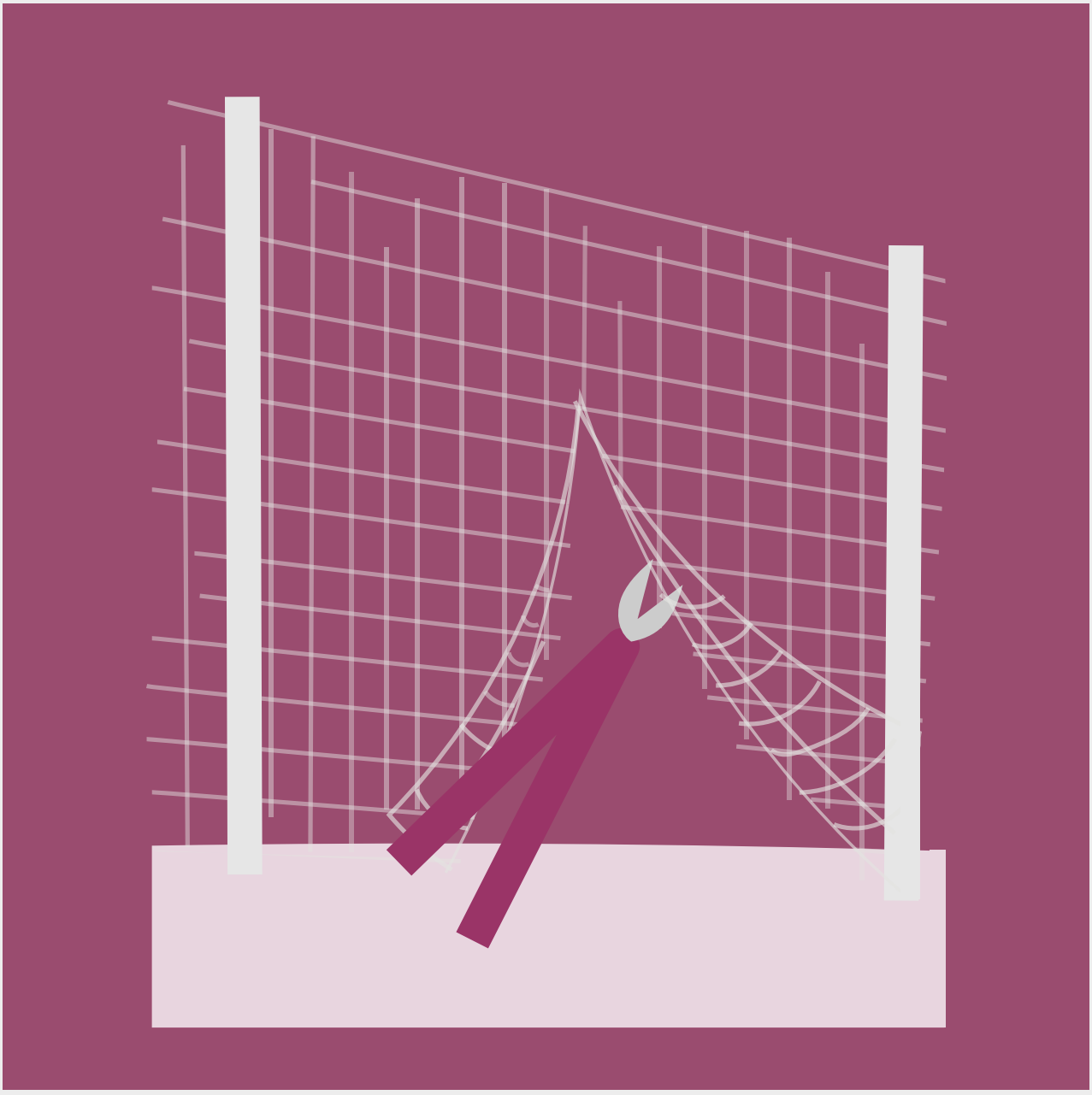
Myndigheten för samhällsskydd och beredskap

Sveriges Kommuner och Regioner

HANDBOK I CIVIL BEREDSKAP FÖR KOMMUNER
4. RISKKATALOG

Sabotage



Handbok i civil beredskap för kommuner – 4. Riskkatalog – Sabotage

Det här kapitlet är en del av publikationsserien *Handbok i civil beredskap för kommuner* där fler kapitel finns.

Produktion: Advant

Publikationsnummer: MSB2308 - maj 2024

Innehåll

Sabotage **4**
Om riskområdet 4
Kort om konsekvenser 5
Osäkerhetsbedömning 5
Utveckling och trender 6
Exempel på inträffade händelser 7
Löpande riskbedömningar 7
Ansvar och roller 7

Sabotage

Som stöd till riskkatalogen finns en användarguide som beskriver syftet med riskkatalogen och förklaringar till den information som finns i respektive kapitel.

Om riskområdet

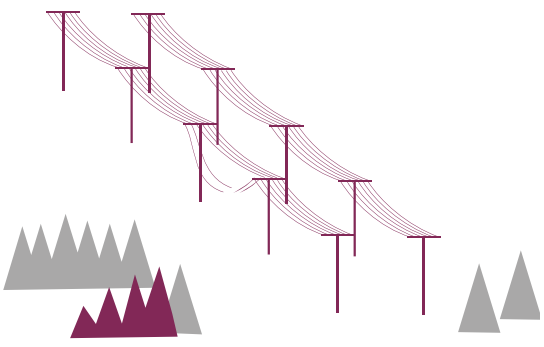
Med sabotage avses alla former av avsiktliga handlingar som genom störning eller förstörelse syftar till att försvaga en verksamhet. Enligt svensk lag är sabotage ett allmänfarligt brott, att någon förstör eller skadar egendom, som har avsevärd betydelse för rikets försvar, folkförsörjning, rättsskipning eller förvaltning eller för upprätthållande av allmän ordning och säkerhet i riket enligt 13 kap. 4 § i brottsbalken (1962:700).

Sabotage kan utföras av många olika typer av aktörer och på många olika sätt. Några exempel är ensamagerande aktörer ur våldsfrämjande extremistmiljöer, ideologiskt motiverade grupper, statliga aktörer, aktörer inom grov organiserad brottslighet samt cyberkriminella. Sabotage kan till exempel utföras av främmande makt inom ramen för hybridkrigföring i syfte att på olika sätt försöka påverka eller destabilisera funktioner och förmågor.

Sabotage kan vara av enklare karaktär eller en komplex operation riktad mot kritisk infrastruktur. Sabotage kan också vara fysiska, digitala händelser eller bådadera. Ett och samma sabotage kan drabba en eller flera samhällssektorer, det kan också bestå av en enskild händelse eller flera koordinerade sådana och kan då ske på flera ställen samtidigt eller flera gånger över tid. Det kan handla både om att helt slå ut ett system eller en verksamhet, eller att få densamma att fungera felaktigt.

Exempel på handlingar av enklare karaktär är att förstöra järnvägsspår, skära sönder bildäck, orsaka elavbrott, anlägga bränder eller påverka en central eller kritisk verksamhet till långsammare processer, till exempel genom att inte utföra arbetsuppgifter effektivt eller se till att rapporteringssystem eller -vägar, delgivningsstrukturer och kommunikationsvägar på en arbetsplats inte fungerar.

Mer avancerade former av sabotage kan exempelvis vara digitalt sabotage som cyberoperationer mot samhällsviktig verksamhet och viktiga samhällsfunktioner, eller angrepp mot energiinfrastruktur som ett kärnkraftverk, det nationella transmissionsnätet eller infrastruktur till havs. Avancerade operationer kan även riktas mot exempelvis transportinfrastruktur, sjukvård samt kommunikations- och betalsystem. Sabotage kan också riktas mot militära mål som militära anläggningar, fordon och master.



Se även

- Handbok i civil beredskap för kommuner – Elektromagnetiska hot (msb.se)
- Handbok i civil beredskap för kommuner – Kemiska och explosiva händelser (msb.se)
- Handbok i civil beredskap för kommuner – Olyckor med radioaktiva ämnen (msb.se)
- Handbok i civil beredskap för kommuner – Terrorism och extremism (msb.se)
- Handbok i civil beredskap för kommuner – Störningar i satellitbaserade navigationssystem (msb.se)

Kort om konsekvenser

Sabotage kan som sagt bestå av handlingar av både enklare och mer avancerad karaktär. Beroende på målval och tillvägagånssätt varierar därmed de potentiella konsekvenserna. Konsekvenserna kan vara fysiska men även psykologiska och påverka befolkningen i olika grader beroende på målval och omfattning. Sabotage genom cyberoperationer kan exempelvis orsaka såväl digitala konsekvenser som fysisk åverkan som i sin tur kan verka förutsättningsskapande för andra typer av skadliga handlingar. Sabotage mot energiinfrastruktur till havs kan till exempel användas för att förvägra energiförsörjning som en form av påtryckning, försvåra leveranser från en konkurrerande energiproducent och orsaka en regional störning i energitillförsel för strategiska ändamål.[1] Sabotage mot en nätstation kan leda till omfattande elavbrott medan sabotage mot tjänster för vattenförsörjning och avlopp kan slå ut dricksvattenförsörjningen i flera städer.[2]

Konsekvenserna av ett sabotage skiljer sig nödvändigtvis inte nämnvärt mellan en olycka, en oavsiktlig handling eller en avsiktlig handling, givet att aktören inte vill bli upptäckt och därför inte kommer vilja riskera upptäckt, till exempel genom att exponera en viss förmåga eller ett tillvägagångssätt, utan endast orsaka en störning eller förstörelse. Konsekvenserna i sig kan potentiellt ändå, oavsett orsak, vara långsiktiga och problematiska att hantera, till exempel vid cyberangrepp som ransomewareattacker mot digitala leveranskedjor, där utnyttjandet av sårbarheter möjliggör angreppet, snarare än en mer kvalificerad antagonist.

Läs mer

MSB har genom myndighetens instruktion fått i uppdrag att ta fram en nationell risk- och sårbarhetsbedömning (NRSB) som ska överlämnas till regeringen vartannat år. MSB har identifierat ett antal oönskade händelser som bedöms utgöra de allvarligaste och mest betydande men även realistiska hoten och riskerna mot Sverige. Om hoten realiseras är farhågorna stora att var och en av händelserna, oberoende av geografiska eller funktionella gränser, skulle få allvarliga till katastrofala konsekvenser med negativ inverkan på Sveriges nationella skyddsvärden och således ge upphov till fredstida krissituationer. Bland dessa händelser ingår sabotage mot kritisk infrastruktur.

- Nationell risk- och sårbarhetsbedömning (msb.se)

Osäkerhetsbedömning

Sabotage sker oftast i det fördolda och kan också i vissa fall vara beroende av att rätt tillfälle uppstår, såväl opportunistiskt som reaktivt, vilket gör att det kan det vara svårt att spåra vem som ligger bakom sabotaget. Givet en aktör som vill agera förnekbart och som inte vill riskera upptäckt, utan endast orsaka en störning eller förstörelse, kan det vidare vara svårt att bedöma om en händelse är sabotage eller inte. Till exempel skulle en skogs- eller vegetationsbrand kunna vara anlagd i syfte att sabotera och orsaka fysiska skador på egendom eller psykologiska effekter på en befolkning, men en brand kan också uppstå av naturliga orsaker.

Sabotage som äger rum i den maritima miljön är särskilt svåra att upptäcka och avvärja. Det är också mycket svårt att hänföra

1. Dupoy, A. C. (2021). *Energy security in the era of hybrid warfare*. Naval Postgraduate School Monterey Center For Contemporary Conflict.
2. FOI. (2021). *Hybrida hot - Scenarier och exempel som stöd för utbildning inom Polismyndigheten,* s. 23. FOI-R--5137--SE.

de potentiella handlingar som kan ha gett upphov till skadorna. En inte obetydlig del av Sveriges energiinfrastruktur återfinns på havsbotten i det omgivande territorialvattnet och den exklusiva ekonomiska zonen (EEZ). Likt cyberdomänen, som också kan användas för att angripa exempelvis elförsörjningssystem,[3] kan sabotage inom den maritima domänen användas under tröskeln för väpnad konflikt.[4] Undervattensarenans vidd och svårnavigerade operativa miljö samt det stora antalet offentliga och privata aktörer som är involverade i energiinfrastrukturprojekt under ytan, gör det komplicerat att avgöra om eventuella skador på energiinfrastrukturen på havsbotten skulle kunna vara resultat av uppsåtliga handlingar.[5] Sannolikheten för sabotage mot energiinfrastrukturen är svårbedömd. Det kan dock sammantaget konstateras att potentiella antagonister har såväl avsikt, förmåga och tillfälle att utföra sabotage mot infrastruktur som är kritisk för Sveriges energiförsörjning.[6]

Att använda angrepp mot andra länders suveränitet som inte kan härledas till avsändaren, är en känd taktik för att uppnå politiska mål. Utöver avsikten att tillgripa taktiken så har flera tänkbara aktörer även de tekniska förutsättningar som krävs för genomförande. På grund av havets vidd är den maritima domänen, trots att betydande tekniska framsteg görs, mycket svår att övervaka.[7]

Utveckling och trender

Fenomenet sabotage har funnits lika länge som krig, och har använts som ett medel för att försvaga motståndarsidan. Sabotage har också genom århundradena använts av civila aktörer, som till exempel arbetarrörelsen under den industriella revolutionen. I takt med den teknologiska utvecklingen har sabotage blivit mer sofistikerade. I dag talas det till exempel om cyberfysisk säkerhet där den fortsatta och snabbt ökande digitala uppkopplingen av saker och industriella processer i samhället har medfört att det har blivit allt svårare att separera cybermiljön och den fysiska världen. Hot och risker måste istället betraktas i en cyberfysisk kontext. När en angripare lyckas göra intrång i en uppkopplad enhet kan denne sedan försöka ta sig vidare in i andra enheter och få ytterligare tillgång till uppgifter, manipulera data och införa skadlig kod - vilket i slutänden kan drabba den fysiska miljön.[8]

Den svårarbetade miljön och betydelsen av viktig infrastruktur har lett till att sabotage under vattenytan har blivit en ny typ av konfliktzon, så kallad seabed warfare. Under ytan finns såväl gasledningar och elkablar, och internettrafik via undervattenskablar som är vitala för att samhället ska fungera såväl i vardagen, som i kris eller krig. Havsbotten har blivit betydligt mer exploaterad och ny teknisk utrustning, vapen och förbättrade fartyg ger en robustare och effektivare möjlighet att verka under ytan.

Läs mer

→ Havsbotten, en ny konfliktzon (forsvarsmakten.se)

3. Exempelvis är den skadliga programvaran Industroyer2, som upptäcktes den 12 april år 2022, ett exempel på angrepp mot energiförsörjning som, om det lyckas, kan lämna kritiska samhällsfunktioner och miljoner invånare utan ström. Liknande angrepp mot elförsörjningen i Ukraina har förekommit även under åren 2014 - 2022. Se MSB. (2023). *När kriget kom nära - Årsrapport it-incidentrapportering 2022.* MSB2179 - mars 2023.
4. Det vill säga att en aktör genomför en aggressiv handling, dock strax under nivån för vad som kan definieras som en öppen attack.
5. Rühle, M., & Grubliauskas, J. (2015). *Energy as a tool of hybrid warfare.* NATO Defense College, Research Division.
6. MSB. (2023). *Nationell risk- och sårbarhetsbedömning (NRSB) 2023. MSB 2022-11265-23.*
7. Bueger, C. & Edmunds, T. (2017). *Beyond Seablindness: A New Agenda For Maritime Security Studies.* International Affairs, International Affairs, 93(6).
8. Ingemarsdotter, J., Eidenskog, D. & Hedtjärn Swaling, V. (2020). *Vilse i lasagnen? - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur,* s. 45-74. FOI-R--4814--SE.

Exempel på inträffade händelser

Sabotage är som tidigare nämnt svåra att bevisa men nedan följer några exempel på fysiska och digitala händelser i närtid som kan definieras som sabotage.

Under 2016 utsattes Häglaredsmasten samt en mast i Tranemo för sabotage. Häglaredsmasten rasade samman efter att någon skruvat bort de muttrar som höll masten på plats och det var nära att kommunikationssystemet Rakel påverkades av sabotaget då dess antenner fanns på masten[9]. Masten i Tranemo fick en kabel sönderklippt.

I Sveriges och Danmarks exklusiva ekonomiska zoner i Östersjön genomfördes sabotage mot gasledningarna Nord Stream 1 och 2 i oktober år 2022. Sabotaget skedde genom detonationer vid gasledningarna som löper på havsbotten. Förundersökningen kring detonationerna har dock sedan lagts ned. Detta eftersom det inte anses finnas möjlighet för svenska myndigheter att bedriva utredningen vidare.[10]

Läs mer

→ Säkerhetspolisen 2022-2023 (sakerhetspolisen.se)

→ Civil-militär samverkan under ytan - Gasläckorna i Östersjön 2022 (foi.se)

I oktober år 2023 upptäcktes skador på undervattenskablar och gasledningen Balticconnector mellan Finland och Estland.

I februari år 2020 genomfördes en cyberattack mot mjukvaran som styr vattenförsörjningen i staden Oldsmar i Florida, USA, där angriparna försökte öka mängden natriumhydroxid (lut) i vattnet till farliga nivåer.[11]

I Ukraina skedde år 2015 en cyberattack mot elnätet. Angreppet inleddes med att mejl med preparerade bilagor skickades till olika eldistributörer. Bilagorna innehöll skadlig kod vilket gjorde det möjligt för angriparna att ta sig förbi brandväggar och in i styrsystemet, och därifrån ta sig vidare till sitt huvudsakliga mål. Cyberattacken ledde till att hundratusentals abonnenter blev strömlösa. Efter några timmar kunde man manuellt återstarta elnätet.[12]

Löpande riskbedömningar

I och med att sabotage är mångfacetterat, kan ske på många olika platser och på olika sätt motverkas det främst genom proaktiva åtgärder i form av bevakning, säkerhetsskydd[13] samt ökat säkerhetsmedvetande inom organisationer.

Ansvar och roller

Ett stort antal aktörer på lokal, regional och nationell nivå har olika ansvar, roller och funktioner i händelse av sabotage, däribland finns polisiära-, underrättelse och brottsförebyggande myndigheter. Det enskilda sabotagets beskaffenhet avgör vilka instanser som ansvarar för att omhänderta konsekvenserna.

9. Svt. Nyhetspublikation. Hämtad 2024-02-20: https://www.svt.se/nyheter/lokalt/vast/nara-att-rakel-drogs-med-i-fallet.

10. Säkerhetspolisen. (2024). Nyhetspublikation. Hämtad 2024-02-20: https://sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2024-02-07-forundersokning-om-grovt-sabotage-laggs-ned.html.

11. Försvarshögskolan & Livsmedelsverket. (2021). *Hotbilden mot dricksvatten- och livsmedelsområdet.*

12. Andersson, M. & Westerdahl, L. (2017). *Särtryck ur strategisk utblick 7: Sveriges elförsörjning - Hur möter vi en ökad sårbarhet?* FOI Memo 6173.

13. Säkerhetspolisen. (2023). *Fysiskt skydd.* Hämtad 2024-01-11: https://sakerhetspolisen.se/verksamheten/sakerhetsskydd/sakerhetsskyddsatgarder/fysisk-sakerhet.html.

Ett samarbete mellan:

Myndigheten för samhällsskydd och beredskap

Sveriges Kommuner och Regioner

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB2308 - maj 2024