energimyndighet, juli 2026
ET 2026:04
ISSN 1403-1892
ISBN (pdf) 978-91-7993-292-3