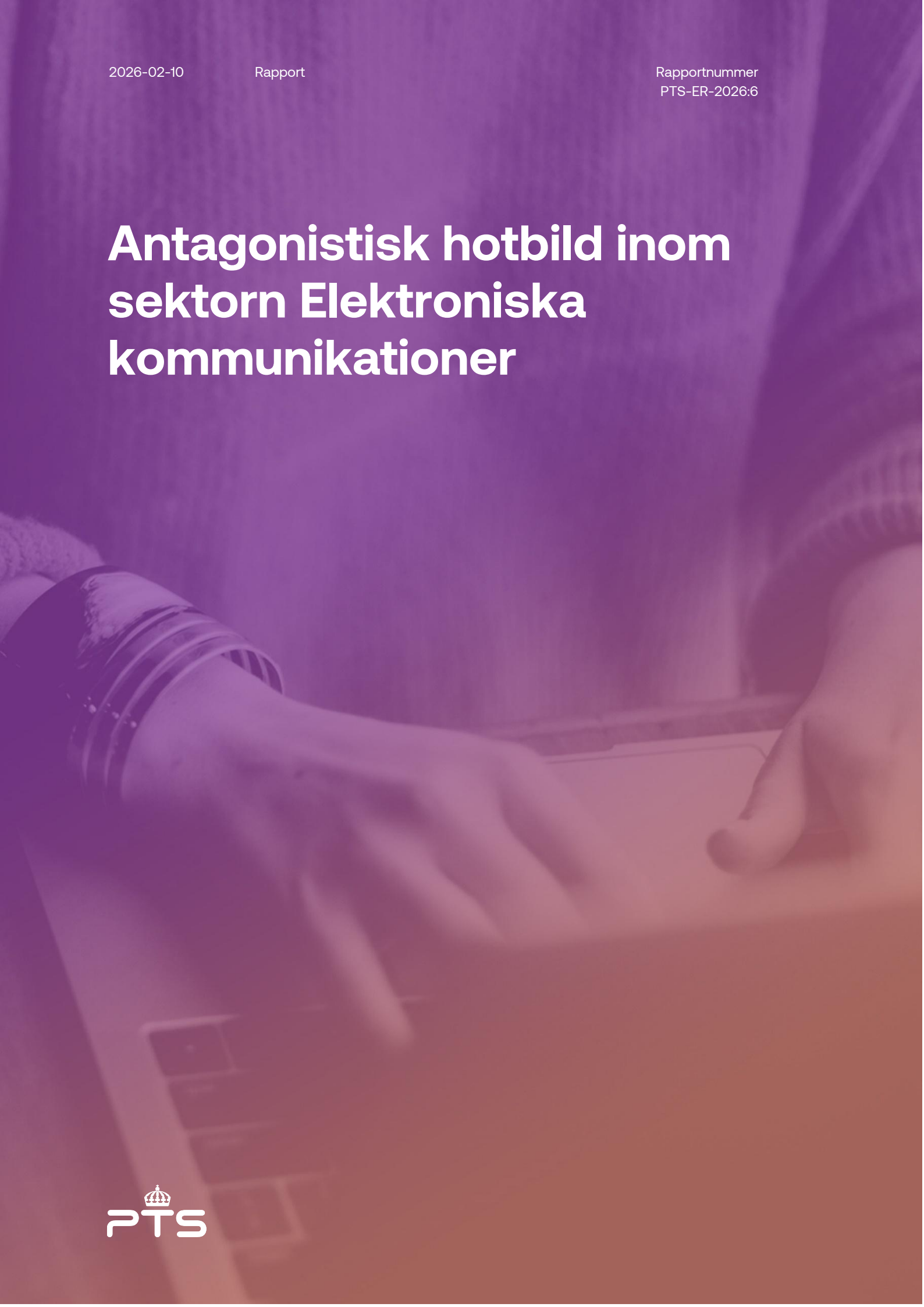
2026-02-10 Rapport Rapportnummer
PTS-ER-2026:6

Antagonistisk hotbild inom sektorn Elektroniska kommunikationer



Rapportnummer
PTS-ER-2026:6

Diarienummer
25-8907

ISSN
1650-9862

Post- och telestyrelsen
Box 6101
102 32 Stockholm

08-678 55 00
pts@pts.se
www.pts.se

Sammanfattning

Sverige befinner sig i ett allvarligt och förändrat omvärldsläge som präglas av ett ökat hot från främmande makt och antagonistiska aktörer. De senaste årens utveckling ställer ökade krav på svenska verksamheters förståelse och hantering av möjliga risker och hot, och kräver allt större fokus på verksamheternas beredskap och säkerhetsskydd.

Syftet med denna rapport är att öka medvetenhet och kunskap kring de hot som sektorn elektroniska kommunikationer och post står inför och därmed underlätta för aktörer inom sektorn att göra strategiska vägval och fatta långsiktiga beslut om beredskap och skyddsåtgärder.

De hot som sektorn möter är i grunden av samma art idag som för några år sedan. Samtidigt är de i ständig förändring och det försämrade säkerhetsläget har gjort vissa hot mer aktuella än tidigare. De senaste åren har sektorn i ökande grad drabbats av bland annat cyberangrepp, och skadade kommunikationskablar både i Östersjön och på land. I flera fall har dessa incidenter väckt misstankar om sabotage från främmande makt.

Underrättelsemyndigheterna bedömer att hotbilden mot Sverige har blivit både allvarligare och mer komplex, vilket kräver en ökad beredskapsförmåga då läget snabbt kan försämras. Alla aktörer behöver göra en egen analys av hotbilden och hur denna utvecklas till följd av förändringar i omvärlden.

Innehåll

1. Inledning

Sverige befinner sig i ett allvarligt och förändrat omvärldsläge som präglas av ett ökat hot från främmande makt och antagonistiska aktörer. De senaste årens utveckling ställer ökade krav på svenska verksamheters förståelse och hantering av möjliga risker och hot, och kräver allt större fokus på verksamheternas beredskap och säkerhetsskydd.

Vårt samhälle knyts samman genom elektronisk kommunikation. Vi människor når varandra, våra digitala tjänster och vår information genom den. De digitala och fysiska system som finns överallt i samhället kommunicerar elektroniskt med varandra. Att elektroniska kommunikationer fungerar som de ska är därför helt avgörande för samhällets funktionalitet.

Elektroniska kommunikationer är också ett viktigt område inom det civila försvaret. I händelse av höjd beredskap eller krig måste kommunikationerna vara resilienta för att i så stor utsträckning som möjligt fungera utan avbrott. Åtgärder för snabb respons, trafikstyrning och reparationer behöver också vara dimensionerade för att minska effekterna av mänsklig påverkan. Det är därför viktigt att aktörer inom sektorn är medvetna om risker och hot, och vidtar nödvändiga åtgärder för att förebygga, och vid behov hantera dem.

Post- och telestyrelsen (PTS) är sektorsansvarig myndighet för Beredskapssektorn *elektroniska kommunikationer och post*. Enligt förordningen (2022:524) om statliga myndigheters beredskap har PTS ansvar att leda arbetet och samordna åtgärder inom sektorn i såväl fredstid som under kriser och vid höjd beredskap. Detta dokument är avsett som ett stöd till sektorns aktörer i arbetet med att identifiera risker och hot som kan påverka elektroniska kommunikationer.

1.1 Syfte

Syftet med denna rapport är att öka medvetenhet och kunskap kring de hot som sektorn står inför hos aktörer inom sektorn och därmed underlätta för dem att göra strategiska vägval och fatta långsiktiga beslut om beredskap och skyddsåtgärder.

1.2 Källor

Underlag till denna rapport har hämtats från rapportering till PTS, bland annat incidentrapportering enligt LEK, identifierade radiostörningar, NIS-rapportering[1], EU- och Natosamverkan genom exempelvis Natos planeringsgrupp för civila kommunikationer (CCPG[2]). Information är även hämtad från årsrapporter från Säkerhetspolisen, Försvarets radioanstalt (FRA), Nationellt centrum för terrorhotbedömning (NCT), Militära underrättelse- och säkerhetstjänsten (Must) samt Nationella cybersäkerhetscentret (NCSC).

1.3 Avgränsningar

Rapporten omfattar endast området elektroniska kommunikationer.

Dokumentet ger en översiktlig bild över hot, risker och sårbarheter. Det är viktigt att alla aktörer själva analyserar hot och risker som kan påverka den egna verksamheten.

Rapporten bör läsas i kombination med ytterligare källor från underrättelsemyndigheter, se exempel nämnda i avsnitt 1.2 *Källor*.

1.4 Målgrupp

Målgruppen för hotbilden är framför allt mindre aktörer, operatörer och stadsnätsföreningar inom sektorn elektroniska kommunikationer.

[1] Sedan 2018 har det skett både obligatorisk och frivillig rapportering enligt NIS (EU:s direktiv om *Network and Information Security*).

[2] Civil Communications Planning Group.

2. En förändrad omvärld

2.1 Omvärldsläget – vikten av stärkt beredskapsförmåga

Underrättelsemyndigheterna bedömer att hotbilden mot Sverige har blivit både allvarligare och mer komplex, vilket kräver en ökad beredskapsförmåga då läget snabbt kan försämras.

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

2.1.1 Sveriges Natomedlemskap

Till följd av Rysslands invasion av Ukraina i februari 2022 ansökte Sverige, tillsammans med Finland, om medlemskap i Nato. Sedan den 7 mars 2024 är Sverige fullvärdig medlem i alliansen. Sedan dess har det säkerhetspolitiska omvärldsläget försämrats ytterligare med en ökad upprustning som följd. I samband med Natos toppmöte i Haag sommaren 2025 beslutade medlemsländerna att årligen lägga 5% av BNP på försvaret. För Sveriges del har det inneburit fokus på att rusta upp totalförsvaret, att fullt integrera Sverige i Nato och att stötta Ukraina.

2.1.2 Lärdomar från kriget i Ukraina

Rysslands krigsföring i Ukraina har visat att infrastrukturen för elektroniska kommunikationer varit ett primärt mål sedan kriget bröt ut. Ryssland har attackerat med flygbomber, drönare och artilleri, kompletterat med cyberattacker,[3] vilket lett till omfattande och mycket kostsam förstörelse av kritisk infrastruktur. Efter Rysslands invasion av Ukraina sågs en våg av överbelastningsattacker mot olika europeiska mål och enligt Europol koordinerades dessa av pro-ryska hackergrupper.

När den största ukrainska telekomoperatören Kyivstar utsattes för ett omfattande cyberangrepp 2023 uppgav Ukrainas säkerhetstjänst (SBU) att det är första gången som en operatörs kärnnät[4], slagits ut. SBU fastslog även att antagonisten varit inne i

[3] *The internet under attack*, chathamhouse.org, 240823.

[4] Ett mobilnäts centrala delar som omfattar viktiga funktioner och databaser, utan vilka systemet inte fungerar

operatörens nät så långt som sex månader i förväg. En konsekvens av attacken var att många butiker inte kunde genomföra kreditkortsköp, bankomater slutade fungera och viktiga funktioner såsom flyglarm slogs ut. Cyberangreppet medförde även att många invånare blev utan såväl mobiltelefoni som internet. Det tog en vecka för Kyivstar att reparera skadan, vilket krävde att ett tusental nätverkstekniker arbetade med hanteringen[5].

Internationella teleunionen (ITU) har emellertid rapporterat att Ukraina har uppvisat en överraskande hög resiliens vid angrepp mot elektroniska kommunikationer. En förklaring är Ukrainas beredskap med bland annat mobila servicekontor för att upprätthålla grundläggande samhällstjänster.

Kriget i Ukraina har aktualiserat ett antal utmaningar i att upprätthålla infrastruktur och tjänster för elektroniska kommunikationer i krig:

- Mobilnät är beroende av stabil strömförsörjning. Trots att operatörerna ofta har reservkraft i form av batterier eller generatorer har reservkraften inte alltid räckt till vid mer långvariga elavbrott.
- Personlig säkerhet för reparatörer.
- Svårigheter att upprätta och upprätthålla leveranskedjor.
- Teknisk utveckling har varit nödvändig under pågående krig för att kunna upprätthålla bland annat blåljuskommunikation, vilket har varit mest kritiskt i de frontnära områdena.[6]
- Vikten av kreativitet i att kunna använda olika teknologier (såsom fiberoptiska drönare i stället för radiostyrda)[7], tillämpning av diversitet i elektroniska kommunikationer för att säkerställa tillgänglighet (t.ex. över wifi till satellitkommunikationer såsom Starlink)[8] samt dynamisk anpassning av mobilnäten för att taktiskt kunna stödja eller stävja luftburna militära operationer[9].
- Utmaningar med personalförsörjning. Inom elektroniska kommunikationer är personalförsörjningen en utmaning redan i fredstid.

En tydlig och framgångsrik strategi från ukrainska myndigheter och operatörer har varit att genomföra snabba reparationer och att optimera tillgängliga tjänster. Samtidigt har kriget visat på riskerna med att förlita sig på enskilda företag.

---

[5] *Cyber attack destroys 40 % of Kyivstar's infrastructure*, Interfax Ukraine, 231222.
[6] *Ukraine digital development country profile*, itu.int, maj 2025.
[7] Uppdatering uao mot fiberoptiska drönare, Ukraine Aid Ops, juni 2025.
[8] *Starlink to Help Ukraine Create Public WiFi Hotspots*, Gwaramedia.com, 250930.
[9] *Ukraine considers limiting mobile service to counter Russian drones*, The Economic Times, 250914. Och *Communications under threat: will Ukraine start jamming mobile internet due to drone attacks?*, Visit Ukraine, 250613.

2.2 Antagonistiska aktörer

Antagonistiska aktörer delas ofta in i olika typgrupper utifrån vilka motiv de har. Med främmande makt menas andra stater som i princip motiveras av att befästa eller utöka sin makt. Våldsbejakande extremister drivs i stället av ideologiska motiv, medan organiserad brottslighet söker ekonomisk vinning. Därutöver förekommer ibland en blandning av dessa motiv och antagonistiska aktörer använder ibland varandra för att uppnå sina mål.

2.2.1 Främmande makt

Svenska underrättelsemyndigheter bedömer att de största hoten mot Sverige kommer från Ryssland, Kina och Iran. Säkerhetspolisen är tydliga med att även det civila försvaret är mål för Rysslands informationsinhämtning.

Statliga hotaktörer har generellt sett en hög uthållighet i kombination med betydande resurser och kunskap. Denna typ av aktör har ofta flera olika syften och mål i sitt agerande för att sabotera och störa.

Efter den fullskaliga 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. NCT nämner specifikt att främmande makt kan använda sig av icke-statliga aktörer som ombud för våldsutövning, eller på andra sätt utöva våld under täckmantel.

2.2.2 Terrorism och våldsbejakande extremism

Terroristbrott omfattar brottsliga handlingar som sker i syfte att skrämma och hota befolkningen och som riskerar att allvarligt skada en stat. Säkerhetspolisen har identifierat tre samhällsviktiga sektorer som särskilt kan riskera att drabbas av angrepp från dessa antagonister. En av dessa är sektorn elektronisk kommunikation, där terrorism genom cyberattacker riskerar att hota exempelvis nödkommunikation eller att överbelasta nätverk.

2.2.3 Organiserad brottslighet

Organiserad brottslighet innebär att personer samarbetar, ofta över landsgränser, för att systematiskt begå allvarliga brott. Brottsligheten kan även stödjas av stater. Exempel på statsunderstödd kriminalitet kan vara vapensmuggling, sanktionsbrott, skeninvandring, människoexploatering, påverkanskampanjer, samt att individer agerar bulvaner för köp av taktiskt eller strategiskt intressanta tillgångar (som exempelvis fastigheter i närheten av skyddsobjekt) eller köp av tjänster för cyberangrepp.

3. Antagonistiska hot

De hot som sektorn möter är i grunden av samma art idag som för några år sedan. Samtidigt är de i ständig förändring och det försämrade säkerhetsläget har gjort vissa hot mer aktuella än tidigare.

De senaste åren har sektorn i ökande grad drabbats av bland annat cyberangrepp, och skadade kommunikationskablar både i Östersjön och på land. I flera fall har dessa incidenter väckt misstankar om sabotage från främmande makt[10].

Alla aktörer behöver göra en egen analys av hotbilden och hur denna utvecklas till följd av förändringar i omvärlden.

3.1 Cyberhot

Cyberhot har blivit del av den nya normalbilden för Sverige. Med cyberangrepp menas avsiktligt skadliga handlingar i syfte att bland annat spionera, stjäla eller sabotera. Antagonisterna kan använda sig av skadlig kod, nätfiske eller personlig kontakt för att på falska grunder tilltvinga sig känsliga uppgifter. Sabotage kan bland annat ske genom överbelastningsattacker. Offentlig sektor är särskilt utsatt givet den stora mängden information som den lagrar.

Hacktivism är en form av cyberkriminalitet där individer eller organisationer använder cyberdomänen för att nå ut med ett politiskt eller ideologiskt budskap. De senaste åren ses en tendens att individerna allt oftare utgörs av statligt mobiliserade grupper. Främmande makt kan även använda sig av cyberkriminella för att dölja sitt motiv.

Det egentliga målet för en antagonist kan vara att komma över data i IT-system, men även att sabotera funktionalitet eller kommunikationskanaler.

Ytterligare angreppsätt kan vara att antagonisten etablerar en dold närvaro i IT-system som styr telefoni, fiber eller elförsörjning. Till skillnad från ett direkt cyberangrepp, exempelvis en överbelastningsattack, är strategin att en sådan operation inte ska märkas alls. Här går den tekniska utvecklingen snabbt framåt och

[10] Säkerhetspolisens lägesbild 2024-2025, sakerhetspolisen.se

angripare kommer i allt större utsträckning att kunna använda bland annat AI för att utveckla sin förmåga till avancerade attacker.

3.2 Fysisk skadegörelse och sabotage

Skadegörelse och sabotage är vanligt förekommande i sektorn och det kan vara svårt att avgöra vilka motiv som ligger bakom. Det är inte heller säkert att den som utför angreppet känner till motivet, och flera angrepp kan koordineras på ett sätt som är svårt att överblicka även för den eller de som utför dem. Det kan röra sig om sönderslagna elskåp och master, batteristölder, avklippta kablar, sprängningar, angrepp mot skalskydd och mycket annat. Händelserna kan vara försumbara var och en för sig men tillsammans kan de bli ett problem.

3.3 Underrättelsehot

Ett underrättelsehot innebär att antagonistiska aktörer försöker inhämta känslig eller hemlig information om ett land eller verksamheter inom landet. Det kan handla om spionage eller värvning av personal, men även om cyberangrepp eller påtryckningar för att komma åt känslig information. En antagonistisk aktör kan sedan använda sig av information som de tillskansat sig för att bland annat utföra sabotage.

Ett exempel på detta sågs i Tyskland år 2022, då antagonistiska aktörers goda kännedom om redundansen i radionätet för tågtrafik hjälpte dem att utföra två välriktade kabelbrott. Till följd av detta påverkades järnvägen och höghastighetståg tvingades stå stilla i flera timmar.

3.4 Insiders och nyttiga idioter

En antagonist kan också välja att försöka värva personer som har tillgång till känslig information på en arbetsplats och på så vis få en så kallad insider. Detta kan ske genom tvång och utpressning men det kan även ske genom att den anställde frivilligt lämnar ifrån sig information, mer eller mindre medvetet. En så kallad nyttig idiot kan också värvas för att utföra sabotage av olika slag utan att förstå innebörden.

3.5 Obemannade luftfarkoster – drönare

Hotet från drönare blir alltmer aktuellt. Drönare kan bland annat användas för att kartlägga infrastruktur, påverka infrastrukturen med vapenverkan eller användas som bärare av störsändare. Drönare kan användas för att utföra sabotage, både i fred och under krig. En lärdom från Rysslands anfallskrig i Ukraina är att drönare är ett hot som behöver vara dimensionerande för skyddsåtgärder. Utvecklingen av både drönare och teknik för att upptäcka och motverka dem går i snabb takt.

3.6 Sårbarheter som har fått ökad aktualitet

3.6.1 Undervattensinfrastruktur

Hot mot undervattensinfrastruktur, eller undervattenskablar, är ett område som fått alltmer uppmärksamhet de senaste åren. Hotbilden är komplex och inkluderar alltifrån sabotage, spionage och annan fientlig aktivitet från främmande makt, till rena olyckshändelser. Precis som med skadegörelse och sabotage av markbunden infrastruktur kan det vara svårt att veta om exempelvis ett kabelbrott skett medvetet eller varit en olycka till följd av okunskap eller oaktsamhet, ibland kanske skadan uppstått av helt vanligt åldersslitage. Redundanta kablar och internets inneboende redundans minskar risken för kännbara konsekvenser, men angreppen innebär samtidigt en försvagning av systemet som helhet. Oaktat detta är undervattensinfrastrukturen ett viktigt och sårbart område som kräver extra bevakning och uppmärksamhet.

3.6.2 Reservdelstillgång och leverantörskedjor

Antagonister kan rikta in sig på att stjäla eller förstöra reservdelskomponenter och utrustning som behövs för att trygga redundans i sektorn. Syftet kan vara ekonomisk vinning, men det kan även handla om sabotage eftersom reserv- eller byggmateriel är en bristvara som kan ta lång tid att ersätta. Lärdomar från kriget i Ukraina visar på vikten av att snabbt kunna reparera och återställa skadad infrastruktur.

3.6.3 Rymddomänen

De senaste åren har även hoten inom rymddomänen uppmärksammats alltmer. Tre exempel på hot som har identifierats är underrättelsehot, radiostörningar och cyberhot. Underrättelsehotet innebär att antagonister kan nyttja olika rymdsystem för att samla in känslig militär och civil information. Cyberhotet utgörs främst av angrepp mot satelliter vilka kan störas eller förstöras för att slå ut de tjänster och förmågor de bidrar till.

Avsiktliga radiostörningar har hittills framför allt påverkat länder med landgräns mot Ryssland, men även Sverige och svenska operatörer inom exempelvis sjö- och flygtrafik har påverkats.

Sedan 2024 har en svensk satellit utsatts för skadliga störningar med ursprung i Ryssland. Ärendet har hanterats av PTS inom ramen för ITU:s etablerade processer, inklusive två bilaterala möten mellan Sverige och Ryssland. Ryssland uppger att störningarna härrör från ryska militära anläggningar och att tekniska detaljer därför inte kan lämnas, men att en vilja till samarbete finns. Störningarna har emellertid fortsatt med varierande grad av påverkan. Det är oklart i vilken utsträckning som störningarna har påverkat satellitleverantörens tjänsteleverans.

Sedan 2022 pågår också regelbundna störsändningar från ryskt territorium kring Östersjön. De störande radiosignalerna påverkar framför allt GNSS[11]-tjänster, dvs. satellit-baserade navigeringstjänster som exempelvis GPS, men på senare tid har även störningar av mobiltelefonitjänster noterats av länder närmare Ryssland. Störsändningarnas primära syfte är inte nödvändigtvis att påverka civil användning av radionavigeringstjänster utan kan avse att försvara ryska tillgångar från attacker med exempelvis drönare. Störsändningarna från ryskt territorium ökar risken för skadekonsekvenser på svensk verksamhet. Luft- och sjöfart över Östersjön är särskilt sårbar och GNSS-tjänsterna i detta område bör betraktas som mindre tillförlitliga än normalt. Flera svenska myndigheter arbetar långsiktigt för att stärka svensk beredskap och motståndskraft mot negativ påverkan till följd av radiostörningar.[12]

[11] Global navigation Satellite Systems

[12] *Submission by the administrations of Estonia, Finland, Latvia and Lithuania, concerning harmful interference to receivers in the radionavigation-satellite and mobile services, Document RRB25-2/19-E*, ITU, *Radio Regulations board* 14-18 juli 2025.