TRAFIKVERKET

RAPPORT

Öppen antagonistisk hotbild mot transportsektorn

NOVEMBER 2025

Till dig som läser en nedladdad eller utskriven kopia av detta dokument:
Kontrollera att du har den senaste versionen från Trafikverkets hemsida.
Version november 2025

Trafikverket
Postadress: Luntgatan 28, 602 19 Norrköping
E-post: trafikverket@trafikverket.se
Telefon: 0771-921 921

Konfidentialitetsnivå: 1 – Ej känslig
Dokumenttitel: Öppen antagonistisk hotbild mot transportsektorn
Författare: Jens Johanson, Senior säkerhetsstrateg
Dokumentdatum: 2025-11-10
Ärendenummer: TRV 2024/25605
Version: November 2025
Fastställd av: Mattias Dejke, Säkerhetsdirektör

Publikationsnummer: 2025:168
ISBN 978-91-8045-525-1 (digital version)
ISBN 978-91-8045-526-8 (tryckt version)

Foto: Trafikverket, Johnér Bildbyrå och Mostphoto

Tryck: Åtta45 Tryckeri AB

Innehåll

Sammanfattning

Omvärlden har förändrats och hotbilden mot Sverige har både breddats och fördjupats. Det påverkar också transportsektorn och de aktörer som verkar inom den, både offentliga och privata. Mycket av det som berörts i den version av detta dokument som publicerades i oktober 2024 gäller än i dag och har inte reviderats. Vissa tidigare kända antagonistiska tillvägagångssätt har intensifierats. Samtidigt har andra, tidigare självklara uppfattningar fått ses i ett nytt ljus. Ett exempel är den världspolitiska förändringar som uppstått efter valet i USA 2024 och den oro som präglat världen under våren 2025, med diskussioner om både tullar och Trumpadministrationens intresse för Grönland.

Alla aktörer behöver ta ett större ansvar för att öka motståndskraften inom den svenska transportsektorn – var för sig och tillsammans. Som Ulf Kristersson, statsminister, uttryckte det under rikskonferensen Folk och Försvar 2025:

Låt oss planera för det värsta, så vi kan fortsätta hoppas på det bästa[1].

En av de tillförda aspekterna som lyfts fram i denna version av sektorshotbilden, jämfört med tidigare version, är tidsperspektivet för totalförsvarsåtertagandet (se avsnitt 2.2.3.1). Syftet är att skapa medvetenhet om att den största bristen är bristen på tid, att den största sårbarheten är oförmågan att förstå att totalförsvarets grundläggande idé är att det omfattar hela samhället och att den viktigaste egenskapen är viljan att agera.

Hotbilden mot den svenska transportsektorn har blivit allvarligare och mer komplex

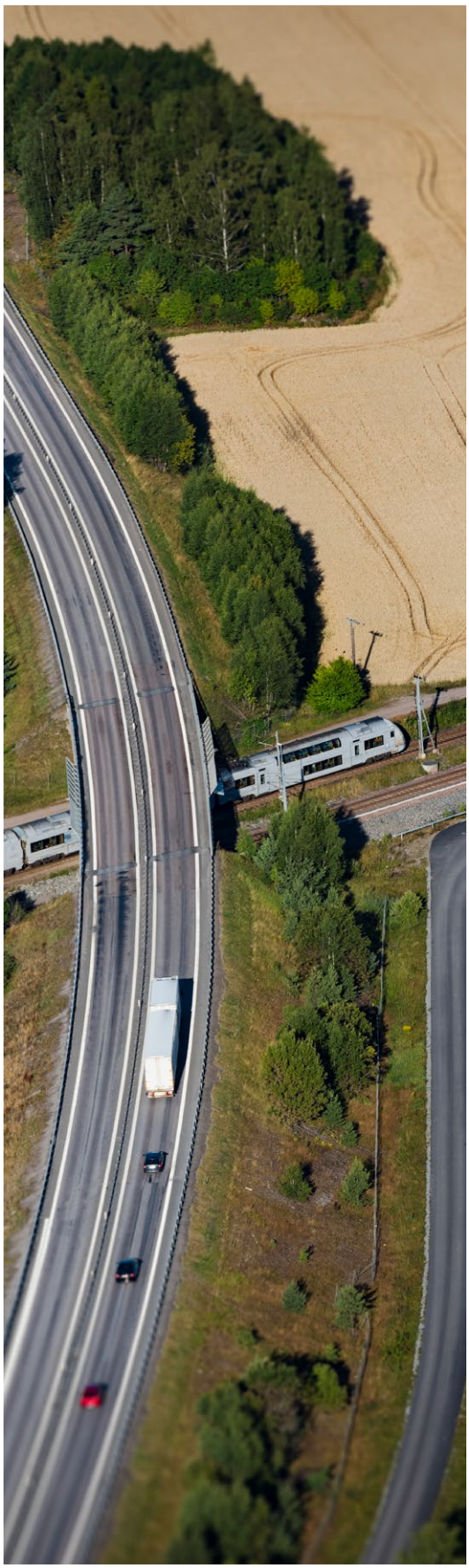
Transportsektorn är en del av den svenska vitala infrastrukturen, vilket innebär att all verksamhet inom den kommer att utvärderas av en antagonist. Hotbilden mot transportsektorn är komplex, i och med att den utgörs av ett spektrum av hot och antagonister. Komplexiteten ökar också i takt med att digitaliseringen och globaliseringen ökar. Hotbilden har blivit allvarligare under de senaste åren och främmande makt agerar alltmer offensivt. Det ökade hotet kommer från flera håll och på flera sätt.

Samtidigt har omvärlden förändrats snabbt under det senaste året. Tidigare ansågs det vara osannolikt att Sverige eller dess allierade skulle utsättas för ett militärt angrepp, men i dag kan det inte längre uteslutas och det militära hotet från Ryssland är uttalat.

Utvecklingen i Sverige och omvärlden visar hur svårbedömda och komplexa hoten är och hur de i allt större utsträckning sammanflätas och går in i varandra.

Charlotte von Essen, säkerhetspolischef

I den nationella säkerhetsstrategin[2] beskrivs hur hoten mot vår säkerhet som kommer från omvärlden och de som kommer inifrån Sverige i dag är nära sammanflätade. Det gör att hotbilden måste ses som en helhet, även om kriget och kriminaliteten bedöms vara de huvudsakliga hoten mot Sveriges säkerhet.



1 https://www.regeringen.se/tal/2025/01/statsministerns-tal-pa-folk-och-forsvars-rikskonferens-i-salen/. (Kontrollerad 2025-07-22).

2 Nationell säkerhetsstrategi. Skr: 2023/24:163. Regeringskansliet, 2024.

Ryssland, Kina och Iran är de länder som utgör de största hoten mot Sverige, enligt Säkerhetspolisen. Alla tre nationer bedriver underrättelseverksamhet och säkerhetshotande verksamhet i och mot Sverige[3], med såväl lagliga som olagliga metoder.

Det ryska anfallskriget mot Ukraina, som är ett uttryck för Rysslands vilja att stöpa om de säkerhetspolitiska förhållandena i Europa, innebär ett ökat hot även mot Sverige. Att Sverige blev medlem i Nato bedöms minska risken för direkt markangrepp från Ryssland, men det ökar troligen risken för rysk påverkan på andra sätt – det så kallade hybrida hotet. Under 2024 har den svenska säkerhetspolisen varnat för en eskalerande fara för ryska sabotageoperationer på svensk mark och under 2025 har vi sett exempel på koordinerade sabotage mot infrastruktur[4].

Många av de antagonistiska aktiviteterna sker i det som brukar kallas för gråzonen – gränslandet mellan fred och väpnad konflikt och mellan laglig och olaglig verksamhet. Främmande makter bedriver exempelvis spioneri, strategiska uppköp och elektroniska angrepp mot Sverige. Numera är det även tydligare inriktat mot att påverka svenskt beslutsfattande, till exempel inom handel, utrikes relationer, säkerhet och försvar. Andra syften är att hindra Sverige från att ta emot eller komma andra till hjälp, försvaga Sverige inför en militär konflikt, störa stödet till Ukraina eller belasta det europeiska samarbetet.

Det senaste året har rymddomänens betydelse för samhällets säkerhet uppmärksammats på bred front. Användandet av rymdtjänster för positionering och kommunikation är centralt inom transportsystemet. Därför har rymddomänen lyfts fram särskilt i syfte att medvetandegöra läsaren i sakfrågan och inspirera till eftertanke om påverkan i den egna verksamheten.

Skyddet av transportsystemet behöver stärkas

Försvarsmakten och Säkerhetspolisen skickar i dag skarpare och tydligare budskap om attentatsrisken mot kritisk infrastruktur. I Försvarsmaktens rapport Skyddsvärden för försvaret av Sverige[5] redogörs kort för att skyddsvärden i det militära försvaret inte enbart återfinns inom Försvarsmakten, utan även inom andra säkerhetskänsliga offentliga och privata verksamheter. Medvetenheten om detta är central då ett flertal myndigheter och organisationer samt delar av näringslivet har viktiga roller i, eller bidrar till, det militära försvaret och därmed det svenska totalförsvaret.

Redan efter sabotaget mot gasledningarna Nordstream 1 och Nordstream 2 hösten 2022 uppmanade Säkerhetspolisen aktörerna som ansvarar för central infrastruktur inom energiförsörjning att skärpa sin förmåga att upptäcka och förhindra incidenter. Något som fortfarande är aktuellt i allra högsta grad.

Det bästa skyddet är att öka medvetenheten och samverka

Transportsystemet är ett komplext system och många aktörer är med och bidrar till att det fungerar. Varje aktörs verksamhet är nära sammankopplad med andra aktörers verksamheter, vilket gör att transportsystemet bygger på samarbete. Detta gäller också nu när vi behöver stärka skyddet av det – vi behöver se transportsystemet som en helhet. Eftersom hotbilden är komplex och ibland diffus, behöver transportsektorns aktörer bygga upp en bred motståndskraft.

Den militära avskräckningsförmågan är välkänd och upprätthålls av Försvarsmakten, men på samma sätt behövs en medvetenhet om behovet av en civil avskräckningsförmåga vilken visar att det kommer att krävas mycket av en angripare för att påverka oss som samhälle. Denna byggs genom en vilja och en motståndskraft som har sin grund i den enskilde individens förmåga att motstå påverkan. För att stå emot hoten mot Sverige behöver vi hålla ihop och ta ansvar för vårt land. Blir vi angripna måste alla hjälpa till att försvara Sveriges självständighet och vår demokrati[6].

Det är svårt att fastställa generella riktlinjer för hur varje enskild del av transportsektorn ska arbeta med säkerhet, eftersom de antagonistiska metoderna är föränderliga. Den bästa skyddsmetoden är därför ökad kunskap och samverkan. Det vill säga att varje aktör ökar sin medvetenhet om hur hotbilden ser ut och att aktörerna sedan ökar samverkan inom området säkerhet.

Genom att dela lägesuppfattning och händelser i de forum som finns inom transportsektorn kan vi skapa en helhetsbild av säkerhetshotet tillsammans. Då blir det också lättare att identifiera större säkerhetshot som kan behöva analyseras och bemötas under ett sektorsansvar.

3 Årsrapportering 2023-2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

4 https://www.svt.se/nyheter/inrikes/granskning-angrepp-mot-30-tal-telemaster-utreds-som-sabotage (Kontrollerad 2025-08-01).

5 Skyddsvärden för försvaret av Sverige – Att identifiera säkerhetskänslig verksamhet. Militära underrättelse- och säkerhetstjänsten, MUST. Försvarsmakten, 2025.

6 Om krisen eller kriget kommer. ISBN: 978-91-7927-527-3. Myndigheten för samhällsskydd och beredskap, 2024.

1 Inledning

Trafikverket är utpekad sektorsansvarig beredskapsmyndighet för den svenska transportsektorn[7]. Inspirerat av det uppdraget publicerade Trafikverket den första versionen av detta dokument i oktober 2024 – ett övergripande stöddokument om den antagonistiska hotbilden, de antagonistiska aktörerna och exempel på antagonistiska tillvägagångssätt, som har betydelse för transportsektorn i Sverige.

Dokumentet riktar sig till både offentliga och privata aktörer och intressenter inom transportsektorn. Det syftar i första hand till att vara ett underlag för aktörernas fördjupade arbete inom beredskaps- och säkerhetsområdet. Det kan också användas av aktörerna i dialogen med samarbetspartners. Omvärldsbilden som presenteras beskrivs genom en sammanställning av information från huvudsakligen offentliga publikationer.

Tanken är således att dokumentet ska skapa förståelse för omvärldens och säkerhetshotets komplexitet och därigenom underlätta för transportsektorns aktörer att göra strategiska vägval och fatta långsiktiga beslut om skyddsåtgärder. Dokumentet tar därför upp bedömningar på en övergripande nivå.

Med antagonistiska, eller aktörsdrivna hot avses medvetna och/eller uppsåtliga beteenden och angrepp av skilda slag som kan påverka verksamheten direkt eller indirekt. Detta särskiljs från olyckor som orsakats av andra omständigheter som exempelvis väder eller slarv. Det antagonistiska perspektivet omfattar underrättelsehotet, påverkan eller angrepp från statsaktörer, terrorism och organiserad brottslighet med flera.

1.1 Målgrupp och syfte

Detta dokument riktar sig till såväl offentliga som privata aktörer och intressenter inom transportsektorn. Syftet med dokumentet är att det ska fungera som en kunskapshöjning brett inom transportsektorn och att det ska kunna nyttjas vid exempelvis utbildning, framtagande av skyddsåtgärder samt strategiska analyser.

1.2 Avgränsning

Hotbilden baseras huvudsakligen på öppna källor vilket gör att den avhandlar hot och aktörer med ett generellt perspektiv. Varje aktör behöver genomföra ett eget arbete med att analysera hot mot den egna verksamheten. I det arbetet är detta dokument ett underlag att beakta, men det kan inte anses vara garanterat heltäckande i samtliga förekommande verksamheter.

1.3 Om denna version

Denna version är en uppdatering av sektorshotbilden som publicerades i oktober 2024. Om du läser en nedladdad eller utskriven kopia av detta dokument, kontrollera att du har den senaste versionen från Trafikverkets hemsida. Detta är versionen från november 2025.

7 SFS 2022:524. Förordning om statliga myndigheters beredskap.

2 Omvärlden

Ambitionen med det här dokumentet är att belysa ett brett spektrum av antagonistiska hot mot transportsektorn. Den svenska bilden av omvärlden har de senaste åren reviderats inom ett antal områden. Tidigare ansågs det vara osannolikt att Sverige eller dess allierade skulle utsättas för ett militärt angrepp, vilket idag inte uteslutas och det militära hotet från Ryssland är uttalat. Mycket av det som berörts i föregående version av detta dokument gäller än i dag. Vissa tidigare kända antagonistiska tillvägagångssätt har intensifierats. Samtidigt har andra, förut självklara, uppfattningar fått ses i ett nytt ljus, exempelvis efter valet i USA 2024 och den politiska oro som kommit att prägla världen under våren 2025 med diskussioner om både handelsrelationer och Trump-administrationens intresse för Grönland. Det har handlat om handelskonflikter, tullar, europeiska beroenden av amerikanska molntjänster och Ukrainas beroende till satellitklustret Starlink och turerna kring hotet om att få denna resurs förvägrad, för att nämna några.

I en orolig omvärld sker snabba förändringar som kan få långsiktiga konsekvenser både för transportsektorn och för de aktörer som verkar inom den. En slutsats inför detta är att en långsiktig strategi för att nå långsiktiga mål kan vara det som skapar stabilitet i verksamheten. Givetvis kan strategin behöva justeras utifrån förändrade förutsättningar, men detta bör alltså lämpligen ske med eftertanke och efter analys av helheten. Kort sagt handlar det om att målmedvetet forma sin egen framtid. Det kan dock vara lätt att hamna i en situation där man reflexmässigt reagerar på plötsliga skiftningar i omvärlden, i synnerhet politiska utspel och låta detta påverka verksamhetens fokus nästan dagligen genom snabba och förhastade slutsatser. Sker detta är det av vikt att då inse att detta i sin tur kan leda till att man som aktör i stället blir förutsägbar och lättmanipulerad.

Det finns således en påtaglig risk att säkerhetsläget kan försämras ytterligare och att det kan ske på sätt som är svåra att förutse. Ett sätt att hantera detta och motstå manipulation är att med en långsiktig målmedvetenhet, regelbundet och strukturerat, analysera den verklighet som man lever och verkar i och samtidigt acceptera att man kan behöva fatta beslut utifrån ofullständiga uppgifter.

I det här kapitlet beskrivs omvärldsläget och komplexiteten i dagens krigföring. Det lyfter också fram säkerhetshotet mot Sverige i allmänhet och transportsektorn i synnerhet. Särskilt beskrivs också hotbilden inom domänerna rymd, Arktis, havsbotten, artificiell intelligens, tystnadskultur samt obemannade luftfarkoster.

2.1 En global oro

Omvärldsläget har förändrats och det har under 2025 blivit alltmer turbulent. Vi ser Rysslands fortsatta anfallskrig mot Ukraina, den instabila situationen i Mellanöstern exemplifierat med konflikten mellan Israel och Iran, det fortsatta kriget i Gaza med direkta följdeffekter på transportkedjan genom till exempel Röda havet. Detta innebär att det fortfarande föreligger ett hot mot Sverige. Vidare utmanar Kina fortsatt västvärlden och hävdar sina intressen, även om tillväxten i landets egna ekonomin riskerar att bli lidande[8].

Säkerhetspolischefen beslutade den 23 maj 2025 att sänka terrorhotnivån från högt hot (4) till förhöjt hot (3) en femgradig skala, som ett resultat av en samlad bedömning[9].

Den samlade bilden är att det är en svårseparerad kombination av statsaktörer och organiserade kriminella som huvudsakligen utgör ett hot även mot den som verkar inom transportsektorn. Exempelvis har kriminella organisationer och nätverks användande av insiders uppmärksammats de senaste åren. Detta ställer krav på såväl att organisationens personalsäkerhet är ändamålsenlig som att arbetsprocesser och tekniska system minimerar insiderns möjligheter att agera.

8 Gråzonsläge i krig och fred. FOI-R-5447. Totalförsvarets forskningsinstitut, juni 2023.

9 https://www.regeringen.se/pressmeddelanden/2025/05/sakerhetspolisen-har-beslutat-om-sankt-terrorhotniva/ (Kontrollerad 2025-07-18)

2.1.1 Kriget i Europa

Det fullskaliga ryska anfallet mot Ukraina i februari 2022 undanröjde alla tvivel om att en väpnad konflikt kan inträffa i Europa och dess närområde. Den ryska aggressionen ligger i linje med viljan att stöpa om de säkerhetspolitiska förhållandena i Europa, något den ryska regimen har framfört sedan 2007. Detta har ytterligare påtalats av den svenske överbefälhavaren Michael Claesson, som särskilt tryckt på att Rysslands strategiska mål ligger fast[10].

Kriget har visat hur angriparens brutalitet drabbar det civila samhället och människorna i det. Erfarenheter från kriget visar hur civil infrastruktur betraktats som ett legitimt mål för angriparen[11]. Syftet med dessa angrepp är att belasta den civila befolkningen, och i linje med detta kan det då förväntas att transportsektorns kritiska förmågor också är mål identifierade av en motståndare.

Lärdomar dras kontinuerligt från kriget. Medialt rapporteras om förändring i användandet av flygande drönare (UAV) exempelvis med övergång till trådbunden styrning för att motverka elektronisk krigföring. Mindre medialt är erfarenheter kring reparationsberedskap och logistik, något som dock är högst intressant för transportsektorn.

Rysslands operationer mot Sverige fortgår med tidigare och nya syften, och med nya tillvägagångssätt. Under våren 2025 har ett flertal omfattande sabotage mot bland annat kommunikationsinfrastruktur genomförts[12] dock utan att någon offentlig, bekräftad gärningsperson har pekats ut. Utvecklingen visar på en allt högre rysk acceptans för allvarliga konsekvenser, även med påverkan på liv och hälsa[13].

Oavsett utgången av kriget i Ukraina kommer samtliga statsaktörer i världen, i olika grad, att studera detta och dess händelseförlopp. Det innebär att slutsatser kommer att dras kring angriparens förberedelser såsom informationsinhämtning, resursuppbyggande, användande av civil teknik i militära syften och medvetna attacker mot civila mål med mera.

2.1.2 Gråzonen – krigföring men ändå inte krig

Hotet från andra länder mot Sverige har ökat under en längre tid. Många av de antagonistiska aktiviteterna sker dock i gränslandet mellan fred och väpnad konflikt, mellan laglig och olaglig verksamhet och samverkande mellan varandra, ibland till synes utan ett tydligt syfte annat än för den som utför dem. Därför är dessa inte alltid uppenbara. Främmande makter bedriver och genomför exempelvis spionerі, strategiska uppköp och elektroniska angrepp mot Sverige, och numera är det tydligare inriktat mot att även påverka svenskt beslutsfattande. Statsminister Ulf Kristersson uttryckte detta under konferensen Folk och Försvar 2025 med orden: ”Sverige är inte i krig. Men det råder inte heller fred.”[14]

Till detta kommer det ökande hotet om sabotageförberedelser. I dag riktas det främst mot verksamhet som syftar till att stödja Ukraina i sitt försvar mot regimen i Kreml, men det riktas även mot det svenska totalförsvarsuppbyggandet. Syftet, målval och tillvägagångssätt kan variera och förändras, vilket innebär att transportsektorn i Sverige behöver bygga upp ett uthålligt, motståndskraftigt och flexibelt skydd med stor bredd. Vi behöver arbeta med de skyddsåtgärder som behövs för alltifrån att förbättra vår it-säkerhet och stärka totalförsvaret till att skydda svenska intressen mot industrispionage eller kringgående av internationella sanktioner[15]. Till stöd finns direktiv och förtydliganden från exempelvis Försvarsmakten om vilken säkerhetskänslig verksamhet som de är beroende av för försvaret av Sverige. Infrastruktur och transporter har här ett eget kapitel[16].

10 Gräns, avsnitt 144. Sveriges Radio, 2025.

11 Erfarenheter från Ukraina – Initiala lärdomar för det civila försvaret – Delredovisning av regeringsuppdrag Fö2023/01325. ISBN: 978-91-7927-438-2. Myndigheten för samhällsskydd och beredskap, 2023.

12 https://www.svt.se/nyheter/inrikes/granskning-angrepp-mot-30-tal-telemaster-utreds-som-sabotage (Kontrollerad 2025-07-22).

13 Lägesbild 2024–2025. ISBN: 9789186661274. Säkerhetspolisen, 2025.

14 https://www.regeringen.se/tal/2025/01/statsministerns-tal-pa-folk-och-forsvars-rikskonferens-i-salen/. (Kontrollerad 2025-07-22).

15 Lägesbild 2024–2025. ISBN: 9789186661274. Säkerhetspolisen, 2025.

16 Skyddsvärden för försvaret av Sverige – Att identifiera säkerhetskänslig verksamhet. Militära underrättelse- och säkerhetstjänsten, MUST. Försvarsmakten, 2025.

Agerandet i gråzonen är inte något som endast kommer att ske vid höjd beredskap eller då Sverige hamnar i en militär konflikt, utan de antagonistiska handlingarna sker redan i dag. Därför är de en realitet att hantera här och nu. Detta är ingen nyhet utan har varit känt i många år. Det som på senare tid möjligen kan ha förändrats är att det spridits en bredare insikt om att detta faktum inte längre kan förnekas. Tillvägagångssättet brukar benämnas hybridkrigföring.

Hybridkrigföring är det kombinerade användandet av öppna och dolda metoder i syfte att uppnå vanligtvis politiska mål inom ramen för gråzonen. Subversion är en av dessa metoder som kan användas för att uppnå liknande effekter som vid militär bekämpning, men utan att behöva ta till militära medel. Det är också en metod som kräver mindre resurser och är lättare att förneka då den kan genomföras av ombud, även benämnt proxy. Subversion kan dock ofta ske i kombination med militära medel och sabotage. Ryssland bedriver psykologisk krigföring och subversion genom att exempelvis underblåsa sociala konflikter och oro[17].

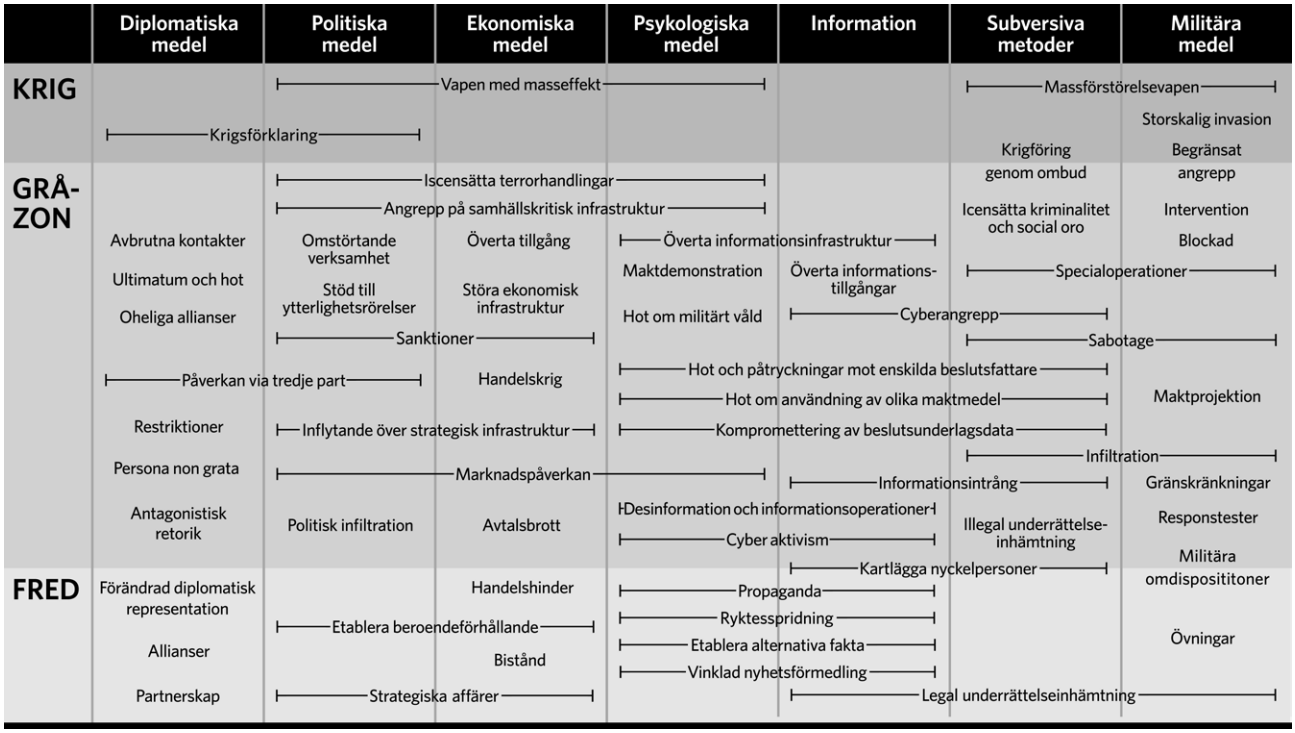
Syftet med de antagonistiska aktiviteterna i gråzonen kan variera. Ett syfte är sannolikt att få Sverige att justera sin politik, exempelvis inom handel, utrikes relationer, säkerhet och försvar. Andra syften är att hindra Sverige från att ta emot eller komma andra till hjälp, försvaga Sverige inför en militär konflikt eller belasta det europeiska samarbetet. Beroende på situation och syfte kan aktiviteterna få olika karaktär. De kan ske dolt för att skapa osäkerhet om vem som ligger bakom dem och därigenom vara förnekbara av antagonisten, eller ske mer öppet för att tydligt hota och skrämmas (se Figur 1).

Genom att använda nämnda verktyg, över tid och med olika intensitet, kan en statsaktör skapa ett handlingsutrymme som kan användas i ett senare läge. Till exempel ger ett datainträng i ett system i dag ett visst informationsläckage, men den egentliga skadan inträffar när en motståndare väl väljer att använda den informationen för att slå ut datasystemet som en del av en större operation.

Hybridkrigstekniken används flitigt av Ryssland, men även av andra stater som till exempel Kina. Länderna använder gråzonens diffusa natur i syfte att skaffa sig ett övertag som kan användas för att påverka ett annat land. De senaste årens snabba tekniska utveckling och globalisering av ekonomier har skapat sårbarheter som gör dessa verktyg kraftfullare än tidigare.

Den gråzon mellan fred och väpnad konflikt som dessa operationer ofta befinner sig i medför att det ibland är svårt att bedöma om det handlar om förberedelser för en konflikteskalering. Även om hybridkrigsföringen kan sluta i en öppet väpnad konflikt bygger den i grunden på att undvika just det och i stället föra över konflikten till den domän där statsaktören har en större förmåga. Denna utveckling skapar ett stort behov av en ökad förmåga att möta sådana angrepp hos organisationer som bedriver säkerhetskänslig verksamhet.

Det är då en viktig men grannlaga uppgift att analysera möjliga orsakssamband mellan inträffade incidenter. Det som först kan framstå som en olycka kan efter en utredning visa sig ha bäring på skyddsvärden som ska omgärdas av till exempel säkerhetsskydd.



Figur 1. Gråzonsarenan och metoder som utgör de hybrida hoten.

17 MUST årsöversikt 2022. Försvarsmakten, 2023.

För att överhuvudtaget kunna analysera incidenter måste dessa vara kända. Det ställer krav på organisatorisk medvetenhet om vikten av rapportering, individuell rapporteringsvilja, förmåga att systematiskt sammanställa och samverka kring händelser med närliggande aktörer både inom och utom transportsektorn med mera.
Vidare innebär detta att även hanteringen av incidenter kan behöva skyddas med säkerhetsskyddsåtgärder, eftersom främmande makt kan ha intresse av att få kunskap om vår förmåga att detektera dessa och om hur vi går tillväga för att hantera dem. Motsvarande problematik kan förekomma i exempelvis olycksutredningar där händelseförlopp och konsekvenser beskrivs.

Exempel på konkreta hot mot transportinfrastrukturen inom gråzonen är

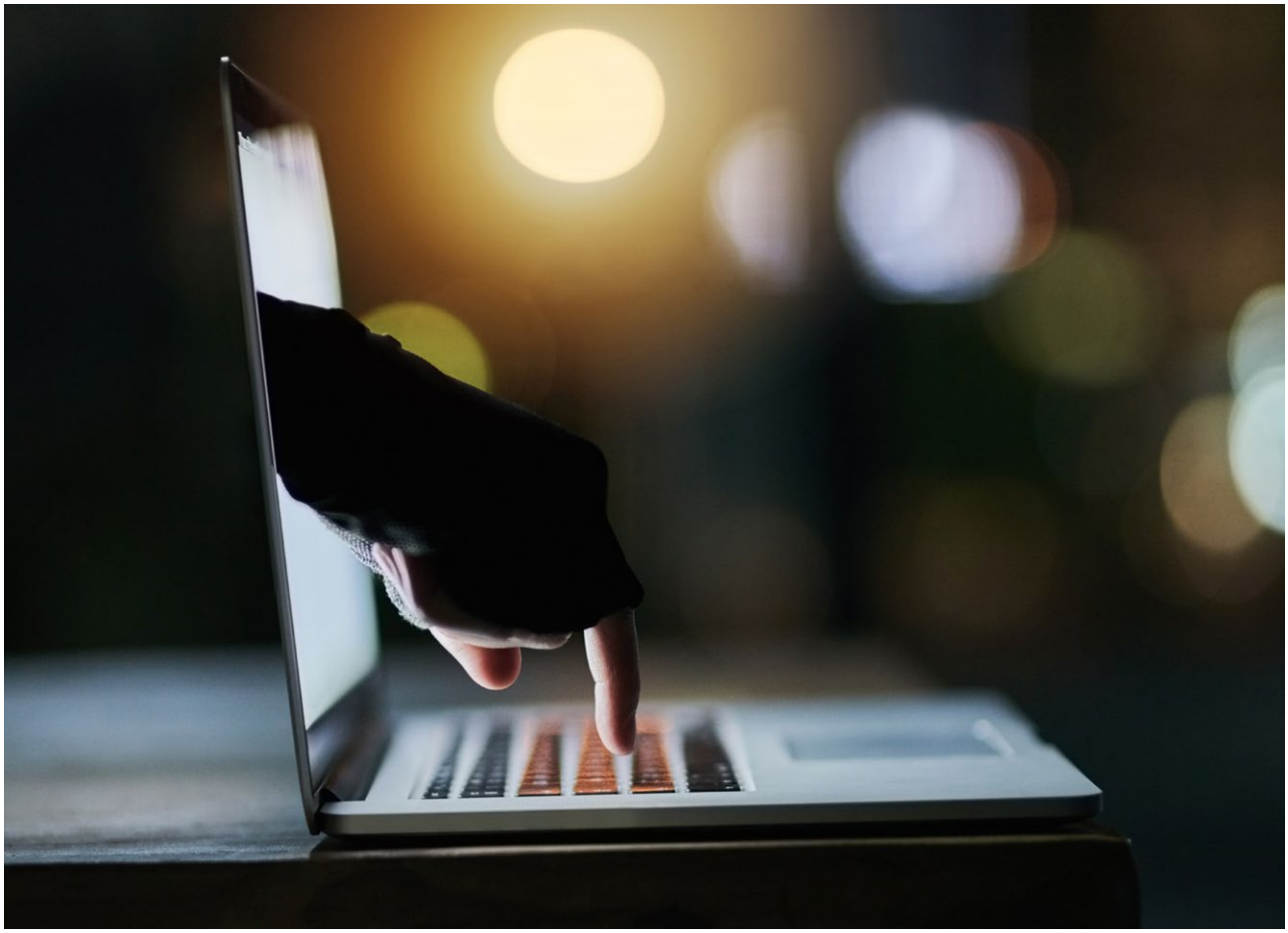
- intrång i informations-, drift- och styrsystem
- infiltration och rekryterandet av möjliggörare (insiders)
- kartläggning av nyckelpersonal
- förberedelse för sabotage
- underrättelseinhämtning.

Digitaliseringen av transportsystemet kan medföra ökade sårbarheter. Bland annat kan cyberangrepp få effekter i form av störningar och avbrott om de realiseras.

I rapporten Cybersäkerhet i Sverige 2024[18] beskrivs hur cyberangrepp kan förändras:

Metoder och verktyg för cyberangrepp utvecklas ständigt och hotaktörernas spelplan förändras i takt med teknikutvecklingen. Hotaktörerna använder sig ofta av enklast möjliga metod för att uppnå önskat resultat och i många fall krävs inte att man använder sig av avancerade metoder.

Vi vet i dag att antalet rapporterade cyberangrepp genom överbelastningsattacker har ökat kraftigt under det senaste året[19]. Att möta gråzonshot handlar i första hand om att utveckla icke-militära motmedel. Ett sådant motmedel är att stärka förmågan att upprätthålla samhällets funktionalitet, vilket inte minst gäller transportsektorn. Robustare transportsystem ger ökad motståndskraft och höjer därmed tröskeln för angrepp.



18 Cybersäkerhet i Sverige 2024. Nationellt Cybersäkerhetscenter, 2025.

19 Cyberangrepp mot samhällsviktiga informationssystem – 25 rekommendationer för stärkt skydd mot cyberangrepp. ISBN: 978-91-7927-459-7. Myndigheten för samhällsskydd och beredskap, 2024

2.1.2.1 Hybrida hot i transportsystemet

På uppdrag av Trafikverket har Försvarets forskningsinstitut (FOI) tagit fram en rapport[20] som förtjänar att uppmärksammas särskilt. I rapporten har FOI dels sammanfattat och exemplifierat ett scenario med en utdragen och eskalerande gråzonsproblematik, dock utan höjd beredskap (typfall 5)[21], dels presenterat och diskuterat sex olika kategorier för hot mot eller sårbarheter inom transportsystemet.

- Marknadsförhållanden skapar spelplanen för företag och antagonister.
- Transportsystemets öppenhet och tillgänglighet kan utnyttjas av en antagonist.
- Intrång och störningar kan drabba anläggningar och system.
- Säkerhetsrisker uppkommer vid upphandling och användning av varor och tjänster.
- Beroenden skapar sårbarheter som kan utnyttjas av en antagonist.
- Utmaningar finns i utvecklingen av en sammanhängande beredskap.

Rapporten kan ses som ett förstärkande dokument för att skapa djupare förståelse för påverkan på den egna verksamheten.

2.1.3 Internet är globalt

Integritetsskyddsmyndigheten (IMY) publicerade den 10 mars 2025[22] ett blogginlägg där man konstaterar att EU–US Data Privacy Framework (adekvansbeslutet) fortfarande säkerställer en tillräcklig skyddsnivå för personuppgifter som överförs till USA – förutsatt att mottagaren är ansluten till ramverket. IMY behöver därför inte föreskriva ytterligare skyddsåtgärder enligt artikel 46 i dataskyddsförordningen (GDPR), men uppmanar alla verksamheter att bevaka utvecklingen och förbereda alternativa överföringsgrunder (standardavtalsklausuler eller bindande företagsbestämmelser) om adekvansbeslutet skulle upphävas[23].

Samtidigt, och troligen till viss del i ljuset av Trump-administrationens uttalande om Grönland, har den danska dataskyddsmyndigheten Datatilsynet varnat för att den amerikanska CLOUD-lagstiftningen ger myndigheter i USA rätt att begära ut data från företag som Microsoft, Google och AWS oavsett var informationen lagras. Datatilsynet rekommenderar därför att danska företag och organisationer vidtar åtgärder[24]. För det första rekommenderas företag och verksamheter att ta fram en alternativplan för att frigöra sig från amerikanska molntjänster om ramverket kärvar eller dras tillbaka. För det andra att man utarbetar en exitstrategi för hur personuppgifter ska hanteras om adekvansbeslutet upphävs och ingen övergångsperiod ges.

Den norska motsvarigheten till IMY, även den kallad Datatilsynet, har gått ut med vägledning efter att ha mottagit flera frågor om överföringsregler till USA.

Myndigheten understryker precis som den svenska IMY att det nuvarande adekvansbeslutet fortfarande gäller men att det kan ifrågasättas i EU-domstolen. Datatilsynet råder norska företag ha en tydlig exitstrategi[25] för att hantera personuppgifter om det inte längre går att använda amerikanska molntjänster på samma sätt. Dessutom råder man till att identifiera och implementera alternativa skyddsåtgärder (till exempel standardavtalsklausuler) i förväg, eftersom en upphävning av adekvansbeslutet sannolikt skulle ske utan en övergångsperiod.

20 Gråzonsproblematik och hybrida hot i transportsystemet. FOIR5118. Totalförsvarets forskningsinstitut, 2021.

21 Typfall 5: Utdragen och eskalerande gråzonsproblematik, FOI MEMO 6338. Totalförsvarets forskningsinstitut, 2018.

22 https://www.imy.se/blogg/overforing-av-personuppgifter-till-usa-vad-galler/ (Kontrollerad 2025-07-29).

23 https://computersweden.se/article/3841156/vart-beroende-av-amerikanska-tjanster-ar-inte-bara-en-gdpr-fraga.html (Kontrollerad 2025-07-29).

24 https://www.computerworld.dk/art/290729/digitaliseringsminister-slaar-fast-efter-cloud-panik-dataaftale-med-usa-staar-ved-magt-men-virksomheder-boer-have-en-plan-b (Kontrollerad 2025-07-30).

25 https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2025/informasjon-om-overforinger-til-usa/ (Kontrollerad 2025-07-30).

2.2 Säkerhetshotet mot Sverige

Säkerhetshotet mot Sverige är fördjupat och har både ökat och breddats under senare år. Främmande makt agerar alltmer offensivt och utnyttjar tillfällen som uppstår för att gynna sin egen agenda på andras bekostnad.

Under det senaste året har de ryska säkerhets- och underrättelsetjänsterna agerat alltmer offensivt gentemot länder i Europa, vilket även påverkar säkerhetsläget i Sverige[26].

Ryssland, Kina och Iran utgör alltjämt de största hoten och de agerar mer offensivt för att främja sina intressen, skapa intressesfärer och påtvinga andra stater att agera i enlighet med deras vilja. Från rysk sida var detta tydligt redan innan den fullskaliga invasionen av Ukraina. Säkerhetspolisen ser att främmande makt i allt större omfattning riktar intresset mot civila mål. Rymden är nu en självklar arena för både underrättelseinhämtning och för framtida konflikter.

I det försämrade omvärldsläget framhävs behovet av att skydda kritisk infrastruktur. Chefen för den militära underrättelse och säkerhetstjänsten (MUST) uttrycker i sin årsöversikt 2024 följande:

> **Hybridhotet är inte nytt, men viktiga förändringar har skett under det senaste året. Bland annat ser vi ett ökat risktagande från rysk sida, och nya metoder såsom användandet av okvalificerade ombud för attentat i flera europeiska länder. Vi lever i en farlig tid – och det kommer vi att göra under överskådlig tid. Hoten mot Sverige är breda, komplexa och allvarliga. Vi måste dra slutsatser av detta och agera därefter[27].**

Statliga aktörer riktar även in sig på lärosäten, industrier och företag i syfte att skaffa sig tillgång till spetsteknologi och spetskompetens. I vissa fall kan anskaffningsbehov och skyddsvärden sammanfalla. I all verksamhet där organisationen inbjuds att ta emot delegationer och inleda samarbeten inom exempelvis forskningsområdet måste en skarp vaksamhet påkallas. Ofta måste de enskilda fallen bedömas separat varför generella riktlinjer är svåra att fastställa. Den bästa skyddsmetoden är medvetenhet och samverkan inom transportsektorn. Användandet av delegationer och skenbart legitima samarbeten ökar ytterligare i betydelse när andra möjligheter till underrättelseinhämtning begränsas, exempelvis genom utvisning av främmande makts ambassadpersonal som vilken misstänkts bedriva olovlig underrättelseverksamhet.

Denna underrättelseinhämtning kombineras även med lagliga metoder via öppna källor, så kallad Open Source Intelligence (OSINT). Detta innebär att stora krav måste ställas på verksamhetens informationssäkerhet.

Vad gäller påverkan och angrepp från statliga aktörer ska hotbilden tas i beaktande både inom och utom Sveriges gränser. Nyckelpersonal utgör mål för underrättelseinhämtning från statsaktörer oavsett om arbete sker på ordinarie tjänsteställe, på distans i exempelvis hemmet eller på resa inom eller utom Sverige.

Vidare är dagens beroenden mellan länder, leverantörer och infrastrukturägare mer komplext än någonsin, och graden av både globalisering och digitalisering har ökat. Den ökade digitaliseringen möjliggör effektiva samarbeten, men den medför samtidigt sårbarheter, bland annat i form av okända beroenden. Det är därför ett faktum att den säkerhetshotande verksamhet från främmande makt som ständigt pågår genom exempelvis olovlig underrättelseverksamhet, påverkansoperationer och cyberangrepp i och med det oroliga omvärldsläget, innebär ett skiftande och föränderligt hot. Inom ramen för detta ingår även de ansträngningar som främmande makt vidtar i syfte att anskaffa avancerad teknologi i Sverige.

2.2.1 Säkerhetshotet mot transportsektorn

I regeringens Nationella säkerhetsstrategi[28] pekas kriget och kriminaliteten ut som de huvudsakliga hoten mot Sveriges säkerhet. Begreppet säkerhet måste hanteras utifrån ett bredare anslag än tidigare och vikten av att förstå hur förändringar i vår omvärld kan påverka hotbilden i Sverige ökar. De senaste årens styrning från Sveriges regering innebär att detta numera omhändertas inom ramen för arbete med civil beredskap, i vilket det civila försvaret inräknas, och i den privat-offentliga samverkan som sker inom transportsektorn.

Transportsektorn är, utöver statsaktörers intresse för infrastruktur och säkerhetskänsliga transporter, även mål för kriminella som har ekonomisk vinning som drivkraft. Detta innebär att kriminella alltid kommer att söka efter nya möjligheter att stjäla pengar, vilket beskrivs senare i dokumentet. Hotbilden som presenteras i detta dokument innehåller i många avseenden information som förändrats mycket lite över åren. Dock ses behovet av att lyfta fram områden som aktualiserats eller bedöms stå inför en större utveckling. Ett exempel på dessa områden är rymddomänen som står inför en kraftig utveckling i betydelse och som inte tidigare omnämnts djupare.

26 Lägesbild 2024–2025. ISBN: 9789186661274. Säkerhetspolisen, 2025.

27 MUST årsöversikt 2024. Försvarsmakten, 2025

28 Nationell säkerhetsstrategi. Skr: 2023/24:163. Regeringskansliet, 2024.

2.2.2 Planeringen av det svenska totalförsvaret

Totalförsvaret består av militär och civil verksamhet, vilka vi känner som militärt försvar och civilt försvar. Med civilt försvar avses den verksamhet som myndigheter, kommuner och regioner vidtar tillsammans med övriga civila aktörer för att förbereda Sverige för krig. De civila aktörerna är såväl enskilda som företag och frivilligorganisationer. Syftet med detta är att stärka samhällets förmåga att motstå prövningar i tider av kris och krig. I fredstid utgörs totalförsvarets verksamhet av beredskapsplanering och förmågehöjande åtgärder, inklusive påkallade säkerhetsåtgärder. Planeringen av det civila försvaret bidrar också till att stärka Försvarsmaktens operativa förmåga vid höjd beredskap, väpnat angrepp eller krig.

I Försvarsberedningens säkerhetspolitiska rapport Allvarstid uttrycks detta bland annat genom:

> **Ett väpnat angrepp mot Sverige kan inte uteslutas. Det kan inte heller uteslutas att militära maktmedel eller ytterligare hot om sådana kan komma att användas mot Sverige. Den antagonistiska hotbilden mot Sverige är bred och blir alltmer komplex. Hoten inkluderar bland annat otillbörlig informationspåverkan, desinformation, påverkansoperationer, cyberangrepp, illegal underrättelseinhämtning, terrorism och sabotage, hot mot kritisk infrastruktur och utnyttjande av ekonomiska beroenden[29].**

Det civila och det militära försvaret förstärker varandra. Därför sker inte planeringen av det civila försvaret enbart genom samverkan mellan samhällets privata och offentliga aktörer, utan följaktligen också genom samverkan med det militära försvaret.

Den mer komplexa hotbilden mot Sverige och den pågående totalförsvarsuppbyggnaden innebär förändringar i vad som är skyddsvärt, då det militära försvaret har starka beroenden till det civila samhällets funktionalitet[30]. Det förutsätter en inneboende robusthet i exempelvis transportsystemet, så att Försvarsmakten kan ges stöd i händelse av höjd beredskap eller krig. Planeringen för genomförandet av detta stöd sker i fredstid och är en verksamhet som är intressant för främst antagonistiska statsaktörer. Därför behöver både planeringen av det civila försvaret och planeringen av genomförande av stöd till Försvarsmakten skyddas, vilket åligger den aktör inom transportsektorn som har till uppgift att hantera dessa skyddsvärden. Konsekvenserna av brister i detta skydd kan i ett värsta scenario bli synliga först i händelse av höjd beredskap eller krig. Stödet till Försvarsmakten är, i enlighet med den försvarspolitiska inriktningen och planeringeringsanvisningarna för det civila försvaret, något som ska genomföras i fred, höjd beredskap och krig.

Säkerhetspolisen uttrycker mycket tydligt synen på behovet av att se en helhet kring hotbild, skyddsvärden och sårbarhetshantering i samtliga skeenden i samhället:

> **Det svenska inträdet i Nato och uppbyggnaden av det svenska totalförsvaret innebär ett mer robust nationellt skydd samtidigt som nya skyddsvärden och potentiellt nya sårbarheter uppstår. Vad som är av betydelse för Sveriges säkerhet förändras delvis över tid. Genom en ständig anpassning av skyddet skapas en ökad motståndskraft mot hotaktörer[31].**

Svenskt artillerisystem 08 "Archer" under järnvägstransport. Foto: Försvarsmakten.

29 Ds 2023:19. Allvarstid. Försvarsberedningens säkerhetspolitiska rapport 2023. Säkerhetspolisen.

30 Skyddsvärden för försvaret av Sverige – Att identifiera säkerhetskänslig verksamhet. Militära underrättelse- och säkerhetstjänsten, MUST. Försvarsmakten, 2025.

31 Lägesbild 2024–2025. ISBN: 9789186661274. Säkerhetspolisen, 2025.

2.2.3 Alla aktörer i transportsektorn har ett ansvar i det svenska totalförsvaret

Den 1 oktober 2022 trädde förordningen om statliga myndigheters beredskap (SFS 2022:524)[32] i kraft. Den innebar att det infördes 10 stycken beredskapssektorer (den 1 juli 2025 utökades dessa till 12 stycken), civilområden (6 stycken) och beredskapsmyndigheter (60 stycken). I samband med att förordningen började gälla fick § 3 a i Trafikverkets instruktion[33] en ny lydelse enligt förordning (2022:552):

> **Trafikverket är beredskapsmyndighet och sektorsansvarig myndighet enligt förordningen (2022:524) om statliga myndigheters beredskap.**

Enligt denna förändring är Trafikverket både beredskapsmyndighet och sektorsansvarig myndighet med ansvar för beredskapssektorn transporter, där även Transportstyrelsen, Sjöfartsverket och Luftfartsverket ingår. Trafikverket som sektorsansvarig myndighet ska driva på arbetet inom sin beredskapssektor, stödja beredskapsmyndigheterna och verka för att samordning sker med andra aktörer.

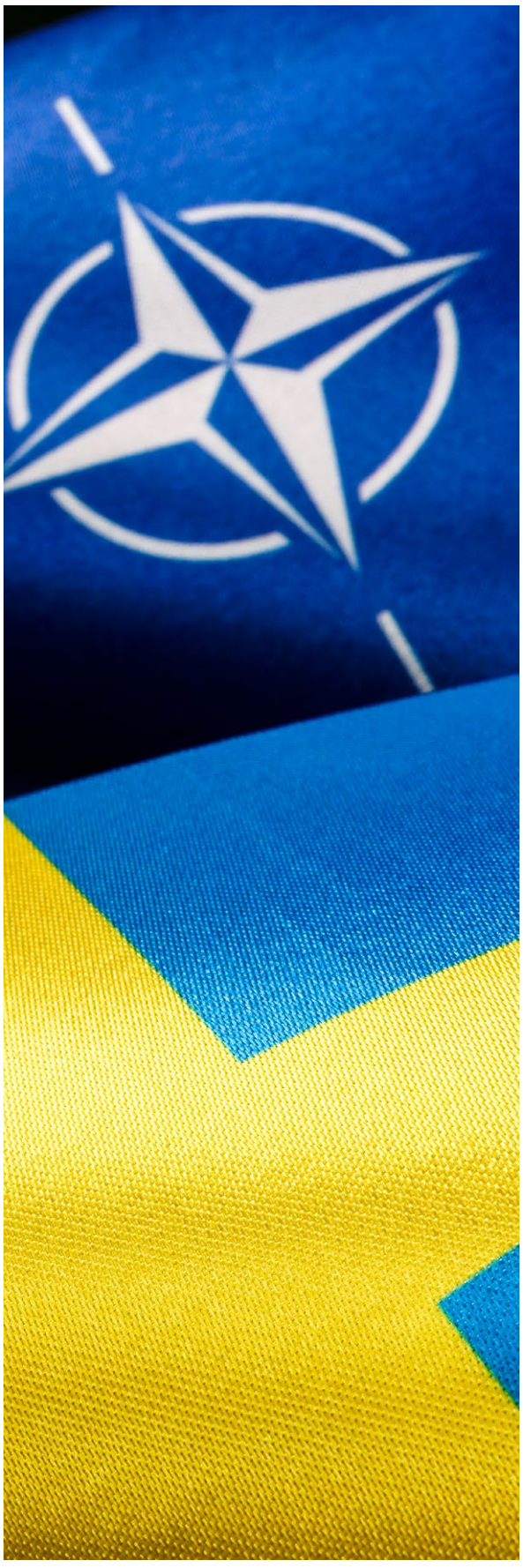
Samtliga aktörer inom transportsektorn ansvarar dock för att bibehålla skyddet för den egna skyddsvärda verksamheten. Följaktligen behöver samtliga leveranser inom transportsystemet som är av betydelse för både civilt och militärt försvar omfattas av ett anpassat och välfungerande säkerhetsskydd redan i ett normalläge. Antagonistiska aktiviteter som Sverige i dag tvingas möta inom ramen för gråzonen får inte förringas, och skyddet kring dessa samt kring nyuppkomna skyddsvärden behöver vara aktivt.

2.2.3.1 Tidsperspektiv för totalförsvarsåtertagandet

Den största bristen är bristen på tid. Den största sårbarheten är oförmågan att förstå att den grundläggande idén är att totalförsvaret omfattar hela samhället. Den viktigaste egenskapen är viljan att agera.

32 SFS 2022:524. Förordning om statliga myndigheters beredskap.

33 SFS 2010:185. Förordning med instruktion för Trafikverket.



Den danska underrättelsetjänsten Forsvarets Efterretningstjeneste (FE) gjorde i februari 2025 bedömningen om tidsperspektiven för den ryska återtagandeförmågan vid ett eldupphör i Ukraina, vilken även militära underrättelse och säkerhetstjänsten (MUST) instämmer i[34]. Den danska bedömningen är följande[35]:

- Efter 6 månader skulle Ryssland kunna utkämpa ett lokalt krig med ett grannland.
- Efter runt två år skulle Ryssland utgöra ett reellt hot mot ett eller flera Nato-länder, eller kunna hantera ett regionalt krig i Östersjöregionen.
- Efter fem år skulle Ryssland vara redo för ett storskaligt krig i Europa.

Detta baseras på att USA inte interfererar och att Natoländerna i övrigt inte upprustar i samma takt som Ryssland.

Detta är de tidsperspektiv som behöver finnas med i all totalförsvarsplanering och omfattar då med självklarhet transportsektorns aktörer. Detta gäller oaktat om frågan handlar om direkt deltagande i totalförsvarsuppbyggnaden eller uppbyggandet av den egna förmågan att kunna bedriva sin verksamhet i ett mycket ansträngt samhällsläge eller krig.

2.2.3.2 Det svenska Natomedlemskapet

Sverige blev fullvärdig allierad i den nordatlantiska försvarsalliansen Nato den 7 mars 2024. I och med detta bedöms Sverige få en förändrad roll som transitland för trupper och materiel inom ramen för alliansens gemensamma försvarsoperationer. Det innebär rimligen även förändringar kopplat till både infrastruktur och logistik.

Eftersom medlemskapet bedöms minska risken för direkt markangrepp på Sverige från Ryssland, bör i stället det hybrida hotet öka. Det hybrida hotet rör sig över ett stort spektrum av metoder och arenor och strävan är att hela tiden utgöras av dolda och förnekbara insatser. Följden av detta är att kritisk infrastruktur kan vara intressanta målval, särskilt känsliga transporter med mera. En angripare kommer att försöka utnyttja sårbarheter i den fysiska säkerheten och inom cyberdomänen. Detta kopplar till både vårt behov av precis positionering och vår planering av transporter, såväl som angriparens möjligheter till infiltration och värvande av möjliggörare (insiders).

Inträdet i alliansen innebär två huvudsakliga förändringar för aktörerna inom den svenska transportsektorn. För det första behöver dessa förhålla sig till de uppgifter som Sverige utför som allierad. Exempelvis ställer Nato krav på informationshantering och gemensamma nivåer av skyddsåtgärder kring informationssäkerheten.

För det andra så kan främst Rysslands syn på vilka förmågor i Sverige som är av intresse för krigsplanläggning påverkas. Nya områden kopplat till exempelvis transportuppgifter kan prioriteras upp. Försvarsmakten bedömer att den kollektiva försvarsplaneringen inom Nato sannolikt kommer innebära att Sverige blir ett viktigt område för basering och transporter av allierade förband. Detta ställer krav på en snabb utveckling av förutsättningsskapande åtgärder, exempelvis inom ramen för värdlandstöd, integrationsåtgärder och förstärkning av infrastruktur[36].

34 https://www.sydsvenskan.se/2025-03-16/must-ryska-militara-hotet-mot-sverige-kan-oka/ (Kontrollerad 2025-07-28).

35 Opdateret vurdering af truslen fra Rusland mod Rigsfællesskab. Forsvarets Efterretningstjeneste, 2025.

36 Överbefälhavarens militära råd – Svensk försvarsförmåga inom ramen för Natos kollektiva försvar. FM2023-23092:14. Försvarsmakten, 2023.

2.3 Särskilda geografiska perspektiv

Med ett geografiskt perspektiv på det antagonistiska hotet ges ytterligare möjligheter att se sammanhang som kan innebära sårbarheter eller möjligheter för transportsektorn. Många geografiska domäner har länge varit självklara såsom luft, land och hav. På senare år har den gängse bilden utökats på ett sätt som gör att dessa återupptäckta domäner förtjänar att omnämnas särskilt. Dessa är rymddomänen, havsbottnen och Arktis.

2.3.1 Rymddomänen

Rymddomänen betraktas som en av de fem operativa domänerna där exempelvis Försvarsmakten måste kunna verka för att både säkerställa Sveriges säkerhet och även stödja multinationella operationer. Närvaron i rymden anses avgörande för att upprätthålla underrättelseinhämtning, geografisk lägesbild och kommunikation, vilka alla är grundläggande för moderna multidomäna operationer[37].

Detta har betydelse för Sveriges säkerhet och måste ses ur ett totalförsvarsperspektiv. Därför behöver vi öka vår kunskap och medvetenhet om rymden som underrättelsearena och om beroenden till rymdteknologin samt de sårbarheter dessa kan innebära.

Den 4 juli 2024 beslutade så regeringen att Sverige ska ha en försvars- och säkerhetsstrategi för rymden, mot bakgrund av rymdens allt större betydelse som strategisk och operativ domän. Strategin understryker att rymdtjänster har blivit en integrerad del av samhällets grundläggande funktioner och att Sverige därför behöver beredskap att vidta tekniska, politiska, diplomatiska och militära åtgärder i rymden när så krävs[38].

Övergripande syftar strategin till att säkerställa Sveriges försvars- och säkerhetsintressen i och genom rymden genom att stärka förmågan att föregå, upptäcka och hantera utmaningar i rymdområdet. Detta omfattar både civil krisberedskap och militär totalförsvarsplanering, med mål att öka motståndskraften mot hybridpåverkan, cyberangrepp och andra hot mot kritisk rymdinfrastruktur.

Strategins fyra pelare är att skapa handlingsfrihet genom prognos- och hanteringsförmåga, bygga en portfölj av tjänster och kapaciteter till stöd för totalförsvar och krisberedskap, agera som en ansvarsfull partner internationellt samt bedriva en sammanhållen och kunskapsbaserad rymdpolitik som stärker krisberedskap och totalförsvar. Genom dessa insatser ska Sverige kunna förebygga och bemöta hot i rymden samt bidra till allierad rymdsäkerhet och samverkan.

En miljard kronor har avsatts för åren 2024–2032 för att utveckla Försvarsmaktens rymdförmågor. Satsningen fokuserar på tre huvudområden: spaning och övervakning från rymden, nationell uppsändningsförmåga och militär rymdlägesbild. Dessa insatser syftar till att ge Sverige egen förmåga att skjuta upp satelliter, förbättra lägesbilden och därigenom stärka totalförsvaret samt bidra till Natos gemensamma rymdförmåga.

Hotet kopplat till rymddomänen riktar sig i dag mot den infrastruktur som den utgör. Både satelliter, markbunden teknik samt de tjänster dessa levererar kan angripas och störas. Ur ett europeiskt perspektiv är det alltmer tydligt att EU och Europa är starkt beroende av den svenska rymdförmågan som en del av den gemensamma. I ett gemensamt meddelande[39] från EU-kommissionen framhålls att Sverige är det enda medlemslandet som kan skjuta upp satelliter från europeiskt fastland. Denna unika förmåga ses som central för EU:s totala försvar, krisberedskap och långsiktiga rymdambitioner och då rymdtransporter är ett av European Space Agency (ESA) utpekade utvecklingsområden kommer detta att återverka på transportsektorn i Sverige.

37 Överbefälhavarens militära råd – Svensk försvarsförmåga inom ramen för Natos kollektiva försvar. FM2023-23092:14. Försvarsmakten, 2023.

38 Rymdens roll i ett nytt säkerhetspolitiskt läge – Sveriges försvars- och säkerhetsstrategi för rymden. Regeringskansliet, 2024.

39 Gemensamt meddelande om EU:s rymdstrategi för säkerhet och försvar. Faktapromemoria 2022/23:FPM67. Regeringskansliet, 2023.

Satellitbaserade system är avgörande för moderna transportnätverk, inklusive satellitbaserade positioneringssystem, kommunikationssatelliter för datatrafik och väderobservation för planering. Om dessa satellitsystem skulle störas eller förstöras, antingen avsiktligt genom militära handlingar eller oavsiktligt, skulle det kunna ha allvarliga konsekvenser för transportinfrastrukturen. Lärdomar kan också dras från kriget i Ukraina (se tidigare avsnitt) där privata aktörers möjligheter att påverka det ukrainska försvaret ger en indikation på att valet av rymdtjänsteleverantör behöver göras med stor eftertänksamhet[40].

Störningar av positioneringstjänster skulle kunna påverka allt från lastbilstransporter till sjöfart och luftfart, vilket skulle göra det svårt att effektivt koordinera transporter och leveranser. Det skulle inte bara påverka den kommersiella sektorn, utan också förmågan att snabbt och effektivt distribuera nödvändiga förnödenheter i händelse av en kris eller katastrof.

Störningar i kommunikationssatelliter skulle också kunna hindra effektiv datakommunikation mellan transportfordon och kontrollcentraler, vilket skulle kunna leda till fördröjningar och potentiellt farliga situationer, särskilt i högt trafikerade områden eller under extrema väderförhållanden.

Sammanfattningsvis är rymdens växande roll som en potentiell arena för konflikt och krigföring något som har en direkt inverkan på Sveriges transportsektor. Detta gör det nödvändigt för både statliga och privata aktörer inom transportsektorn att vara medvetna om dessa risker och att vidta åtgärder för att minimera deras potentiella påverkan.

För transportsektorns del är påverkan från rymddomänen en del av det komplexa hotet och samtliga aktörer måste i sitt löpande arbete beakta de konsekvenser det kan innebära med beroenden till rymdteknologi bland annat vid kommunikation och positionering. Det innebär exempelvis att utarbeta rutiner för att hantera bortfall av kritiska tjänster som säkerställer det fortsatta genomförandet av verksamheten.

2.3.1.1 Användandet av rymdtjänster och ett paradigmskifte

Rymddomänen genomgår en begreppsmässig förskjutning där Old Space och New Space illustrerar övergången från traditionellt statligt drivna, långsiktiga rymdprojekt till kommersiellt ledda, snabbrörliga satsningar. Old Space präglas något förenklat av stora, centraliserade system, främst till för både civila infrastrukturer som väder- och kommunikationssatelliter samt militära spanings- och navigationssystem. New Space kännetecknas av bland annat småsatelliter, återanvändbara uppskjutningsfordon, tjänsteförvaltning och agil utveckling, där privata aktörer snabbt levererar tjänster för global uppkoppling, miljöövervakning och underrättelseinhämtning.

OLD SPACE refererar till den traditionella rymdindustrin som tog sin början under den första rymdåldern. Denna era präglas av att staten stod i centrum. Stora nationella rymdorgan, som Nasa, Roskosmos och andra statliga aktörer, drev tidigare rymdverksamheten och då ofta med enorma statliga budgetar och långa, byråkratiska processer. Aktiviteterna då var huvudsakligen inriktade på upptäcktsresor, vetenskaplig forskning och nationell säkerhet. Exempel på sådana projekt är rymdfärjor, byggandet av internationella rymdstationer, satellituppskjutningar för kommunikation och säkerhet, samt en stor mängd uppskickade rymdsonder. Ibland kan uttrycket ”det var Old Space som tog oss till månen” höras.

40 https://www.svt.se/nyheter/utrikes/direktrapport-forsamrat-sakerhetslage?inlagg=ecdcc21031b50540c60b6aa7c3685d79 (Kontrollerad 2025-07-28).

NEW SPACE representerar en mer modern och dynamisk modell där privata företag och entreprenörer får spela en framträdande roll i stället för statliga organ. Tanken är att ett marknadsbaserat och innovationsdrivet angreppssätt ska sätta ett betydligt större fokus på att sänka kostnader, snabba på utvecklingstakten och öppna upp rymden för kommersiella tillämpningar. Företag som SpaceX, Planet Lab och liknande har utmanat den traditionella modellen med Old Space genom att introducera innovativ teknik, exempelvis återanvändbara raketer och nya affärsmodeller. Förespråkare anser att detta har möjliggjort kostnadseffektiva uppdrag, ökad access till rymden och nya användningsområden för exempelvis satellitbaserad jordobservation och telekommunikation.

Denna övergång innebär inte enbart en teknologisk förändring, utan också en omdefiniering av hur rymden kan användas. Ur ett perspektiv innebär det en förflyttning som kan vara från tilldelad finansiering genom forskningsanslag till säkrad finansiering hos utvecklare genom löfte om köp av framtagen rymdtjänst samt dess förvaltning. Detta ökar det kommersiella utrymmet då leverantören kan sälja tjänster till fler aktörer, och det har rent erfarenhetsmässigt visat på en större sannolikhet till livskraftiga avknoppningar från de ursprungligen finansierade uppdragen.

För transportsektorn betyder detta då att det för det första finns beroenden till rymdtjänster såsom kommunikation, tidsangivelser och positionering redan i dag. För det andra uppstår det en möjlighet att möta rymdbranschen i dialog om den verksamhet som utgör transportsektorn och vilka behov och utmaningar som den har att möta. Med en god förståelse för dessa bör då rymdbranschens aktörer kunna ge förslag på typer av tjänster och produkter som effektiviserar och underlättar transportverksamhet samt även modeller för hur dessa ska förvaltas och finansieras över tid.

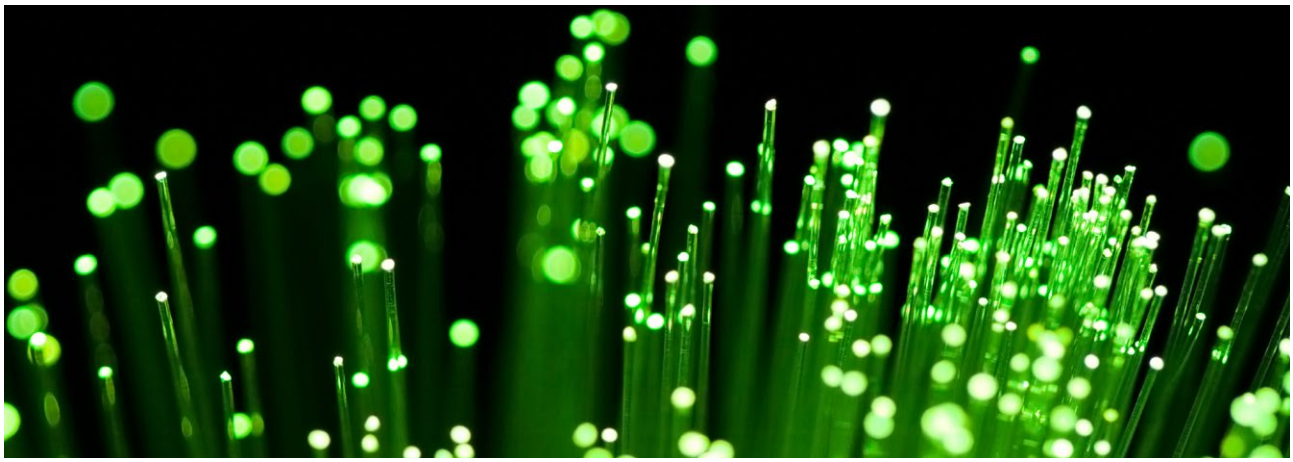
Rymdberoenden behöver dokumenteras tydligt i de olika analyser som verksamheter genomför i dag, exempelvis säkerhetsskydds-, risk och sårbarhets- eller analyser av styrkor och svagheter inför utvecklingsarbete. Detta kommer att bygga upp en förståelse och en kunskapsbank kring sakområdet vilket i förlängningen underlättar nuvarande verksamhet och framtida utveckling. Som exempel kan kunskapen om hur fysisk placering av GNSS-mottagare (Global Navigation Satellite Systems) för olika ändamål påverkar funktionen praktiskt vara användbar. Exempelvis så placeras en mottagare för tidsangivelse i vissa situationer med fördel lågt utan att för den skull täckas av snö och så att den ser så mycket fri himmel som möjligt, samtidigt som den skärmas från instrålning i marknivå. Praktiskt innebär detta exempel då att mottagaren blir mindre sårbar för markbaserade störsystem.

Det är viktigt att lyfta fram uppenbara beroenden till rymdtjänster eller rymdbaserad teknik som i dag saknar redundans i verksamheten. Situationen är samma för havsbottnen, vilket beskrivs nedan. Avslutningsvis bör påpekas att det kan finnas stora vinster med en samordnad användning av framtida och befintliga rymdsystem inom totalförsvaret, och det är önskvärt att arbeta mer integrerat militärt och civilt framöver.

2.3.2 Havsbottnen – bärare av energi och kommunikation

Den 25 december 2024 inträffade en incident som liknade sabotaget mot gasledningen Balticconnector och en datakabel i Finska viken i oktober 2023. Tankfartyget Eagle S passerade elkabeln Estlink 2 mellan Estland och Finland, och strax därefter upptäcktes det att kabeln förlorat kontakt. Operatören larmade då om ett plötsligt avbrott i Finska viken. Det misstänktes att fartygets ankare släpat på havsbotten och orsakat skador på kabeln[41].

Detta är exempel på händelser som ökar i frekvens[42] och som tillsammans med sabotagen mot Nord Stream 1 och Nord Stream 2 under 2022 visar på vikten av att beakta beroenden till den kritiska infrastrukturen på havsbotten. Redan under 2022 uppmanade Säkerhetspolisen alla aktörer som ansvarar för kritisk infrastruktur i Sverige att skärpa sin upptäckandeförmåga, något som fortfarande gäller i allra högsta grad. Detta är inte heller ett fenomen enbart förekommande eller ökande i Östersjön eller enbart riktat mot Sverige, utan det har rapporterats som ett frekvent tillvägagångssätt även på andra platser[43].



41 https://www.sverigesradio.se/artikel/polisutredning-om-eagle-s-klar-tre-personer-misstanks-for-brott (Kontrollerad 2025-07-24).

42 https://regeringen.se/pressmeddelanden/2025/04/inbjudan-till-presstraff-om-starkt-formaga-att-hantera-storningar-pa-undervattensinfrastruktur/ (Kontrollerad 2025-07-24).

43 Risk of undersea cable attacks backed by Russia and China likely to rise, report warns | Telecoms | The Guardian (Kontrollerad 2025-07-24).

Den absoluta huvuddelen av det sjötransporterade godset fraktas på ytgående fartyg. Den infrastruktur som går över havsbottnen handlar främst om energi och kommunikation, men den är grundläggande för transportinfrastrukturen och representerar stora värden i händelse av bortfall. Mycket av infrastrukturen är dessutom mycket sårbar[44].

För transportsektorns aktörers del bör det beaktas att kommunikationssystem som avses att fungera som redundans till exempelvis rymdbunden kommunikation också blir en del av en sårbar helhet som i förlängningen kan påverka den egna verksamheten om den faller bort. Det är därför rimligt att anta att möjligheten till datakommunikation mellan Skandinavien och övriga Europa i ett skärpt säkerhetspolitiskt läge helt eller delvis kan komma att upphöra på grund av antagonistiska händelser.

I syfte att tydliggöra havsbottenkablars betydelse, och ett kombinerat användande av artificiell intelligens (AI) som hot-modellerande verktyg, ställde Trafikverket i ett internt arbete frågor om betydelsen för den svenska internettrafiken till ChatGPT. Svaren som levererades beskrev teoretiska konsekvenser vid olika grader av bortfall av den havsbotten-förlagda it-infrastrukturen i Östersjön och Nordsjön. Påverkan bedömdes i vissa fall, där möjligheterna till omdirigering av trafiken begränsats, vara så stor som 95–100 % för Sverige och Finland. Observera att dessa resultat inte är verifierade och syftar enbart till att åskådliggöra hur AI kan användas för att ge indikationer på områden som kan vara av intresse för en antagonist. Det ger samtidigt en indikation på ett möjligt beroende mellan förmågan till internetkommunikation och havskablar. Det ger i sin tur transportsektorns aktörer anledning att analysera vilken betydelse de kabelbrott som det emellanåt rapporteras om kan ha för verksamheten, om dessa avbrott är omfattande.

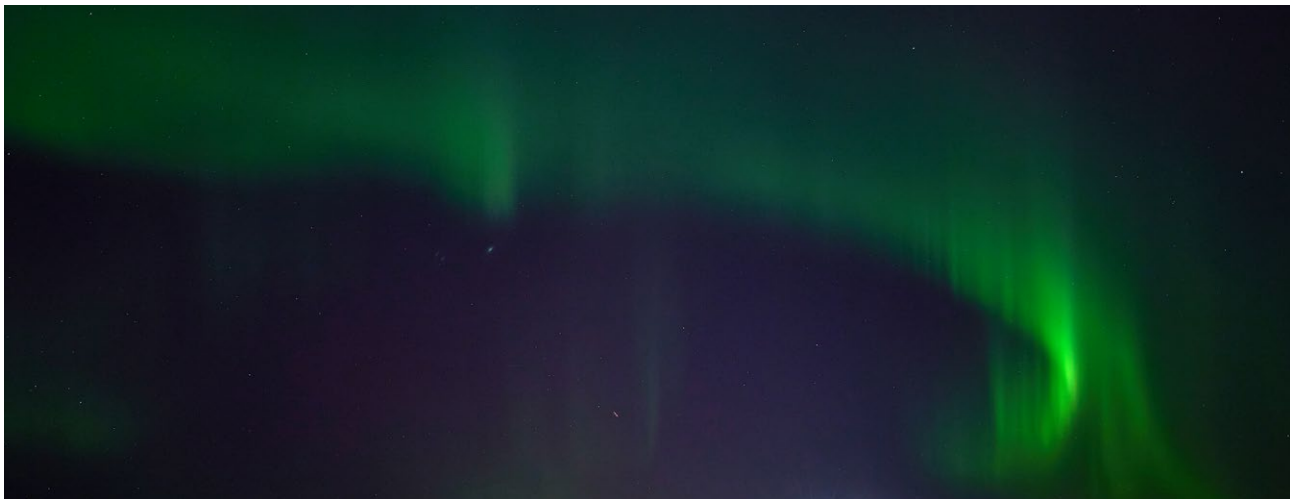
2.3.3 Arktis

Det finns olika definitioner av Arktis. En vanligt förekommande definition är att det omfattar området norr om polcirkeln (latitud 66° 33 N), där man i teorin har minst ett dygn med midnattssol på sommaren och polarnatt på vintern.

Stormaktskonkurrens, geopolitiska konflikter och teknikutveckling definierar de ökande säkerhetshoten i Arktis. Tillgång till och utvinning av råvaror i norra Sverige kan komma att öka den strategiska och ekonomiska betydelsen för området, vilket även kan komma att leda till en ökad säkerhetshotande verksamhet från främmande makt[45]. Säkerhetspolisen noterar underrättelse- och påverkningsverksamhet riktad mot svenska arktiska intressen, främst från Kina och Ryssland.

Den svenska strategin för Arktis från 2020[46] är i behov av revidering och en ny avses presenteras under 2026[47]. Omvärlden har förändrats snabbt och vi ser hur det globala intresset för Arktis ökat[48]. Utöver ryska och kinesiska initiativ så är de politiska utspelen från USA kopplat till Grönland under tidigt 2025 det som fått mest medial uppmärksamhet. Det var uppseendeväckande inte minst för att det handlar om relationen mellan två allierade Natoländer[49].

I takt med att intresset för Arktis ökar behöver även säkerhetsmedvetenheten hos de aktörer som verkar i regionen öka. Detta gäller både identifiering av säkerhetskänslig verksamhet eller utredning av incidenter vars syfte kan vara svårbegripligt[50]. Även GPS-störningarna har ökat i delar av regionen vilket innebär att den som är beroende av dessa måste agera med åtgärder och redundanta förfaranden[51].



44 https://www.svt.se/nyheter/inrikes/kansliga-svenska-internetkablar-ligger-oskyddade-pa-havsbotten (Kontrollerad 2027-07-24).

45 Årsrapportering 2023–2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

46 Sveriges strategi för den arktiska regionen. Regeringskansliet, 2020.

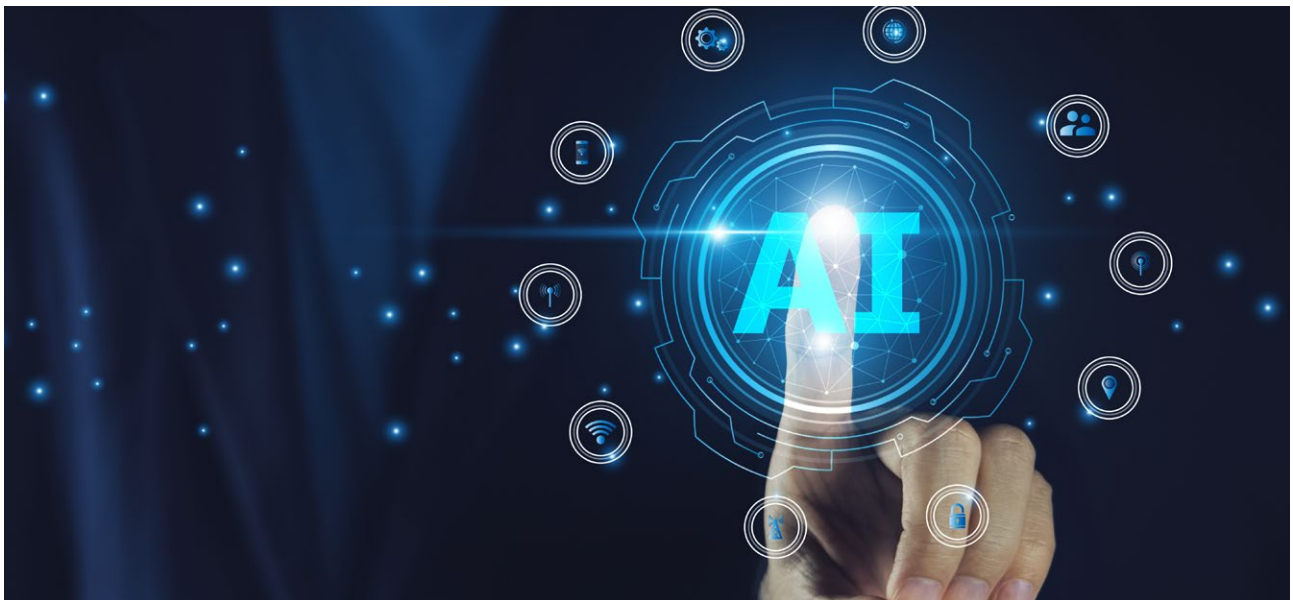
47 https://www.svt.se/nyheter/utrikes/natotoppmotet-i-haag?inlagg=661b5d861ccfc61ce1e38363406b5554 (Kontrollerad 2025-07-24).

48 https://www.thebarentsobserver.com/security/russia-locates-major-naval-exercise-in-previous-disputed-area-of-the-barents-sea/433793 (Kontrollerad 2025-07-24).

49 https://www.svt.se/nyheter/utrikes/trump-utesluter-inte-att-ta-over-gronland-med-vald (Kontrollerad 2025-07-24).

50 https://omni.se/skadegorelse-i-skyddsrum-hos-lkab-kablar-avklippta/a/Av9kRr (Kontrollerad 2025-07-24).

51 https://www.thebarentsobserver.com/news/someone-is-messing-with-gps-signals-in-svalbard-airspace/433658 (Kontrollerad 2025-07-24).



2.4 Särskilda tekniska områden

Rymddomänen och Arktis har hanterats tidigare i detta dokument. Här beskrivs två mycket aktuella tekniska ämnen: Artificiell Intelligens (AI) och Drönare och obemannade luftfarkoster.

Säkerhetspolisen uttalade följande redan 2024[52]:

> **Ny teknik och nya områden i fokus medför konsekvenser för Sveriges säkerhet. Arktis råvaror och strategiska position tilldrar sig ett växande intresse från främmande makt vilket även påverkar svenska intressen. En tilltagande kapprustning och militarisering av rymden får också konsekvenser för Sverige då stora delar av säkerhetskänsliga och samhällsviktiga verksamheter är beroende av rymdtjänster. Den snabba tekniska utvecklingen, inte minst inom AI, innebär möjligheter men också nya hot och sårbarheter.**

2.4.1 Artificiell intelligens – möjligheter och hot

I den digitala eran har artificiell intelligens (AI) och maskininlärning blivit alltmer integrerat i vårt dagliga liv och arbete. Utvecklingen av AI har förändrat förutsättningarna för både antagonister och den som skyddar sig mot angrepp. Ur ett hotperspektiv är det statsaktörer som har störst kapacitet vad gäller användandet av AI[53].

En av de mer framstående tillämpningarna av AI är Generative Pre-trained Transformers (GPT), som används i chattbotar som exempelvis ChatGPT. Medan dessa teknologier erbjuder en rad fördelar, inklusive effektivitet och användarvänlighet, är det viktigt att noggrant överväga de potentiella säkerhetsriskerna. Detta bör göras ur två hotbildsperspektiv där det första är hur AI används av den egna organisationen, och det andra är hur en antagonist kan använda AI mot samma organisation.

I det första fallet blir frågor kring dataintegritet och i synnerhet konfidentialitet extremt viktiga. Användare kan oavsiktligt dela känslig eller personlig information med en GPT-baserad chattbot. Om denna data inte hanteras på ett säkert sätt, kan det utgöra en risk för användarens integritet. Dessutom kan all data som har delats med boten vara i fara, om den server där chattboten drivs skulle kompromitteras. Vidare finns det risker förknippade med desinformation och manipulation.

Ur det antagonistiska perspektivet så beskrivs det i den myndighetsgemensamma lägesbilden från 2023 om organiserad brottslighet[54] och hur AI utgör både hot och möjligheter:

> **Att följa teknikutvecklingen blir därmed viktigt för myndigheter för att förstå vilka sårbarheter som kan utnyttjas i framtiden och hur myndigheterna själva kan utnyttja fördelarna med AI, exempelvis hitta systematiska avvikelser. Vidare behöver myndigheterna säkerställa att automatiserade urval och avancerad dataanalys tillåts i syfte att identifiera kontrollvärda objekt avseende systematisk brottslighet.**

Även internationellt ses exempel där hotet från användandet av AI beaktas. I USA startar exempelvis Nasa ett center inriktat på översyn av användandet av AI.

AI behöver således beaktas ur flera perspektiv. De primära frågor som transportsektorns aktörer behöver ställa sig internt är hur den egna organisationen kommer att använda sig av AI och hur AI kan användas av antagonister. Då området utvecklas extremt fort i samhället arbetar i dag samtliga samhällssektorer med att analysera påverkan av AI.

52 Årsrapportering 2023–2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

53 Årsrapportering 2023–2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

54 Myndighetsgemensam lägesbild om organiserad brottslighet 2023. Polismyndigheten, 2023.

Användning av AI-verktyg för att producera och sprida innehåll i informationspåverkanssyfte är ett av de mest uppmärksammade och omskrivna sätten som hotaktörer kan nyttja AI på. En kraftig ökning av manipulering av sociala medier, desinformation och allmänt icke-autentiskt material på digitala plattformar kan göra det svårt att säkerställa trovärdigheten i den information som ges. Det finns redan exempel på hur främmande makt och våldsbejakande extremister använder AI för att generera propaganda och påverkansmaterial och hur organiserad brottslighet använder sig av AI vid bedrägerier. Som motåtgärd till detta finns i dag så kallade verifieringstjänster, där organisationer granskar material på internet i syfte att skapa en transparens kring deras riktighet. Ett exempel är SVT Verifieringshjälpen[55] där nyhetsinslag som sprids på internet granskas.

AI-verktyg kan även användas i ett ont uppsåt genom hotmodellering. Med hjälp av AI och frågeställningar till denna, kan en antagonist använda tekniken för att identifiera och prioritera mål för ett angrepp (se vidare avsnitt 2.3.2).

Slutligen måste vi också ta hänsyn till etiska och juridiska aspekter. Användningen av AI för att analysera eller generera text kan potentiellt strida mot sekretesslagar, upphovsrätten eller internationella regler om dataskydd. Detta är särskilt relevant i länder med strikta dataskyddsregler, som länderna inom EU, där GDPR (General Data Protection Regulation) styr hanteringen av personuppgifter.

Medan GPT-baserade chattbotar som ChatGPT erbjuder många fördelar är det alltså av yttersta vikt att noggrant överväga och hantera de potentiella säkerhetsriskerna. Denna typ av AI tränas mot ett stort antal texter och genom att analysera svaren som ges har forskare vid FOI lyckats extrahera 20 procent av träningsmaterialet[56]. En chattbot som tränats på sekretessbelagd information men som själv inte lagrar den, blir följaktligen skyddsvärd.

Allt detta kräver en multidisciplinär strategi som inkluderar teknologiska, etiska och juridiska överväganden för att säkerställa en säker och ansvarsfull användning av denna framväxande teknologi.

2.4.2 Drönare och obemannade luftfarkoster

Den teknologiska utvecklingen av UAV:er *(engelska: unmanned aerial vehicle)* har gått fort och under 2020-talet har dessa nyttjats både i civila och militära sammanhang. Samtidigt har drönare blivit ett växande säkerhetshot mot Sverige. Säkerhetspolisen och Försvarsmakten framhåller att hybridhotet med obemannade system kräver stärkt underrättelseinhämtning, säkerhetsskydd och samverkan mellan myndigheter.

Under 2025 rapporterades flera inkräktningar med oregistrerade drönare vid svenska flygplatser och kraftverk, vilket tvingade myndigheter att samordna responsen och förbättra rapporteringsrutiner på kort tid. Detta visar på vikten av att belysa frågan om hantering av drönare, som kan användas i flera scenarier inom gråzonen. Säkerhetspolisen beskriver läget och lämnar ett klokt budskap i sin senaste lägesbild[57]:

> **Flera gånger under det senaste året har det skett olika former av incidenter som cyberangrepp, dataintrång, drönarflygningar och uppmärksammade kabelbrott i Östersjön. Det är viktigt att vi är uppmärksamma på det som sker och är beredda att agera när det behövs. Samtidigt måste vi behålla lugnet och i så stor utsträckning som möjligt tar reda på fakta. För snabbt dragna slutsatser riskerar att gynna de krafter som inte vill Sverige väl.**

Myndigheten för samhällsskydd och beredskap (MSB) publicerade därför under våren introducerande stödmaterial för hur samhällsviktig verksamhet kan handlägga och rapportera drönarincidenter. Man producerade minneskort och färdiga rapportmallar väl värda för transportsektorns aktörer att använda i sin egen verksamhet[58].

55 https://www.svt.se/nyheter/inrikes/nu-kan-du-tipsa-svt-verifierar-med-verifieringshjalpen (Kontrollerad 2025-08-29).

56 Totalförsvarets forskningsinstitut. Attacking and Deceiving Military AI Systems, FOI-R--5396—SE. Totalförsvarets forskningsinstitut, mars 2023.

57 Lägesbild 2024–2025. ISBN: 9789186661274. Säkerhetspolisen, 2025.

58 https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/oka-skyddet-mot-terrorism-i-offentliga-miljoer/skydd-mot-dronare/ (Kontrollerad 2025-07-25).

Drönaranvändningen i Ukraina har utvecklats till en kärna i det moderna stridsfältet. Radiostyrda quadrokoptrar används för spaning, målval och snabba angrepp på avstånd, men deras effekt begränsas alltmer av elektroniska motåtgärder. Som svar har båda sidor börjat använda trådstyrda (fiberoptiska) drönare, vilka motstår störsändning och kan leverera obruten videoström och styrsignal upp till 30 km, om än med begränsad manövrerbarhet på grund av kabeln. Genom att kombinera snabbrörliga radiostyrda enheter med tåliga trådbundna system uppnås både räckvidd och hög precision, anpassat efter motmedelsläget och terrängen.

Frågan om hanteringen av en drönare blir i de flesta fall, och i ett normalläge i samhället, en polisiär fråga. Lagstiftningen kring bekämpning av drönare med utstörning är ett område som regleras inom ramen för lagen om elektronisk kommunikation (SFS 2022:482) och förordningen om elektronisk kommunikation (SFS 2022:511).

Radiostörsändare är något som ofta förs fram i debatten om motmedel mot obemannade luftfartyg. I kapitel 5 i förordningen om elektronisk kommunikation tydliggörs dock att användandet av radiostörsändare inte är tillgängligt brett, men att det kan vara ett verktyg för exempelvis Polismyndigheten.

Ett alternativt för transportsektorns aktörer kan då vara olika metoder eller stöd för detektering av drönare eller drönarpilot. Detta dokument redogör dock inte för djupare tekniska möjligheter eller juridiken kring området, utan belyser i stället vikten av att kunna tillhandahålla så aktuell och precis information som möjligt till de myndigheter som har i uppgift att operativt hantera incidenten, exempelvis Polismyndigheten eller Försvarsmakten. Samtidigt behöver man som verksam inom transportsektorn analysera på vilket sätt en antagonist skulle kunna gå till väga exempelvis genom att använda lätta, eventuellt också trådbundna, drönare försedda med fjärraktiverad last såsom en störsändare.

2.5 Tystnadskultur som sårbarhet

Rapporteringsviljan kring missförhållanden i en organisation är viktig ur ett säkerhetsperspektiv. När en organisation, eller delar av den, präglas av en tystnadskultur, blir den sårbar för antagonister. Tystnadskultur som sådan kan inte med självklarhet sägas ha ett antagonistiskt uppsåt. Däremot utgör den en direkt sårbarhet i verksamheten då den motverkar skapandet av tillit inom organisationen och blir en katalyserande grogrund för uppkomsten av insiders. Brist på transparens kan leda till missnöje i en organisation, vilket gynnar antagonistiska krafter.

Tystnadskultur har en stark koppling till uppkomsten av möjliggörare. Under 2025 har TCO publicerat en rapport om tystnadskultur[59] i det offentliga. Man skriver där bland annat att ett antal studier har också visat att det blivit svårare för offentliganställda att föra fram kritik och avvikande synpunkter, bland annat på grund av att rädslan för repressalier har ökat. Vidare finns det andra studier som indikerar samma sak och beskriver en utökad och utbredd rädsla för repressalier än vad som tidigare varit fallet[60].

Efter de amerikanska bombningarna av iranska kärnanläggningar sommaren 2025 gavs något motstridiga uppgifter kring vilken verkan som uppnåtts i målen. President Donald Trump meddelade att anläggningarna utplånats, vilket motsades av läckta underrättelsedokument. Det intressanta med denna händelse var de efterföljande reaktionerna från presidenten och administrationen, som i princip kunde tolkas som förvarning om inkommande repressalier och inkompetensförklarande av den egna underrättelsetjänsten då man milt sagt inte delade samma bild av situationen. Presidenten ansåg sig här ha ett uppenbart tolkningsföreträde framför underrättelseexperterna.

59 Tyst förvaltning – Tjänsteman i offentlig förvaltning – om roller, reformer och konsekvenser för demokratin. TCO, 2025.

60 På upplyst grund – en ESO-rapport om myndigheternas remissarbete. Expertgruppen för studier i offentlig ekonomi 2024:5. Berglöf, E., Settergren, O & Sundström, G. Regeringskansliet, 2024.

För att ta detta resonemang vidare backar vi till tiden inför Rysslands fullskaliga invasion av Ukraina. Flera källor har över tid uppgett att den ryska statsledningen med president Vladimir Putin i spetsen hade förväntat sig en enkel militär operation som skulle vara över på några dagar. Det kan nog med viss trygghet antas att det råder något av en tystnadskultur inom den ryska byråkratin. Den ryska staten tycks ha skapat en förnämlig kultur där framförandet av dåliga besked bestraffas och goda nyheter belönas[61]. I förlängningen leder detta rimligen till en viss motvilja inför möjligheten att vara den budbärare som behöver framföra ett av ledningen inte uppskattat besked. Det leder i sin tur till att dessa besked inte når ledningen som följaktligen fattar beslut på fel grunder.

Mot bakgrund av att Ryssland gjorde tre avgörande strategiska antaganden[62] som alla skulle motbevisas inom det första dygnet av kriget är ett rimligt antagande att beslutsunderlaget har varit behäftat med vissa brister. För det första trodde man att den ukrainska regeringen var svag och skulle falla under trycket från ryska militära operationer. För det andra antog man att den ukrainska militären var svag och inte skulle slåss länge om den utmanades av Rysslands militära övermakt. För det tredje, och kanske viktigast, antog president Putin att Nato inte skulle erbjuda något betydande diplomatiskt eller militärt stöd till Ukraina, med tanke på deras i stort sett passiva inställning till invasionen av Krim och östra Ukraina 2014.

För att återgå till påverkan på den svenska transportsektorn är det av yttersta vikt att motverka tystnadskultur och ja-sägande. Transportsektorns aktörer behöver också vara medvetna om att detta innebär att det även är en säkerhetshöjande åtgärd att tydligt informera både underentreprenörer och egen personal om uppförandekoder i allmänhet och om möjligheten att använda visslarsystem i synnerhet. Om det finns en obenägenhet att rapportera missförhållanden eller sårbarheter inom en entreprenörs organisation riskerar uppdragsgivaren att drabbas som tredje part. En tystnadskultur ger även en grogrund för tillkomsten av insiders och kan även resultera i en rapporteringsovilja avseende säkerhetsbrister eller att skyddsvärden på alla nivåer negligeras av bekvämlighetsskäl.

Transportsektorns huvudaktörer involverar i sin tur ett stort antal underentreprenörer och leverantörer i sina verksamheter. Dessa involveras i olika grad i både icke säkerhetskänslig och säkerhetskänslig verksamhet. Det innebär oftast att frågor och problem löses på daglig basis tillsammans med underentreprenörer. I vissa fall är svårigheterna av allvarligare art, som vilka kan innebära skada för huvudmannen.

Det finns exempel där en myndighet under en längre period påtalat svårigheter kopplat till säkerhetsbrister utan att leverantören lyckats presentera en lösning. När problematiken eskalerats i motpartens organisation har det framkommit att den högre ledningen meddelar att frågan inte har lyfts internt och därmed ska ha varit okänd för dem. I detta läge finns flera möjliga förklaringar till händelseutvecklingen varav tystnadskultur inom underentreprenörens organisation är en. Huvudmannen drabbades således genom att en säkerhetsfråga inte får sin lösning på grund av en tystnadskultur hos underentreprenören, bland annat av rädsla för repressalier.

Det är också viktigt att vara på uppmärksamhet på situationer där problem kopplade till säkerhetsfrågor drar ut på tiden, att agera snabbt och tydligt och att eskalera säkerhetsproblem internt såväl som externt.

Många organisationer har avtal med en extern part för mottagande av tips om mutor, korruption eller andra missförhållanden. Den som lämnar ett tips till tipsmottagningen bör rimligen kunna välja att vara anonym. Det finns även ideella organisationer mot korruption såsom Transparency International. Till dem kan den som vill rapportera missförhållanden vända sig till för rådgivning (om rapportering i den egna organisationen inte bedöms som ett möjligt alternativ). Trafikverket har också som sektorsansvarig beredskapsmyndighet ett anmälningssystem för missförhållanden på www.trafikverket.se.

61 Försvaret av Sverige. Jonsson, 2024. ISBN 9789180025003. Mondial ,2024.

62 https://www.lowyinstitute.org/the-interpreter/why-putin-keeps-making-same-ukraine-mistakes (Kontrollerad 2025-07-25).

3 Antagonister

I den nationella säkerhetsstrategin beskrivs hur de hot mot vår säkerhet som kommer från omvärlden och de som kommer inifrån Sverige i dag är så nära sammanflätade att hotbilden måste ses som en helhet[63]. Som strukturerat stöd vid dimensionering av skyddsåtgärder beskrivs dock ett antal antagonister. Nedan följer en mer fördjupad genomgång av den information som finns om dessa, baserat på de källor som redovisas under kapitlet Litteratur och referenser i detta dokument.

De antagonister som redogörs för är statsaktörer, terrorister samt den organiserade brottsligheten. Olika typer av antagonister kan använda sig av samma tillvägagångssätt, men med olika syfte. Ett exempel på detta är cyberangrepp som varieras beroende på i vilket syfte tillvägagångssättet är aktuellt. Syftet kan exempelvis vara att tjäna pengar via utpressning genom så kallad ransomware eller att stänga ner driften av samhällsviktiga system.

Även om detta kapitel har delat upp de olika huvudtyperna av antagonister så går utvecklingen av antagonistiska samarbeten fort. Kopplingen mellan statsaktörer och organiserade kriminella har tidigare identifierats. Det har dessutom bland annat blivit uppenbart att Ryssland rekryterar väldigt unga personer med hjälp av sociala medier och kommunikationsappar, utan att dessa för den delen tillhör en organiserat kriminell kontext. Konsekvensen av detta är att det nu tydligt framgår att en möjliggörare, eller infiltratör således kan vara mycket ung och svår att upptäcka vid bakgrunds- eller registerkontroll.

I avsnittet förekommer begreppen materiell förmåga och immateriell förmåga. Materiell förmåga handlar om de materiella resurser som en antagonist har till sitt förfogande. Immateriell förmåga handlar om den kunskap, träning eller liknande som antagonisten har till sitt förfogande i avsikt att nyttja sin materiella förmåga.

Ryssland, Kina och Iran är de statsaktörer som enligt Säkerhetspolisen utgör de största hoten mot Sverige. Alla tre nationer bedriver underrättelseverksamhet och säkerhetshotande verksamhet i och mot Sverige[64]. I detta kapitel beskrivs antagonisterna och deras karaktär. I nästa kapitel beskrivs deras bedömda tillvägagångssätt och intresseområden mot transportsektorn.

3.1 Påverkan och angrepp från statliga aktörer

Statsaktörer bedöms ha såväl hög förmåga (materiell förmåga) och avsikt (immateriell förmåga) att operera mot Sverige. Dessa kan även ha även kapacitet för upprätthållande av stora personella resurser till olika inhämtningsbehov, då statsaktören har bredden av en komplett statsapparat att tillgå och kan inhämta förmågor från hela samhället. Förutsättningar möjliggör mycket samordnade attacker. Vissa statliga aktörer är även mycket kvalificerade inom cyberdomänen och genomför cyberangrepp på ett sätt som är storskaligt, systematiskt, uthålligt och globalt för att tillgodose det egna landets intressen. En statsaktör kännetecknas vidare av möjligheten att ha ett mycket långt tidsperspektiv som möjliggör en verkan som sträcker sig över många år. Detta är ett faktum som måste beaktas i allt arbete och i andra sammanhang där kontakter med främmande makt kan föreligga, såväl öppet som dolt.

Enligt Must är Sverige, på grund av sitt militärgeografiska läge[65], sin högteknologiska kompetens och behov av en fungerande världshandel ett land som är extra sårbart i den nu försämrade säkerhetspolitiska miljön. Must bedömer att risken har ökat för att Sverige eller svenska intressen ska utsättas för påtryckningar. Den alltmer komplexa hotbilden karaktäriseras av att olika maktmedel kopplas ihop och betraktas som delar av en och samma strategiska helhet. Dessutom har den tekniska utvecklingen möjliggjort att användandet av nya tillvägagångssätt för antagonistiskt agerande blivit vanligare, ofta oberoende av geografiskt avstånd.

63 Nationell säkerhetsstrategi. Skr: 2023/24:163. Regeringskansliet, 2024.

64 Årsrapportering 2023-2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

65 Försvarsmakten. Must årsöversikt 2023. Försvarsmakten, 2024.

3.1.1 Ryssland

Utöver den uppenbara avsikten att med våld angripa andra länder i syfte att uppnå sin politiska strävan har den ryska ledningen i Kreml både avsikt och förmåga att under tröskeln för en väpnad konflikt försvaga Sveriges handlingskraft. Ryssland använder kontinuerligt en rad lagliga och olagliga metoder. Det handlar om att få Sveriges och andra länders politiska och ekonomiska samarbeten samt försvarssamarbeten att försvagas.

Ryssland saknar i dag förutsättningar för en större konventionell invasion av Sverige, men kan genomföra begränsade markinsatser, maritima operationer och hybridangrepp i Östersjöområdet. Must noterar att ryska stridsfartyg, taktiska flygförband, missilsystem (Iskander i Kaliningrad) och högt utvecklade cyberförmågor finns utplacerade och kan slå mot kritisk infrastruktur.

Rysslands krig i Ukraina riktar sig såväl mot Ukrainas existens som självständig stat som mot den europeiska säkerhetsordningen i sin helhet. I stället för den regelbaserade världsordning som växt fram efter andra världskriget försöker Ryssland uppnå ett system med intressesfärer för stormakterna, där mindre och medelstora stater inte tillerkänns någon självständighet i sina säkerhetspolitiska vägval. Långsiktigheten i Rysslands agerande mot Ukraina och andra grannländer gör att det finns anledning att tro att Rysslands säkerhetspolitiska ambitioner kommer att kvarstå oavsett utgång i kriget och att dessa inte nödvändigtvis ändras av ett skifte på presidentposten.

Ryssland har under de senaste åren visat en tydlig avsikt och utvecklat sin förmåga att aktivt och dolt påverka andra stater. Denna avsikt och förmåga märks tydligt, inte minst i relationerna med västländer och i Rysslands närområde. Ryssland använder i högre grad än tidigare andra aktörer i syfte att kunna agera dolt och förnekbart, vilket har eskalerat under 2024. Målen finns i både Europa och Sverige och riskaptiten tycks ökande. Omvärldshändelser som kan gynna den ryska ledningens narrativ används utan att för den skull ha iscensatt händelseförloppet. Ryssland bedriver därmed påverkanskampanjer och använder sig bland annat av organisationer och enskilda individer[66]. Händelser i närtid som visare på ett åsidosättande av internationell rätt som direkt berör transporter är exempelvis kapningen av fartyget Green Admire under gång på en överenskommen farled[67].

Ryssland har i och med västvärldens stöd till Ukraina också visat större intresse och högre riskbenägenhet när det kommer till agerande som syftar till att störa understödsleveranser. Under 2024 har säkerhetshotande verksamhet som sabotage, angrepp och kartläggningsförsök riktats mot säkerhetskänsliga verksamheter i Sverige och övriga Europa. Detta är en utveckling som bedöms vara eskalerande och som även kan komma att involvera operationer genom ombud (proxy). Brister i den fysiska säkerheten är den vanligaste orsaken till incidenter[68]. Sedan tidigare har Ryssland utökat användningen av så kallade illegalister som en kompensation för utvisning av underrättelsepersonal från utländska beskickningar. Såväl den svenska säkerhetspolisen som andra europeiska säkerhetstjänster har i slutet av sommaren 2024 gått ut med information om att Ryssland även rekryterar kriminella i avsikt att exempelvis utföra sabotage.

Säkerhetspolisen beskriver begreppet förbrukningsagenter och den metod som tycks bli vanligare, möjligen som en konsekvens av det stora antalet utvisade ryska ambassadtjänstemän runt om i Europa.

> **Under senare tid finns indikationer på att Ryssland i allt högre utsträckning använder sig av vad som kan kallas förbrukningsagenter, det vill säga personer som används för enstaka uppdrag. Dessa förbrukningsagenter rekryteras och instrueras huvudsakligen via sociala medieplattformar och används sedan för att utföra både enklare och mer komplexa sabotage- och påverkansoperationer i Europa. Vad som därefter händer med de här personerna är ur ryskt perspektiv ofta inte intressant[69].**

Det finns dokumenterade fall kring denna verksamhet där till exempel belgiska journalister infiltrerade ett ryskt internetforum och erbjöds olika typer av uppdrag mot ersättning[70].

66 Årsrapportering 2023-2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

67 https://kkrva.se/kapning-i-ostersjon/ (Kontrollerad 2025-07-28).

68 Årsrapportering 2023-2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

69 Årsrapportering 2023-2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

70 https://www.svt.se/nyheter/inrikes/journalister-infiltrerade-ryskt-forum-erbjods-sabotageuppdrag (Kontrollerad 2025-08-29).

3.1.2 Kina

Kina har en långsiktig avsikt att stärka landets position ekonomiskt och ideologiskt genom en förändrad världsordning. Landet har avsikt och förmåga att försvaga Sveriges handlingskraft. Sverige ligger geografiskt långt från Kina, men tydligt inom den kinesiska intressesfären vad gäller Kinas långsiktiga militära, ekonomiska och politiska mål. Man söker aktivt information och kunskap som finns och utvecklas i Sverige och landet har infört lagkrav på kinesiska medborgare och företag att dessa ska stötta och samarbeta med de nationella underrättelsetjänsterna.

För att nå en ökad militär förmåga sker i Kina en fusion mellan civil och militär verksamhet, vilket innebär att civil teknik inkorporeras i militär materielutveckling. Den kinesiska staten nyttjar kinesiska medborgare vid svenska högskolor och universitet i syfte att inhämta teknik och kunskap som ökar den kinesiska militära förmågan[71].

Säkerhetspolisen har sett hur det kinesiska underrättelsehotet har breddats och fördjupats vilket nu även omfattar cyberspionage, strategiska uppköp och påtryckningar eller hot mot bland annat svenska politiska beslutsfattare, forskare och offentliga personer. Mycket av Kinas underrättelseinhämtning mot Sverige sker genom cyberinhämtning. Utöver detta bedriver landet också underrättelseverksamhet med bas i den egna ambassaden. Likt ryska underrättelseofficerare agerar även kinesiska underrättelseofficerare under diplomatisk täckmantel i Sverige och de använder sig även av journalistisk täckmantel. Kina arbetar också aktivt med värvning vilket ofta sker i ett tredje land, men det sker även rekryteringsförsök genom falska profiler på sociala medier.

3.1.3 Iran

Iran har huvudsakligen fokus på oppositionella grupper eller enskilda individer. Iran har använt våld i Europa. Landet använder sig även av ombud och i februari 2024 rapporterade media om avslöjade iranska mordplaner riktade mot personer bosatta i Sverige. I maj samma år informerade Säkerhetspolisen om att man hade uppgifter om att Iran agerade genom kriminella nätverk i Sverige främst mot israeliska mål. Fokuset på den egna diasporan innebär inte att Iran inte riktar sig mot andra stater.

Nationellt centrum för terrorhotbedömning (NCT) bedömer att Iran, genom ombud, har utfört terrorattentat och nyttjats till stöd för iranska förnekbara attentat riktat mot oppositionella, amerikanska, judiska och israeliska mål. Det är troligt att Iran under 2025 har för avsikt att genomföra attentat mot mål i Sverige, själva eller genom ombud. Potentiella mål utgörs sannolikt främst av judiska eller israeliska mål samt iranska dissidenter och andra upplevda meningsmotståndare[72].

3.2 Den organiserade brottsligheten – komplex och med pengar som drivkraft

Den organiserade brottsligheten är verksam inom flera brottsområden och den faller ofta in under flera sektorsansvariga myndigheters ansvarsområde[73]. Ett förekommande syfte för de kriminella aktörerna är möjligheten till ekonomisk vinning genom olika brottsliga upplägg. Regeringen lade den 1 februari 2024 fram en nationell strategi mot organiserad brottslighet[74]. I denna är det två av fem strategiska mål som särskilt kan lyftas i detta sammanhang. Det ena är ”Slå sönder den kriminella ekonomin” med delmålen ”Förhindra utnyttjandet av offentliga medel”, ”Förhindra att företag används som brottsverktyg” och ”Öka återtagandet av brottsvinster”. Ett annat strategiskt mål är ”Bygga robusthet mot otillåten och otillbörlig påverkan” med delmålen ”Värna integriteten i offentligt beslutsfattande”, ”Ta fram en ny handlingsplan mot korruption” och ”Förebygga hot från insidan i form av insiders och infiltratörer”.

Kärnan i strategins resonemang är ekonomins betydelse som drivkraft för den organiserade brottsligheten.

Ekonomisk vinning är en av de viktigaste drivkrafterna för organiserad brottslighet. Genom kriminaliteten pågår en omfattande omfördelning av medel från skattebetalare och brottsutsatta personer och företag till kriminella individer och nätverk. Inkomsterna från brottslighet möjliggör inte bara grundläggande försörjning och statushöjande konsumtion för kriminella individer utan används också för återinvesteringar i brottslig verksamhet, inklusive terrorism. Brottsvinster används exempelvis för att köpa upp företag och ger därigenom en ingång till legala marknader.

Utöver detta lyfts risken för målinriktad infiltration och tillskapandet av insiders i skrivelsen. I kommande kapitel beskrivs mer om arbetsmetoder för infiltration och insiders i den egna organisationen.

Sveriges brottsbekämpande myndigheter identifierar i sin lägesbild från 2025[75] kring organiserad brottslighet att det allvarligaste hotet utgörs av dess förmåga att utöva samhällshotande strategier mot:

- den fria konkurrensen inom den ekonomiska sfären
- det demokratiska statsskickets grundläggande processer
- medborgarnas fysiska säkerhet.

71 Årsrapportering 2023–2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

72 Nationellt centrum för terrorhotbedömning. Helårsbedömning 2025. Nationellt centrum för terrorhotbedömning, 2025.

73 Myndigheter i samverkan mot den organiserade brottsligheten 2024. Polismyndigheten, 2025.

74 Motståndskraft och handlingskraft - en nationell strategi mot organiserad brottslighet, Skr: 2023/24:67. Regeringskansliet, 2024.

75 Myndighetsgemensam lägesbild om organiserad brottslighet 2025. Polismyndigheten, 2025.

Flera av hoten som identifierades i lägesbilden 2021 respektive 2023 gäller fortfarande vilket de kan vara bra att ha i åtanke vid bedömning av hur och var organiserad brottslighet kan angripa den egna verksamheten:

- ekonomisk brottslighet som ett allt viktigare inslag i organiserad brottslighet
- den geografiska utbredningen av organiserad brottslighet och dess påverkan på lokalsamhället
- otillåten påverkan
- angrepp på utbetalande system och undandragande av skatter och avgifter
- framväxandet av parallella samhällsstrukturer som utmanar rättsstaten.

Beskrivningen av hoten visar att bilden av den kriminella organisationen har förändrats de senaste åren, både till strukturen och tillvägagångssättet[76]. Hotbildsaktörer kan uppträda i synligt legala strukturer genom företag och offentliga roller. Detta kan skapa möjligheter att utnyttja sårbarheter hos myndigheter och organisationer genom korruptionsförsök, infiltration och otillåten påverkan för att skaffa information, påverka ett beslut eller för att tillgodogöra sig pengar från brott.

Ur ett europeiskt perspektiv bedöms den organiserade brottsligheten som samhällsfarlig och korruptionsskapande för samtliga ingående länder. Europol liknar denna typ av brottslighet med den mytologiska hydran som inte dör om man hugger huvudet av den, utan nya huvuden växer ut och ersätter det tidigare. Europeiska polismyndigheter har genom årtionden och med omfattande resurser försökt tackla fenomenet, men konstaterar att den organiserade brottslighetens flexibla strukturer och benägenhet till förändring och anpassning har gjort att den aldrig avstannat eller bräckts[77]. Europol menar vidare att allvarlig och organiserad brottslighet utgör ett av de allvarligaste hoten mot EU och dess medlemsstater.

Europols SOCTA-rapport listar följande brottsområden som de huvudsakliga kriminella hoten mot de europeiska länderna:

Kriminella nätverk, inkluderat infiltration och korruption, penningtvätt och skjutvapenvåld.

Cyberangrepp, med en ökande trend i antalet attacker samt tilltagande förmåga i området.

Smuggling av varor, narkotika och människor. Bland annat nätverk som specialiserar mot smuggling av illegal arbetskraft från områden som kännetecknas av hög arbetslöshet och låg kunskap om moderna arbetsrättsvillkor. Bedrägerier, ofta med myndigheter och företag som måltavlor. Detta inkluderar phishing och andra typer av bedrägerier som sker i den digitala miljön.

Egendomsbrott. Denna brottstyp är vanligt förekommande i Europa och inkluderar tillgrepp och specialiserade stöldligor. Kringresande aktörer kan genom fri rörlighet och goda kommunikationer röra sig snabbt mellan länder och regioner inom Europa på kort tid.

Miljöbrott. Organiserad brottslighet utnyttjar och infiltrerar pågående klimat- och miljöinitiativ genom stölder eller oegentligheter inom återvinning och förnybara råvaror.

76 Myndighetsgemensam lägesbild om organiserad brottslighet 2023. Polismyndigheten, 2023.

77 Myndighetsgemensam lägesbild om organiserad brottslighet 2023. Polismyndigheten, 2023.

3.2.1 Digitalisering och globalisering skapar möjligheter för den organiserade brottsligheten

Det svenska samhällets höga grad av digitalisering med exempelvis e-förvaltning, automatiserade system och service till allmänheten dygnet runt skapar möjligheter för den organiserade brottsligheten. Den därtill pågående globaliseringen innebär att kriminella och deras nätverk i allt mindre grad knyts till geografiska platser. Den organiserade brottsligheten har exempelvis fått ökade möjligheter att anskaffa de resurser som behövs för olika brottsupplägg och för att flytta brottsvinster mellan länder. Fri rörlighet mellan länder gör det lättare för internationella nätverk att verka i flera länder.

Organiserad brottslighet drivs av möjligheten att med så liten risk som möjligt tjäna så stora summor som möjligt. Den materiella förmågan kan bestå av pengar eller våldskapital.

I de fall som immateriell förmåga, det vill säga kunskap och kompetens, saknas kan denna hyras in. Detta upplägg är känt som "crime-as-a-service" och berörs längre fram i texten. Det är en rimlig bedömning att motivationen från de kriminellas håll att investera tid och pengar ökar i proportion till möjligheten till ekonomisk vinst. Europol rapporterar att korruption och utnyttjande av legala affärsstrukturer är framgångsfaktorer för den allvarliga och organiserade brottsligheten i Europa. Två tredjedelar av de kriminella använder sig av korruption regelbundet och mer än 80 procent av de kriminella nätverken använder sig av legala affärsstrukturer[78]. I detta kan konstateras att kriminella nätverk strävar efter att infiltrera legitima företag eller myndigheter i syfte att stödja eller bedriva sin egen verksamhet i skydd av företagets egen.

I den myndighetsgemensamma lägesbilden om organiserad brottslighet från 2023 lyfts lågkonjunkturens påverkan fram. Då antalet arenor för de kriminella nätverken minskar i en lågkonjunktur ökar risken för de mål som kvarstår. Polismyndigheten uttrycker det så här i sin lägesbild från 2023:

> **Den ekonomiskt ansträngda situationen med hög inflation, högt ränteläge och lågkonjunktur kommer sannolikt att hämma investeringsviljan och begränsa marknaden för riskbranscher. Ett exempel är byggbranschen som har en central roll vad gäller konjunkturen och en viktig roll inom organiserad brottslighet. Stora infrastrukturprojekt blir tydligare målval när andra byggprojekt bromsas och avstannar[79].**

3.2.2 Den ekonomiska brottslighetens påverkan på transportsektorn

Transportsektorn omsätter varje år stora summor. Detta sker i samband med transporter samt utveckling och underhåll av infrastruktur. Diversiteten inom sektorn gör att den enskilde aktören behöver analysera sin ekonomi och det monetära flödet inom verksamheten och skärpa sin vaksamhet på oegentligheter.

Detta måste kombineras med hänsyn till risken för otillbörlig påverkan eller infiltration från exempelvis kriminella nätverk. Vid bedömning av vilja och uppsåt hos antagonister att attackera verksamheten måste vikt läggas vid de ekonomiska volymerna som ingår i bedömningen samt att det finns ett reellt hot om användandet av infiltration och korruption.

78 European SOCTA 2021 – Serious and organised crime threat assessment. ISBN 978-92-95220-23-2. Europol, 2021.

79 Myndighetsgemensam lägesbild om organiserad brottslighet 2023. Polismyndigheten, 2023.

Det bedöms råda en generellt bristande kunskap både om korruptionens negativa konsekvenser och om hur korruptionsbrott faktiskt kan yttra sig i praktiken. Polisens rapporter beskriver flera metoder som är relevanta att inkludera i analysen av den egna verksamheten – exempelvis hur intressekonflikter i kombination med mutor kan ta sig konkreta uttryck. Ett sätt är att en anställd attesterar fakturor från en leverantör till vilken den anställda har en personlig koppling, till exempel genom släktskap eller äktenskap med leverantörsföreträdaren[80].

Större vinst per insats ger högre sannolikhet för brott. Det ökar också sannolikheten för att de immateriella och materiella resurserna som den kriminella organisationen är villig att investera ökar.

3.3 Terrorism och utvecklingen i extremistmiljöerna

Terrororganisationer strävar efter att med våld eller hot om våld injaga fruktan i befolkningen och därigenom påverka samhället i syfte att uppnå religiösa eller ideologiska mål. Vid bedömning av terrorhot används även här begreppen förmåga samt avsikt hos antagonisten att genomföra ett attentat. Förmågan kan ha inskaffats exempelvis vid resor till konfliktområden och återförs sedan när terroristen återvänder till Sverige. Avgörande är därefter om avsikten, det vill säga viljan att genomföra attentat i Sverige är bibehållen. Både materiell och immateriell förmåga varierar, men kan antas vara lägre än för statsaktören.

I februari 2025 inträffade den värsta masskjutningen i Sveriges historia när en ensam gärningsman öppnade eld på Campus Risbergska i Örebro. Elva personer, inklusive gärningsmannen, dödades och sex personer skadades. Den 2 juni 2025 meddelade polisen att förundersökningen lagts ned[81] samt att brottet inte klassades som terrorbrott. Det som skiljer denna händelse från en terrorhandling är att syftet med skjutningen i detta fall inte är fastställt i enlighet med kriterierna för terrorbrott. Attentatet som sådant, med en ensamagerande gärningsperson, är en situation som varje organisation behöver ta i beaktande i sin krishanteringsplanering oavsett bakomliggande motiv.

I Sverige används en femgradig skala för att ange hotnivå och nivåstegen är följande: inget hot (1), lågt hot (2), förhöjt hot (3), högt hot (4) och mycket högt hot (5). Nationellt centrum för terrorhotbedömnings (NCT) terrorhotnivåer för Sverige grundar sig på strategiska bedömningar av aktörers avsikt och förmåga att begå terrorhot mot Sverige.

Under 2024 har Sverige återgått till att betraktas som ett legitimt mål, jämte många andra västländer, för internationella islamistiska terrororganisationer. Det ska jämföras med det mer specifika utpekandet som rådde under 2023[82].

Säkerhetspolischefen beslutade den 23 maj 2025 att sänka terrorhotnivån från högt hot (4) till förhöjt hot (3) på en femgradig skala, som ett resultat av en samlad bedömning[83]. Inom ramen för denna hotnivå ryms att terrorattentat kan komma att ske. Fokuset kring Sverige som målval kan röra sig i olika allvarlighetsgrad över året och kan periodvis vara högre eller lägre. Utvecklingen inom området kan dock snabbt accelereras baserat på enskilda händelser i Sverige eller utomlands. NCT beskriver i sin sammanfattande bedömning för 2024[84] att Israels krig mot den terrorstämplade organisationen Hamas sannolikt kan ha bidragit till en lägre intensitet i de hot som specifikt riktades mot Sverige under slutet av 2023.

80 Korruption i Sverige – En lägesbild. Årsrapport från Nationella Antikorruptionsgruppen. Polismyndigheten, 2024.

81 https://polisen.se/aktuellt/nyheter/bergslagen/2025/juni/forundersokningen-efter-skolattacken-pa-campus-risbergska-ar-nerlagd/ (Kontrollerad 2025-07-29).

82 Helårsbedömning 2025. Nationellt centrum för terrorhotbedömning, 2025.

83 https://www.regeringen.se/pressmeddelanden/2025/05/sakerhetspolisen-har-beslutat-om-sankt-terrorhotniva/ (Kontrollerad 2025-07-18)

84 Helårsbedömning 2024 Sammanfattning. Nationellt centrum för terrorhotbedömning, 2024.

3.3.1 Våldsbejakande islamistiska och högerextrema rörelser står för största hoten

Den våldsbejakande högerextremistiska miljön och den våldsbejakande islamistiska miljön utgör de främsta terrorattentatshoten mot Sverige. NCT bedömer att den högerextremistiska miljön är i en trolig uppåtgående trend. Den islamistiska miljön bedömdes tidigare som något stagnerande i jämförelse med de höga nivåerna under IS-kalifatets tid. Inom dessa miljöer finns det sannolikt enstaka personer som med avsikt och förmåga kan utföra ett terrorattentat i Sverige.

Terrorhotet mot Sverige, på en mer strategisk nivå, måste ses i en bredare, författningshotande kontext inom ramen för gråzonen. Etablering av mer subversiva metoder riskerar att bland annat verka polariserande och undergräva förtroendet för samhällets institutioner. Denna utveckling noteras i såväl de våldsbejakande islamistiska som de våldsbejakande högerextremistiska miljöerna[85].

De flesta attentat i västvärlden har sedan ett antal år utförts av ensamutförande individer som på eget initiativ inspireras och utvecklar attentatsavsikt och därefter planerar samt genomför ett terrorattentat. Det är troligt att denna trend kommer fortsätta även framgent. Om ett terrorattentat genomförs i Sverige i dagsläget kommer det troligen utföras av en ensamutförande gärningsperson eller en mindre grupp av likasinnade med hjälp av lättillgängliga medel[86].

Ensamutförande gärningspersoner befinner sig ofta utanför eller i utkanten av kända våldsbejakande extremistmiljöer. Deras motivbild är ofta konstruerad utifrån våldsbejakande extremistisk propaganda och tidigare utförda terrorattentat. Det är även vanligt att individuella omständigheter som personliga motgångar, psykisk ohälsa och upplevd frustration till följd av omvärldshändelser har en pådrivande effekt till att en person utvecklar attentatsavsikt. En bidragande arena till radikalisering bedöms vara den virtuella gemenskapen på digitala plattformar. I dessa sociala nätverk och slutna forum har ensamutförande funnit ideologiska kontexter som inspirerar och uppmuntrat till planering och utförande av terrorattentat. Detta är en trend som bedömts som sannolik att fortsätta.

Säkerhetspolisen oroas över att det radikaliserande internetklimatet med ökande desinformation och spridning av konspirationsteorier kan bidra till en minskad tilltro till samhället och ett hat mot myndighetsföreträdare. Detta kan även förändra den traditionella synen på de våldsbejakande miljöerna, där indelningen i en vänster-till-höger-skala ersätts med ett bredare hot mot samhällsföreträdare som är att anse som antidemokratiskt och samhällsföraktande. På längre sikt riskerar utvecklingen att driva på polariseringen i samhället och bidra till attentatshot såväl som författningshot.

3.3.2 Terrorhot och attentat

Det finns således ett långsiktigt hot mot demokratin från islamistiskt, högerextremistiskt och vänsterextremistiskt våldsbejakande miljöer. Det främsta terrorattentatshotet mot Sverige under 2025 kommer sannolikt från aktörer som agerar utifrån en våldsbejakande islamistisk alternativt en våldsbejakande högerextremistisk bevekelsegrund enligt NCT.

85 Helårsbedömning 2025. Nationellt centrum för terrorhotbedömning, 2025.

86 Helårsbedömning 2022. Nationellt centrum för terrorhot-bedömning, 2022.

Terrorattentatshotet från både våldsbejakande islamister och våldsbejakande högerextremister har minskat under 2024. Under 2024 har det skett sju terrorattentat med våldsbejakande islamistisk motivbild i väst. I tre av dessa var kriget mellan Israel och Hamas den främsta motiverande och legitimerande faktorn. Under 2024 har ett terrorattentat med våldsbejakande högerextremistisk motivbild genomförts. Sammantaget utgör detta en påtaglig minskning jämfört med året dessförinnan[87].

De terrorhandlingar som utförts i västvärlden bedöms i första hand rikta sig mot större samlade grupper av allmänhet, mot militära anläggningar eller annan offentlig verksamhet inom främst rättsväsendet. Större infrastrukturella knutpunkter där mer omfattande folksamlingar mer eller mindre konstant återfinns är i sammanhanget potentiella objekt för terrorattacker, till exempel större flygplatser och järnvägsstationer.

Enligt NCT kan terrorattentatshotet även komma ifrån statsaktörer i syfte att främja dess egna strategiska intressen. Det är möjligt att terrorattentat kan ske inom ramen för så kallad statlig förnekbar våldsförmåga[88].

För transportsektorns aktörer innebär detta att sektorn inte nödvändigtvis behöver utgöra det primära målvalet av ensamutförande gärningspersoner, men att både personal, anläggningar och funktioner kan träffas som en del av en överförd hotbild där exempelvis en större folksamling utgör det primära målet. Sektorn kan direkt påverkas om exempelvis en statsaktör genom ombud, proxyaktörer, utför terrorattentat som syftar till att slå ut eller störa infrastruktur, kommunikationer eller delar av transportsektorn exempelvis kopplat till västvärldens stöd till Ukraina.

3.3.3 Våldsbejakande misantropi

Nationellt centrum för terrorhotbedömning (NCT) har granskat våldsbejakande misantropi ur ett svenskt perspektiv[89] och konstaterar att fenomenet i nuläget inte påverkar den övergripande terrorhotnivån i Sverige. Det innebär att våldsbejakande misantropi inte uppfyller NCT:s kriterier för terrorism, trots att de accelerationistiska[90] inslagen bedöms utgöra en potentiell risk för samhällssäkerheten.

Våldsbejakande misantropi är ett samlingsbegrepp för extremistisk våldsutövning som motiveras av ett generellt förakt mot människor. Fenomenet yttrar sig främst i löst sammansatta nätverk av unga personer som kommunicerar och rekryterar via digitala plattformar. Inom dessa kretsar sprids idéer om oprovocerat våld, ofta dokumenterat och glorifierat genom videoklipp som delas online. Internationellt har flera av de mest framträdande grupperna betecknats som terrororganisationer, vilket understryker våldets spridningskraft och symboliska betydelse.

I Sverige har ett antal våldsdåd kopplats till våldsbejakande misantropi. Dessa incidenter har i huvudsak karaktäriserats av impulsivitet och bristande organisatorisk struktur, där enskilda gärningsmän agerar utan långsiktig planering. Många av de utövade handlingarna motiveras av accelerationistiska idéer med föreställningen att våldet kan påskynda ett samhälleligt sammanbrott. Det pekar ut detta inslag som den mest oroande delen av fenomenet ur ett säkerhetsperspektiv.

Även om hotnivån enligt NCT är begränsad, bidrar våldsbejakande misantropiska nätverk till att sänka trösklarna för våldsanvändning, särskilt bland unga. Utöver uppmaningar till våld finns även kopplingar till annan brottslighet, såsom spridning av övergreppsmaterial, cyberbrott och utpressning, vilket komplicerar brottsbekämpande insatser.

Sammanfattningsvis framstår våldsbejakande misantropi som ett växande fenomen, men som enligt NCT för närvarande inte klassificeras som terrorism i Sverige.

87 Helårsbedömning 2025. Nationellt centrum för terrorhotbedömning, 2025.

88 Statlig förnekbar våldsförmåga- avser här statligt sanktionerad våldsanvändning utanför statens gränser som utförs av individer, grupper eller organisationer som är svåra att attribuera tillbaka till staten.

89 Våldsbejakande misantropi. Nationellt centrum för terrorhotbedömning, 2025.

90 Accelerationism kan beskrivas som en politisk strategi som bygger på grundtanken att samhällsutvecklingen följer ett ideologiskt förutbestämt schema mot undergång. Center mot våldsbejakande extremism, januari 2021.

4 Antagonistens intresseområden och arbetsmetoder

Flera europeiska länder har under 2024 pekat ut Ryssland som ansvarigt för sabotageverksamhet och incidenter såsom mordbränder och skadegörelse. Utvecklingen visar på en allt högre rysk acceptans för allvarliga konsekvenser, även med påverkan på liv och hälsa.

Så skriver Säkerhetspolisen i sin årsrapport, där de ser att främmande makts tröskel för att agera har sänkts[91].

Detta visar på behovet av vaksamhet, medvetenhet, observationsförmåga samt god rapporteringsbenägenhet inom och mellan transportsektorns aktörer. Transportsektorn är en del av den svenska vitala infrastrukturen, vilket innebär att all verksamhet inom den kommer att utvärderas av en antagonist. Detta kan ske som del i förberedelse inför framtida aktioner, i syfte att inhämta underrättelse eller helt enkelt för att studera olika verksamhetsdelar för att utvärdera om de innehåller möjligheter för angriparen att utnyttja.

Då ett flertal myndigheter och organisationer samt delar av näringslivet har viktiga roller i, eller bidrar till, det militära försvaret och därmed det svenska totalförsvaret, har Försvarsmakten under 2025 publicerat skriften Skyddsvärden för försvaret av Sverige[92]. I detta dokument redogörs kort för att skyddsvärden i det militära försvaret inte enbart återfinns inom Försvarsmakten, utan även inom andra offentliga och privata verksamheter med fokus på säkerhetskänslig verksamhet.

Det är i detta sammanhang då också viktigt att inte enbart hålla blicken på hot kopplat till väpnad konflikt eller förberedelser inför en sådan. Statsaktörer har även andra agendor kopplat till industriella försteg och flyktingspionage och det finns en ökad risk för att främmande makt bedriver olovlig underrättelseinhämtning för att inhämta skyddsvärd information kopplat till beslutsfattande och offentlig förvaltning. Till detta har debatten kring organiserade kriminellas agerande förtydligats den senaste tiden, inte minst vad gäller avsikten att infiltrera myndigheter och företag eller vad gäller situationer där kriminella anlitas av statsaktörer i olika syften.

Utländska direktinvesteringar är ett verktyg både för främmande makt och för den organiserade brottsligheten. Även handelsförbindelser används i detta perspektiv, som Säkerhetspolisen skriver i sin årsrapport för 2023–2024:

När Sverige införde ett exportförbud gentemot ett svenskt företag som Kina köpt upp slutade företaget att leverera till svensk och europeisk försvarsindustri. Kina har även tidigare infört importförbud av både norska och litauiska varor när länderna agerat på ett sätt som Kina ansett strider mot landets egna mål[93].

För transportsektorn innebär det att en god kännedom om leveranskedjans olika länkar samt de ägarförhållanden[94] som omger dessa måste beaktas för att kunna genomföra en så korrekt bedömning som möjligt av de sårbarheter och beroenden som kan uppstå.

Efter valet i USA hösten 2024 har de internationella relationerna inom väst prövats. Sårbarheter i leverantörsberoenden både inom industrin och it-området har ifrågasatts, vilket beskrivs tidigare i detta dokument.

Detta kan sedan vägas tillsammans med de intressemetoder och arbetsområden som belyses nedan såsom otillåten underrättelseinhämtning, strategiska uppköp eller investeringar, desinformation och påverkanskampanjer, otillbörlig och otillåten påverkan, cyberbrottslighet samt sabotage och organiserade stölder.

91 Lägesbild 2024–2025. ISBN: 9789186661274. Säkerhetspolisen, 2025.

92 Skyddsvärden för försvaret av Sverige – Att identifiera säkerhetskänslig verksamhet. Militära underrättelse- och säkerhetstjänsten, MUST. Försvarsmakten, 2025.

93 Årsrapportering 2023–2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

94 Research for TRAN Committee – Chinese Investments in European Maritime Infrastructure, Ghiretti et al (2023), European Parliament, Policy Department for Structural and Cohesion Policies, Brussels. Europaparlamentet, 2024.

4.1 Otillåten underrättelseinhämtning

Underrättelsehotet från andra länder mot Sverige har breddats och fördjupats. Det omfattar såväl olagliga som lagliga metoder. Vid sidan om den mer traditionella underrättelseverksamheten, där andra länder värvar agenter, eller där flyktingspionage genomförs, genomförs även andra former av säkerhetshotande verksamhet.

Säkerhetspolisen konstaterar följande i sin årsrapportering 2023–2024[95]:

> **Det allvarliga omvärldsläget påverkar hotet mot Sverige, och främmande makt agerar allt mer offensivt. Säkerhetspolisen ser att främmande makts tröskel för att agera har sänkts. Den säkerhetshotande verksamheten mot Sverige bedrivs brett där utgången av Rysslands krig mot Ukraina är avgörande för svensk säkerhet då Rysslands fokus kan komma att riktas allt mer mot väst.**

För transportsektorns aktörer är det viktigt att inte skapa möjligheter för statsaktörer att inhämta information under dolda förevändningar, exempelvis inleda samarbeten eller erbjuda studiebesök eller forskningsutbyten. Det innebär även att uppmärksamma kartläggningsförsök av egen eller underentreprenörers personal. Som exempel är uppgifter om huruvida tjänster är säkerhetsklassade enligt säkerhetsskyddslagen (SFS 2018:585), och på vilken nivå denna klassning ligger, uppgifter som bedöms vara intressanta inhämtningsmål. Nivån på säkerhetsklassningen samt orsaken bakom är skyddsvärda uppgifter och ska behandlas därefter.

Det är av intresse för en antagonist att kartlägga vem som innehar en säkerhetsskyddsklassificerad tjänst och orsaken bakom att tjänsten bedömts som skyddsvärd. Om det har bäring på Sveriges säkerhet ska detta hanteras inom ramen för organisationens säkerhetsskyddsarbete och analyseras och dokumenteras genom säkerhetsskyddsanalys[96].

4.1.1 Innovativa antagonistiska möjligheter i cyberdomänen

Detta dokument kommer inte att lista samtliga möjligheter en antagonist kan finna inom cyberdomänen utan istället beskriva några talande exempel på hur teknik, fantasi och innovation har använts av antagonister och som alltså utgör ett reellt hot.

Den främsta fördelen med informationsinhämtning genom cyberdomänen är att den kan ske utan att den som hämtar informationen behöver lämna sitt eget land. Informationen kan via internet samlas in var som helst i världen. Detta är en grundläggande motivator för all underrättelsetjänst.

Under våren 2025 riktade bland annat brittiska myndigheter skarp kritik mot Rysslands militära underrättelsetjänst GRU för ett omfattande försök att störa och kartlägga västerländskt bistånd till Ukraina genom nätverksintrång mot övervakningskameror vid gränsövergångar, järnvägsstationer och militära installationer[97]. Angriparna lyckades, utan fysisk tillgång till kamerorna, manipulera omkring 10 000 kameror i Ukraina såväl som i Rumänien, Polen, Ungern och Slovakien. Exempelvis stals autentiseringsuppgifter och sårbarheter i molnbaserade plattformar utnyttjades. Med realtidsåtkomst till kamerornas bildmaterial kunde de noggrant kartlägga rutter, tidtabeller och storlek på biståndskonvojer. Utifrån omfattningen och precisionen i angreppet bedömdes att liknande cyberspionage mot logistiska och transportrelaterade mål kommer fortsätta utgöra ett allvarligt hot under överskådlig framtid.

95 Årsrapportering 2023-2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

96 Säkerhetsskyddsanalys i teori och praktik. Söderlund & von Zeipel, 2024. ISBN 9789139027058. Norstedts Juridik, 2024.

97 https://www.theguardian.com/world/2025/may/21/russia-accused-trying-disrupt-aid-ukraine-hacking-border-crossings (Kontrollerad 2025-07-30).

En annan intressant möjlighet till kartläggning genom tillgång till annans befintliga infrastruktur publicerades i en artikel från Carnegie Mellon University[98]. I denna beskrivs hur signalen från en router för trådlöst nätverk analyseras i syfte att kartlägga personer som rör sig i ett rum. Analysen genomförs med en tränad artificiell intelligens och har en mycket god noggrannhet. Vanligen brukar det säkerhetsmässiga resonemanget kring trådlösa nätverk röra deras kryptering och motståndskraft mot avlyssning. Detta ger en ny aspekt som mer riktar sig mot signalstyrkan.

Den uppkopplade tekniken i dagens bilar öppnar för ytterligare en sårbarhet som måste adresseras. Elbilar tillverkade i länder vars lagstiftning kräver att även privata företag lämnar uppgifter till landets underrättelsetjänst kan innebära en informationssäkerhetsrisk. I detta fall är det kinesiska elbilar som undersökts och som visar på att en betydande mängd information skickas till servrar i Kina[99]. Hänsyn till att bilarna kan vara försedda med en stor mängd ljud- och bildupptagningsutrustning behöver tas ur ett säkerhetsskyddsperspektiv inte minst för när, var, hur och i vilken verksamhet bilarna är tänkta att användas.

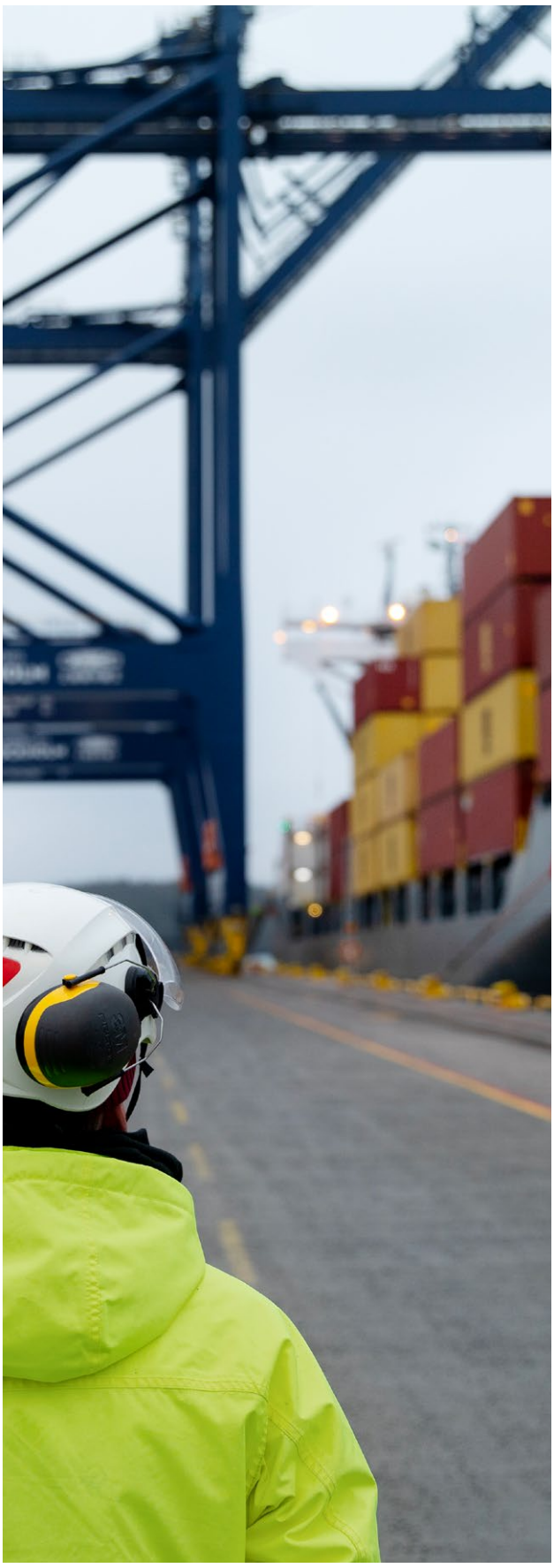
Genom dataintrång och cyberattacker stjäls i dag data som är krypterad. Detta är en fjärde aspekt där en teori är att den stulna informationen sparas tills de teknologiska framstegen inom kvantdatorer möjliggör att den dekrypteras. Detta medför i sin tur att den som i dag förvarar känslig information krypterat men med access till internet behöver värdera konsekvenserna av ett teknologiskt genombrott som innebär en enkel, obehörig, dekryptering av information om den stjäls.

Slutsatsen för transportsektorns aktörer bör bli att det är viktigt att generellt ställa sig frågan hur den utrustning som planeras att installeras eller den information som kommer att genereras kan användas av en antagonist. Installeras utrustningen i rätt, eller snarare fel, områden? Vilken data genererar vår utrustning och hur hanteras den? Den viktigaste insikten är att om en möjlighet uppenbaras för motståndaren, som i exemplen ovan, så kommer dessa att utforskas, exploateras och användas mot oss.

4.1.2 Möjliggörare (insider)

Kriminella nätverk använder personer inom legala sektorer för att underlätta brottslighet, genomföra brott, undgå upptäckt, undgå eller påverka straff eller andra åtgärder samt för att omsätta brottsvinster[100].

En annan mycket viktig aspekt att komma ihåg avseende möjliggörare (insiders) är att de inte enbart behöver inriktas på att komma över information eller medel från organisationen eller annat som nämnts ovan. Ett alternativt användningssätt, vilket kanske främst intresserar statsaktörer, skulle kunna vara att använda en insider till att försöka påverka den egna verksamheten i en riktning som är fördelaktig för angriparen.



98 DensePose From WiFi. Geng J, Huang D, och F. De la Torre. Carnegie Mellon University, 2025.

99 https://www.dagensps.se/motor/datatrafik-vacker-oro-kring-kinesiska-elbilar/ (Kontrollerad 2025-10-09).

100 Möjliggörare för kriminella nätverk – Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2. Brottsförebyggande rådet, 2024.

Det skulle kunna handla om allt från bortprioritering av säkerhetsåtgärder av till synes ekonomiska skäl till att verksamheter eller uppgifter som rimligen borde omges med säkerhetsskydd med hänsyn till Sveriges säkerhet förminskas i betydelse. Insidern kan även agera lågaffektivt och ineffektivt i den egna organisationen. I "Simple sabotage field manual"[101] från 1944 beskrivs metoder för att motarbeta den nazi-tyska ockupationsmakten. Under rubriken "Specific suggestions for simple sabotage" finns underkategorin "General interference with organizations and production", där det redogörs för ett antal möjliga antagonistiska tillvägagångssätt. Följaktligen är detta inte nya tillvägagångssätt utan utmärkta exempel på antagonistiska handlingar som är relevanta än i dag och som erbjuder en hög grad av förnekbarhet.

Problematiken här är att ett medvetet och uppdragsdrivet antagonistiskt agerande såsom konfliktsökande, baktalande och allmänt otrevligt uppträdande med mera mycket svårligen kan särskiljas från icke uppsåtligt olämpligt beteende, inkompetens eller brist på handlingskraft. Kännedomen om att detta kan förekomma innebär tyvärr också en risk att det sprids en obefogad misstänksamhet mot individer med beteendebrister i den egna organisationen som i sin tur kan bli kontraproduktivt.

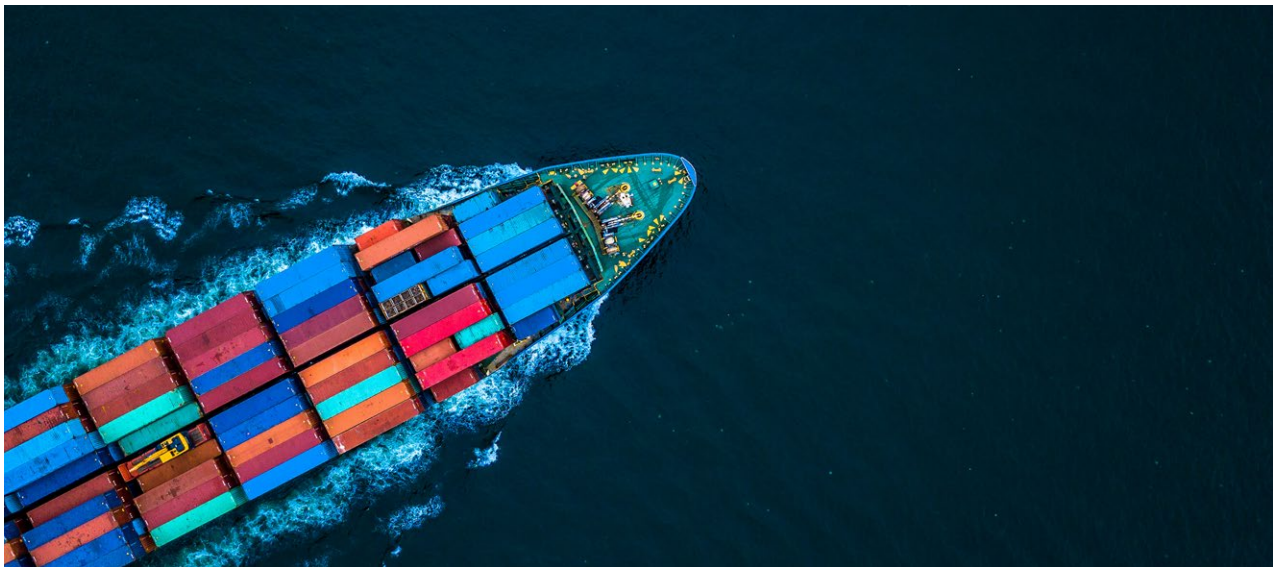
En god säkerhetsmedvetenhet, ett gott debattklimat och en transparens kring beslutsfattande är alla faktorer som syftar till att skapa en god säkerhetskultur. Säkerhetskulturen bygger på tillit och förtroende både mellan organisationsdelar och mellan de hierarkiska nivåerna i en organisation. Med en god säkerhetskultur som stöd till ledningen finns förutsättningar att för det första motverka att obefogade misstankar uppstår som påverkar samarbetsklimatet i organisationen. För det andra blir det med en förtroendeingivande säkerhetskultur mycket svårare för en insider att agera kontraproduktivt eller destruktivt. I en organisation som upplevs ge utrymme för allianser och informella styrstrukturer kan förtroende och därmed säkerhetskultur snabbt försämras.

En kraftfull hybridmetod är annars att utnyttja polarisering och misstro mellan grupper. Detta gäller för samhället i stort såväl som inom en organisation. Det kommer att bli ytterligt mycket svårare för en sabotör att så split och missämja i organisationen om samtalsklimatet mellan kollegor inte ger utrymme för den typen av beteende, utan att detta snarare upplevs som något avvikande. I det skedet kommer antagonisten själv vara den som genom sitt konfliktskapande beteende utmärker sig och därmed exponeras och riskerar att avslöja sig. Förutom att försvåra för antagonisten så ökar även en psykologiskt trygg arbetsmiljö, baserad på välvillighet och samarbetsvilja, även organisationens effektivitet[102].

4.1.3 Snäv användning av nyckelpersonal

Ytterligare en sårbarhet som kan uppstå är en snäv användning av nyckelpersonal. Det ligger i sakens natur att säkerhetsskyddsklassificerade uppgifter enbart ska delas med den som är utbildad och behörig samt har behov av uppgiften i sitt arbete. Det kan dock vara säkerhetsåtgärd att den säkerhetskänsliga verksamheten fördelas på flera behöriga och utbildade personer som var och en har behov av sin del i ett aktuellt uppdrag. Ett exempel där detta fallerat är spionen Stig Bergling som under en tjänstgöring kunde kopiera en stor mängd information om olika verksamheter som passerade honom. Bergling gavs tillgång till information som beskrev helhetssituationen för skyddsvärden och gavs möjligheten att delta i olika säkerhetskänsliga verksamheter där han kunde samla material.

Genom att säkerställa att säkerhetskänslig verksamhet, i både beslut och genomförande fördelas på ett inte alltför snävt antal individer kan skadan från exempelvis en insider minimeras. Detta kallas tjänsteseparering *(separation of duties på engelska)* och inkluderar både utförande samt flerfaktorsautentisering på beslut. En snäv användning av nyckelpersonal öppnar dessutom upp dessa individer som högintressanta för värvning.



101 Simple sabotage field manual – Strategic services field manual No. 3. Office of Strategic Services, 1944. Declassified by Central Intelligence Agency, 2008.

102 Snällast vinner. Hansson, 2024. ISBN 9789189740662. The Book Affair, 2024.

Vidare behöver risken för infiltration vid anställning eller utkontraktering bedömas, i synnerhet på positioner med centrala roller i informationsflöde eller verksamhetsstyrning. Detta behöver inte på något sätt per automatik innebära chefspositioner. Även handläggartjänster ger en antagonist dessa möjligheter.

Annan inhämtning kan också inriktas mot kunskapstung verksamhet. Det innebär att bredden av vilka mål som betraktas som intressanta ökar, exempelvis genom olika forskningssamarbeten.

För samtliga aktörer inom transportsektorn är det viktigt att komma ihåg att underrättelseområdet består av tillvägagångssätt för att nå och påverka information och motåtgärder mot dessa. Ett exempel kan utläsas ur dokumentation från ett spionerimål[103]. I detta mål tycks den misstänkte ha försökt undkomma systemövervakande åtgärder i informationssystemen kopplat till nedladdning av dokument genom att fotografera dem från en bildskärm. Ett antagande baserat på detta är då att den misstänkte har fått en instruktion från den person som har agerat som hanterare/källdrivare om hur informationen ska extraheras utan att lämna synliga spår i loggar. Denna typ av innovativt agerande kan vara svårt att förutse. Men genom att i detta fall observera ett konstaterat tillvägagångssätt, så kallat modus operandi, kan det bedömas utgöra ett beprövat arbetssätt från antagonister som alltså måste bedömas utifrån den egna organisationens identifierade sårbarheter i sina informationssystem.

4.1.4 Värvning

Vanligen används den så kallade värvningstrappan för att beskriva ett tillvägagångssätt där en statsaktör värvar en agent till sin sak. Det finns inget som motsäger att organiserade kriminella skulle använda motsvarande metod i syfte att värva en insider enbart därför att motiven från de bägge antagonisterna skulle skilja sig åt.

I Musts årsöversikt 2024[104] är Försvarsmakten tydlig med att den som är anställd, eller har kontakter i Försvarsmakten, dess samarbetspartners, totalförsvaret eller företag med försvarsinriktning kan vara intressant för främmande makts underrättelse- och säkerhetstjänst. Under rubriken ”Du är intressant!” ges ett antal exempel på personer som kan vara intressanta som målval för främmande makt, såsom trafikledare av tåg. Detta kapitel bör studeras och appliceras i egen verksamhet hos varje transportaktör vid genomförandet av risk- och sårbarhetsanalyser eller säkerhetsskyddsanalyser för att nämna några exempel. Långsiktigheten och målmedvetenheten ges ytterligare tydlighet genom beskrivningen av händelserna i boken Honungsfällan[105].

Värvningsmetodens sex steg är direkt hämtade från Säkerhetspolisens Handbok Personlig säkerhet[106].

1. Analys. Värvningsprocessen börjar med en analys av vilken information som den utländska underrättelsetjänsten behöver.
2. Målsökning. Denna analys utgör grunden för målsökningsfasen, då en underrättelseofficer får i uppdrag att hitta en person som kan dela med sig av den efterfrågade informationen.
3. Studie. Personen som underrättelseofficeren bedömer har tillgång till rätt information kartläggs sedan i en studiefas. Uppgifter om personliga egenskaper, svagheter, ekonomi och familjesituation ligger till grund för en bedömning av möjligheterna att få personen att arbeta för ett annat land.
4. Närmande. Om underrättelseofficeren anser att den utvalda personen är lämplig söker han eller hon kontakt i en närmandefas. Närmandet sker på ett sätt som ska uppfattas som spontant och slumpmässigt, men i själva verket sker kontakten mycket välplanerat utifrån de uppgifter som framkommit i studiefasen.
5. Vänskap. Om det första mötet blir lyckat inleder underrättelseofficeren en relation med den tilltänkta agenten i en vänskapsfas. Den utvalda personen utsätts för en charmoffensiv och får också oskyldiga uppdrag för att testa relationen, exempelvis genom att han eller hon blir ombedd att lämna över dokument som inte är hemliga. Personen vänjs också vid att ta emot gåvor av olika slag. Vaksamheten och omdömet bryts ner hos den utvalda personen, ibland under flera års tid.
6. Värvning. Slutligen ställer underrättelseofficeren den tilltänkta agenten inför frågan att lämna ut hemlig eller känslig information. Värvningsfasen är det svåraste ögonblicket i processen, men om det faller ut väl för underrättelseofficeren har personen blivit agent för ett annat lands underrättelsetjänst.

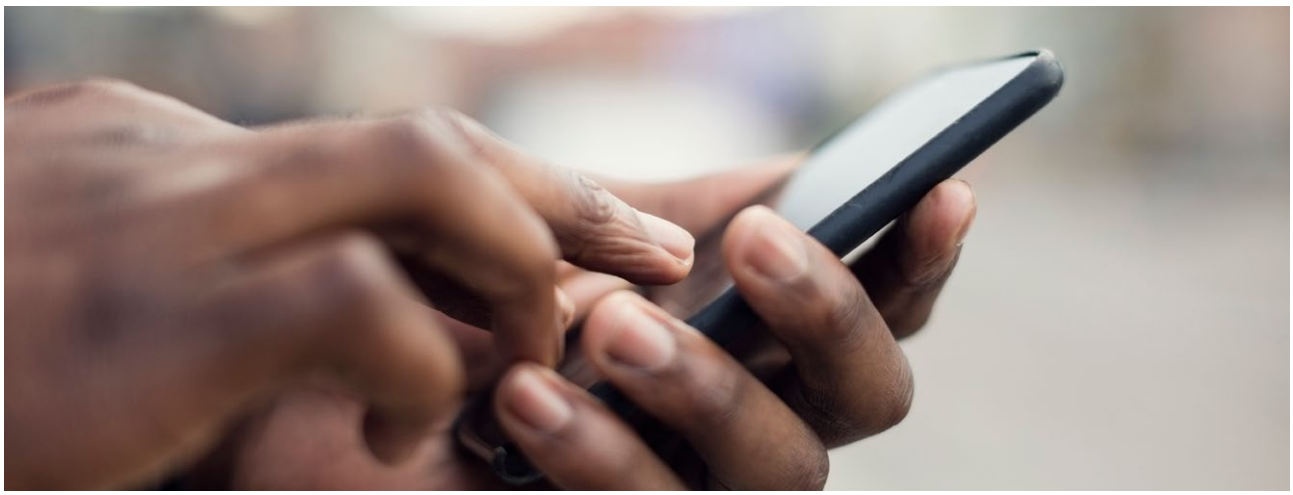
Med kännedom om metoden för värvning ökar motståndskraften och medvetenheten hos individen. Samtliga aktörer inom transportsektorn kan, med utgångspunkt i denna kunskap, initiera eget arbete i syfte att uppmärksamma egen och underentreprenörers personal på hotet. Metodbeskrivningen kan även användas i arbetet med att etablera rapporteringsvägar om misstänkta händelser och där återge steg från värvningstrappan som beskrivande exempel.

103 Göteborgs tingsrätt. Mål B 18567-20.

104 MUST årsöversikt 2024. Försvarsmakten, 2025.

105 Honungsfällan. Berge & Gordh Humlesjö, 2024. ISBN 9789100185015. Albert Bonniers Förlag AB, 2024.

106 Personlig säkerhet, fjärde upplagan. ISBN: 9789186661212. Säkerhetspolisen, 2021.



4.1.5 Kriminalitet och infiltration i den egna verksamheten

Infiltration har traditionellt fört tankarna till agerandet hos statsaktörer och då att inom ramen för olovlig underrättelseverksamhet plantera en agent i en organisation. I och med att bilden av den kriminella organisationen har förändrats de senaste åren både till struktur och tillvägagångssätt förs infiltrationshotet även från andra aktörer fram. Flera hundra internationella brottsnätverk har varit aktiva i Sverige sedan början av 2020-talet och flera nätverk med hög hotkapacitet ägnar sig åt organiserade tillgreppsbrott. Nätverken kommer bland annat från Sydamerika, Rumänien, Litauen och Polen eller från rysktalande länder. Pengar som genereras i Sverige flödar sannolikt i stor omfattning tillbaka till nätverkens ursprungsländer[107].

I flera regioner har de kriminella nätverkens förmåga blivit tydligare i fråga om att utnyttja insiders i legala verksamheter såsom banker, myndigheter och låneinstitut. Bland aktörerna finns både kriminella nätverk och mc-gäng[108].

Exempel på misstänkt infiltration som avslöjats är ett fall där en anställd på domstol misstänktes för att ha läckt uppgifter och ett annat fall där en åklagare åtalats för att ha läckt sekretessbelagd information[109]. Sådan infiltration är systemhotande verksamhet. Utöver åtgärder på personalsäkerhetsområdet så är, som tidigare nämnts, effektiva motåtgärder bland annat transparens i beslutsprocesser, välskött dokumentation och diarieföring i syfte att motverka underlag för ryktesspridning.

Inom säkerhetsskyddet finns åtgärdsområdet personalsäkerhet där säkerhetsprövning, registerkontroll och inplacering i säkerhetsklass används. Detta är inte de enda verktygen som står tillbuds vid bedömningen av en persons tillförlitlighet. Inom exempelvis reglering från Myndigheten för samhällsskydd och beredskap (MSBFS 2020:6)[110] ska bakgrundskontroll genomföras. Där anges att ”bakgrundskontroller bör ske genom intervju, kontakt med referenser samt verifiering av akademiska, yrkesmässiga och övriga kvalifikationer”. Föreskriften riktar sig till statliga myndigheter, men exempelvis standarden ISO 27001[111] omhändertar frågan om bakgrundskontroller och är applicerbar på samtliga typer av verksamheter.

För varje aktör inom transportsektorn innebär detta att medvetenheten kring hotet om infiltration behöver beaktas vid rekrytering och vid framtagande av arbetssätt och processer. Det kan exempelvis handla om att säkerställa att avgörande beslut verifieras av fler nivåer av beslutsfattare och att återkommande vidareutveckla och följa upp efterlevnaden av regelverket kring jäv och intressekonflikter[112].

Medvetenheten om infiltration har dock en uppenbar baksida i form av obefogad misstänksamhet. I alla sammanhang där en individs lämplighet ska bedömas är det den individuella prövningen som väger tyngst. En fråga som ofta diskuteras är hur dubbelt medborgarskap ska hanteras samt motiveringen till avslagen inplacering i säkerhetsklassad tjänst efter genomförd säkerhetsprövning enligt säkerhetsskyddslagen.

När ett avgörande av lämplighet ska fällas kan det vara lämpligt att reflektera över hur dialogen och återkopplingen ska föras. Om exempelvis en hotbild mot familj och släkt i ett andra medborgarland beaktats skulle detta kunna kommuniceras till den prövade i syfte att skapa en förståelse och förhoppningsvis också en samsyn om den prövades situation. Det är lika fullt möjligt att en felaktigt utförd säkerhetsprövning och olämpligt hanterad återkoppling snarare skapar förutsättningar som gör att individens lojalitetskänsla mot Sverige minskar och därmed blir processen kontraproduktiv.

I synnerhet kan detta vara värdefullt att beakta om det handlar om individer som redan har eller tidigare har haft tjänster inplacerade i säkerhetsklass inom organisationen.

107 Myndighetsgemensam lägesbild om organiserad brottslighet 2025. Polismyndigheten, 2025.

108 Myndighetsgemensam lägesbild om organiserad brottslighet 2023. Polismyndigheten, 2023.

109 Brottsmål B 2595-24. Stämningsansökan – Ärende AM-137440-24/Handling 123. Södertörns tingsrätt, 2024.

110 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter, MSBFS 2020:6.

111 Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi. ISO/IEC 27000:2018. SS-EN ISO/IEC 27000:2020.

112 Den statliga värdegrunden – gemensamma principer för en god förvaltning. ISBN 978-91-88865-23-6. Statskontoret, 2019.

4.2 Strategiska uppköp eller investeringar

Utländska direktinvesteringar är viktiga för Sveriges ekonomi och näringsliv. Det kan samtidigt leda till beroenden som möjliggör säkerhetshotande verksamhet från främmande makt[113]. Sedan 2023 gäller lagen om granskning av utländska direktinvesteringar i Sverige[114]. Syftet är att motverka strategiska uppköp eller investeringar, vilket är ett verktyg som används i dag.

Det innebär att en stat, via statsägda eller statskontrollerade företag, köper upp till exempel hamnar, transportföretag och teknikföretag. Dessa kan sedan användas för att påverka eller inhämta information eller för att skapa ett beroendeförhållande till andra länder när det gäller kritiska varor eller tjänster som är viktiga för samhällets grundläggande funktionalitet och försvarsförmåga. Likväl kan målsättningen vara att köpa upp mindre företag och entreprenörer som har tillträde till säkerhetskänslig verksamhet. Tillgång till eller kontroll över system, infrastruktur eller data möjliggör övervakning, planering inför eller genomförande av sabotage.

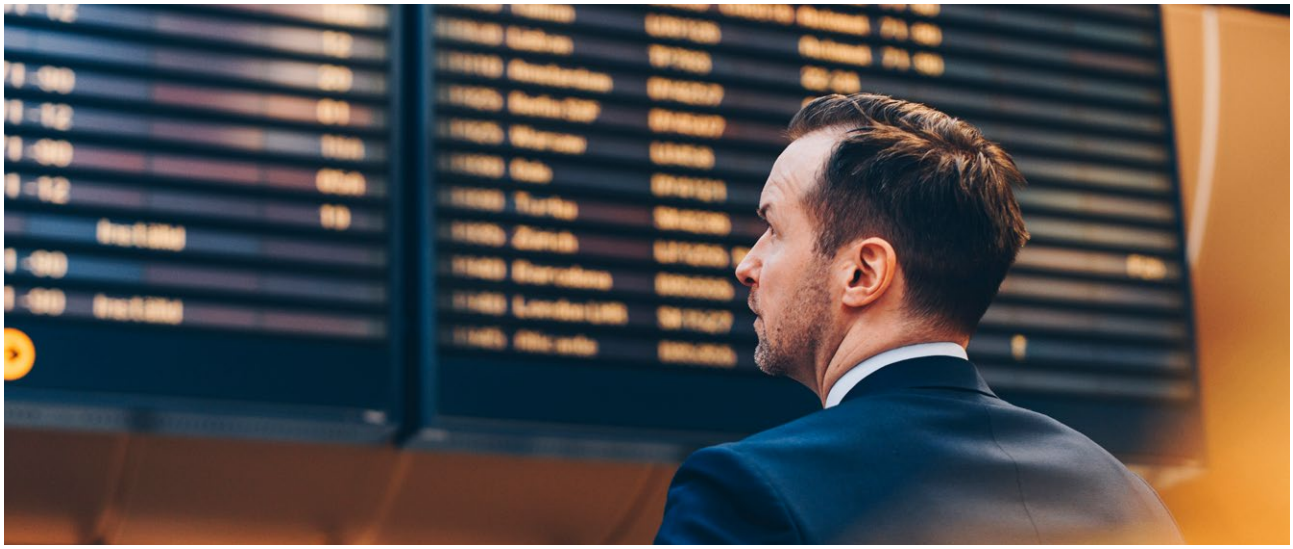
På sikt kan detta även innebära att kompetens och innovationer som är viktiga för Sverige inte längre finns kvar i landet. Företag som hamnar i en negativ ekonomisk belägenhet kan utgöra enkla och billiga mål för strategiska uppköp.

Kina utgör ett hot mot Sveriges ekonomiska säkerhet och har som mål att bli en global stormakt. Kina anskaffar svenska innovationer, tekniskt kunnande och spetskompetens från näringsliv och lärosäten, och svenska företag köps upp och strategiska investeringar i Sverige görs[115].

Under 2025 har det publicerats informativa rapporter[116] [117] om ryska intressen i Sverige. Dessa rapporter knyter i sin tur an till bland annat rapporter och memo tidigare publicerade av Totalförsvarets forskningsinstitut (FOI)[118] [119].

Detta material är värdefullt underlag för transportsektorns olika branscher i sitt kontinuerliga arbete med snabbt upptäckande av skiftande ägarförhållanden bland leverantörer och underentreprenörer, något som är särskilt viktigt för den som bedriver en verksamhet som bedöms samhällsviktig eller säkerhetskänslig. Ägarförhållanden kan behöva bevakas även i flera led bakom den direkta avtalsparten, i synnerhet om det handlar om internationella företag. Företagsutredning är ett resurskrävande arbete. Den sannolikt effektivaste metoden är att upparbeta en välfungerande samverkan och informationsdelning med centrala myndigheter som exempelvis Säkerhetspolisen, Finansinspektionen, Ekobrottsmyndigheten och inte minst Inspektionen för strategiska produkter som har uppdraget att utgöra granskningsmyndighet för utländska direktinvesteringar. Transportsektorsaktören kan bidra med finansiell underrättelseinformation, vilket resoneras kring i kapitlet Ekonomiskt försvar i boken Försvaret av Sverige[120].

I ljuset av detta är det också av yttersta vikt att förstå motståndarens långsiktighet i arbetet att uppnå sina mål. Denna målinriktade och mycket långsiktiga antagonistiska verksamhet beskrivs tydligt i boken Honungsfällan[121]. Långsiktigheten måste beaktas i all hot-, risk- och sårbarhetsbedömning som sker inom ramen för den egna verksamheten.



113 Årsrapportering 2023-2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

114 SFS 2023:560. Lag om granskning av utländska direktinvesteringar.

115 Årsrapportering 2023-2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.

116 Ryska intressen – En fördjupad studie av svenska bolag med rysk koppling. Rapport 2025:1. Acta Publica, 2025.

117 Fördjupad modusrapport – Systematisk penningtvätt inom den rysktalande organiserade brottsligheten. Finanspolissektionen, NOA. Polismyndigheten, 2024.

118 Totalförsvarets forskningsinstitut. Kinesiska bolagsförvärv i Sverige: en kartläggning, FOI MEMO 6903. Totalförsvarets forskningsinstitut, 2019.

119 Totalförsvarets forskningsinstitut. Ryska investeringar och ekonomiska intressen i Sverige. FOI-R-5377. Totalförsvarets forskningsinstitut, december 2022.

120 Försvaret av Sverige. Jonsson, 2024. ISBN 9789180025003. Mondial ,2024.

121 Honungsfällan. Berge & Gordh Humlesjö, 2024. ISBN 9789100185015. Albert Bonniers Förlag AB, 2024.

4.3 Desinformation och påverkanskampanjer

Ett exempel på påverkansoperationer är rapporteringen kring koranbränningarna under 2023 och hur rapporteringen kring dessa vinklades i olika informationskanaler och media. Koranbränningarna är verkliga händelser, men det spreds mycket falsk information kring dem. Exempelvis spreds det information om att det i Sverige skulle vara förbjudet att bränna den judiska skriften toran, som jämförelse[122]. Även falsk och misskrediterande information om polisens uppdrag och agerande vid dessa demonstrationer spreds. Varje myndighet eller företag kan komma att användas som fingerad avsändare av falsk information eller bli måltavla för falska uppgifter. Syftet med desinformationen är att skapa misstro och oro hos samhällets invånare.

Som motvikt till desinformation så har ett antal verifieringsmöjligheter etablerats, exempelvis SVT Verifierar[123]. Det finns både nationella och internationella möjligheter till faktaverifiering som användaren dock alltid har ett eget ansvar för vad gäller att kontrollera deras legitimitet. Ett sätt för detta kan vara att kontrollera om verifieringstjänsten till exempel lever upp till principerna från International Fact-Checking Network (IFCN)[124].

4.3.1 Från källkritik till källtillit

Upparbetade kommunikationskanaler och rutiner behöver säkerställas vid organisering av en verksamhets säkerhetsarbete. Detta behöver göras både inom och utanför den egna organisationen. En brist på anpassade kommunikationsfunktioner, exempelvis genom kryptering, kan leda till att nödvändig information inte delges med hänvisning till säkerheten. Då varje del av samhället kan nyttjas för att misskreditera förtroendet för samhället och demokratin innebär det att allmänhetens krav på staten vad gäller transparens, objektivitet och professionalism är av största betydelse. Myndigheten för psykologiskt försvar[125] arbetar kontinuerligt mot påverkanskampanjer och desinformation samt för att underlätta möjligheterna till källkritik.

Under lång tid har vikten av källkritik lyfts. Till detta behöver nu begreppet källtillit kopplas. Källtillit innebär att identifiera tillförlitliga och trovärdiga informationskällor som strävar efter att förhålla sig objektiva eller med andra ord att våga ha förtroende för pålitliga källor. Denna typ av källor kännetecknas exempelvis av att de prestigelöst använder sig av tydliga rättelser om en felaktig uppgift publicerats.

4.3.2 Författningshotande verksamhet från extremistmiljöer

Även om den svenska demokratin står stark behöver vi vara vaksamma på en utveckling med spridda antistatliga narrativ och konspirationsteorier som på sikt och i värsta fall kan utvecklas till författningshotande verksamhet och aktiviteter[126].

Så skriver Säkerhetspolisen i sin lägesbild för 2024–2025.

122 https://sverigesradio.se/artikel/al-jazeera-sprider-falska-nyheter-om-sverige (Kontrollerad 2025-07-25).

123 https://omoss.svt.se/arkiv/bloggarkiv/2024-09-29-darfor-lanserar-svt-verifieringshjalpen.html (Kontrollerad 2025-07-31).

124 https://ifcncodeofprinciples.poynter.org/ (Kontrollerad 2025-07-31).

125 https://mpf.se/ (Kontrollerad 2025-07-31).

126 Lägesbild 2024–2025. ISBN: 9789186661274. Säkerhetspolisen, 2025.

Gråzonens komplexitet ger vid handen att mycket av den verksamhet som bedrivs inom transportsektorn kan utgöra mål för verksamhet som ligger någonstans på gränsen mellan terrorism och övrig brottslighet. Syftet kan vara att störa eller förstöra verksamhet samt påverka personal i beslutande position. Den slutsatsen kan dras baserat på vetskapen om att exempelvis gränsen mellan våldsbejakande högerextremism och ickevåldsbejakande högerextremism blir alltmer diffus. Dessutom bedöms samtliga tre våldsbejakande extremistmiljöer som Säkerhetspolisen följer bedriva författningshotande verksamhet.

Nationellt centrum för terrorhotbedömning skriver följande i sin helårsbedömning 2025:[127]

> **Samtidigt som internationella våldsbejakande islamistiska organisationer stärkt sin avsikt att begå terrorattentat i Sverige har olika typer av författningshot utkristalliserats de senaste åren. Etablerade våldsbejakande islamistiska aktörer i Sverige tenderar att röra sig från våldsbejakande till författningshotande aktiviteter. Detta exempelvis genom att närma sig demokratiska plattformar för att bedriva långsiktig påverkan med legala medel och att använda exempelvis politiska partier, skolverksamhet, civilsamhället, föreningsliv och trossamfund som utgångspunkt för radikala men inte explicit och öppet våldsbejakande budskap. Även internationellt syns exempel på att våldsbejakande islamistiska organisationer och terrororganisationer politiserats och försökt att förändra de samhällen de verkar i genom alternativa strategier inom ramen för demokratiska processer.**

Detta belyser i någon mån komplexiteten i problematiken. En sammanfattning av detta kan vara att antagonisten försöker påverka samhället till en ickedemokratisk ordning genom att använda demokratiska metoder. Under 2024 har både våldsbejakande högerextremister och våldsbejakande islamister fortsatt sprida desinformation, konspirationsteorier och antistatliga narrativ[128].

4.4 Otillbörlig påverkan, otillåten påverkan och självcensur

Otillbörlig påverkan kan ses som ett verktyg som exempelvis organiserad brottslighet använder för att få ekonomisk vinning, inflytande och makt eller för att påverka rättsprocessen eller beslutsfattare. Denna påverkan tar sig uttryck i exempelvis obehagliga telefonsamtal, okvädningsord eller oönskade kontaktförsök utanför kontorstid. Otillbörlig påverkan övergår till otillåten påverkan då den genomförs med metoder som i sig utgör brott, såsom hot eller ofredande[129].

Vetskapen om den här typen av påverkan kan leda till självcensur, det vill säga att en person agerar annorlunda i tjänsten än vad den vanligen skulle ha gjort, av rädsla för att drabbas av otillåten påverkan. Självcensur påverkar rättssäkerheten och skadar tilltron till främst myndigheter. Självcensur kan till exempel innebära att personen fattar ett positivt beslut utan att göra en granskning, fattar ett negativt beslut trots att granskning talar för det motsatta, eller låter bli att göra de kontroller som myndigheten ansvarar för när det rör personer med kopplingar till grov organiserad brottslighet.

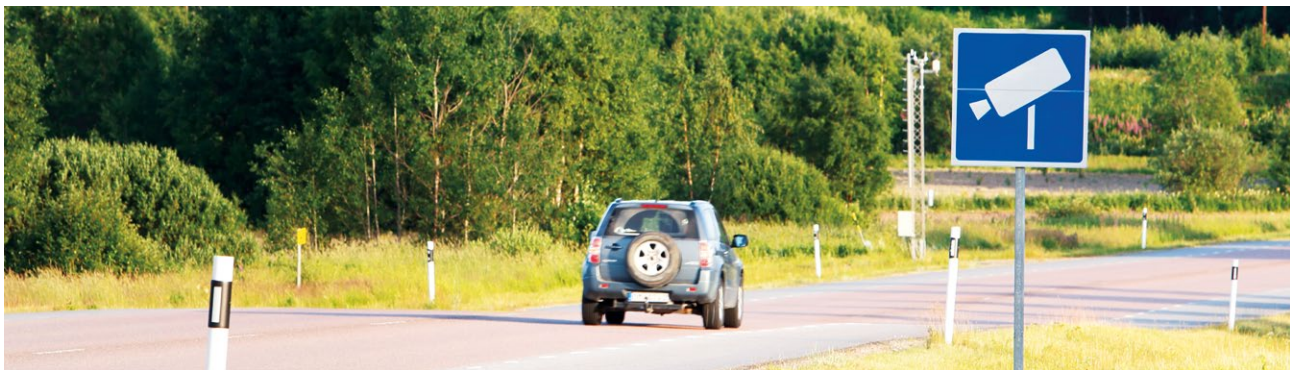
Självcensur är ett sätt att undvika att bli föremål för andras misstycke eller att utsättas för kritik. Det innebär att tjänstemannen handlar enligt sin upplevelse av den kriminella aktörens vilja utan att den kriminella aktören har agerat. Effekten av självcensur hos en myndighetshandläggare är densamma som av otillåten påverkan. Vikten av stöd från arbetsgivaren till den enskilde arbetstagaren med att hantera denna typ av situationer kan inte nog understrykas. Säkerhetskulturen kan enbart byggas med ett föredömligt ledarskap som grund.

Ur detta perspektiv behöver varje organisation vara uppmärksam på trender i sin verksamhetsuppföljning som kan tyda på exempelvis systematisk otillbörlig påverkan. Genom öppen informationsdelning i de forum som transportsektorn erbjuder för sina aktörer kan denna helhetsbild lättare skapas. Större sammanhang som kan behöva analyseras och bemötas under ett sektorsansvar kan då lättare tydliggöras. Detta kan liknas vid när incidentrapportering av till synes enklare incidenter vid en djupare analys kan få bäring på säkerhetsskydd och Sveriges säkerhet.

127 Helårsbedömning 2024 – sammanfattning. Nationellt centrum för terrorhotbedömning, 2024.

128 Helårsbedömning 2025. Nationellt centrum för terrorhotbedömning, 2025.

129 Otillåten påverkan från kriminella och extremistiska grupperingar Påverkansförsök mot förtroendevalda och kommunal förvaltning. Rapport 2025:4. Brottsförebyggande rådet, 2025.



4.5 Cyberangrepp och cyberbrottslighet

Antalet inrapporterade cyberangreppsförsök har minskat över tid, men det ökade igen under 2023. Ökningen består av ett onormalt stort antal överbelastningsangrepp under inledningen av 2023[130]. Under 2024 har rapporterats att uppgången nu omfattar 36 000 skanningar per sekund[131] [132].

Nationellt cybersäkerhetscenter publicerar exempel från verkligheten i sin rapport Cybersäkerhet i Sverige 2024. Dessa kan, utöver de exempel som ges nedan, ge mycket värdefulla insikter och förslag på åtgärder i egen verksamhet för att motstå angrepp inom cyberdomänen[133].

DDoS-attackerna under 2023 kom bland annat som attacker från så kallade hacktivister där det är ett ideologiskt perspektiv som är det bakomliggande motivet. Enligt uppgifter[134] utsätts Sverige sedan en tid för näst flest attacker i världen. Även andelen krypterade DDoS-attacker (distributed denial of service) ökade markant[135] under 2023, vilket pekar på att Sverige som nation anses vara ett prioriterat mål. DDoS-attacker är inte ett sofistikerat hot utan kan utföras med enkla medel och även köpas som tjänst av kriminella grupperingar.

Under början på sommaren 2024 riktades DDoS-attacker mot svenska myndigheter, bland annat Trafikverket och Transportstyrelsen. Motivet som uppgavs av den aktivistgrupp som tog på sig ansvaret för detta var det svenska beslutet om militärt stöd till Ukraina bland annat radarspaningsflygplan. Attacker kan alltså riktas mot svenska intressen oaktat att dessa inte har direkt koppling till det motiv som antagonisten uppger.

Komplex cyberbrottslighet utgörs främst av olika former av dataintrång. Av de mer komplexa brotten är utpressningsvirus (ransomware) ett vanligt tillvägagångssätt. I internationell rapportering förekommer uppgifter om att digitala utpressnings-attacker dessutom har kombinerats med hot om våld mot personal eller deras anhöriga. Utvecklingen visar åter på behovet av domänöverskridande säkerhetsåtgärder och säkerhetsprocesser där, som i detta fall, cybersäkerhetssidan hos en verksamhet behöver arbeta tätt tillsammans med den del av organisationen som ansvarar för medarbetarskydd och personalens säkerhet[136].

En ännu mer cynisk utveckling av hot är att utpressaren hotar med att anmäla verksamhetsutövaren till tillsynsmyndigheter för att denne i samband med cyberattacken, på ett eller annat sätt, har brustit i sina åtaganden inom cybersäkerhetsområdet. Detta ställer krav på att det finns en medvetenhet hos både tillsynsorgan och verksamhetsutövare om att hotet om legala sanktioner i sig kan leda till att exempelvis informationssäkerhetsincidenter inte lyfts fram, vilket kan leda till att skadan på samhället blir större. I en undersökning av fall där utpressningsvirus har använts beskrivs att illasinnade aktörer hittar nya sätt att tvinga offren att agera. Antagonisterna använde i 47 procent av fallen hot om att lämna in anmälningar till tillsynsmyndigheter och i 40 procent av fallen använde de fysiska hot mot personal[137].

Överbelastningsattacker är ytterligare en typ av dataintrång som kan vara allt från enkla till mycket avancerade i sitt genomförande och få stora konsekvenser för den verksamhet som drabbas. Sådana attacker används sällan för ekonomisk vinning utan av ideologiska, politiska eller andra antagonistiska skäl. Komplex cyberbrottslighet avser brott där digital information eller verktyg som hanterar digital information antingen är brottsverktyg eller mål för brottet. Brotten kan anses vara komplexa när de riktas mot samhällsviktig verksamhet, har internationell eller annan geografisk förgrening eller när de har ett organiserat brottsupplägg.

Under inledningen av 2024 inträffade ett angrepp mot it-leverantören TietoEvry vilket i förlängningen drabbade uppemot 120 myndigheter. Angreppet riktades inte direkt mot myndigheter, men det träffade brett i och med att många myndigheter använder samma system för personaladministration. Ett annat exempel är attacken mot det danska rederiet A.P. Moller-Maersk under 2017, där verksamheten för ett av världens största rederier slogs ut under 10 dagar.

130 Cyberangrepp mot samhällsviktiga informationssystem – 25 rekommendationer för stärkt skydd mot cyberangrepp. ISBN: 978-91-7927-459-7. Myndigheten för samhällsskydd och beredskap, 2024.

131 https://www.aktuellsakerhet.se/cyberbrott-okar-kraftigt-36-000-skanningar-i-sekunden-under-2024/ (Kontrollerad 2025-07-31).

132 Global Threat Landscape Report 2025. FortiGuard Labs, 2025.

133 Cybersäkerhet i Sverige 2024. Nationellt Cybersäkerhetscenter, 2025.

134 https://www.dagensinfrastruktur.se/2023/05/17/sverige-utsatts-for-nast-flest-hacktivist-attacker-i-varlden/ (Kontrollerad 2025-07-25).

135 https://www.aktuellsakerhet.se/undersokning-stor-okning-av-krypterade-ddos-attacker-mot-sverige-under-senaste-aret/ (Kontrollerad 2025-07-25).

136 https://www.theregister.com/2025/07/31/ransomware_physical_harm_threats/ (Kontrollerad 2025-08-29).

137 Ransomware risk report 2025. Semperis, 2025.

Båda dessa händelser är exempel som belyser hur stora konsekvenserna av ett enskilt cyberangrepp kan bli. Aktörerna inom transportsektorn behöver därför reflektera över vilka systemberoenden som de är en del av och som kan ha byggts in i det samhällsviktiga transportflödet.

4.5.1 Kunskap om sektorsaktörers rutiner, kontroller och svagheter

De antagonistiska aktörerna använder kunskap om transportsektorns aktörers verksamheter för att identifiera framgångsrika brottsupplägg. De använder också olika typer av associationsformer och it-lösningar för att dölja sin involvering i den brottsliga verksamheten. De antagonistiska aktörerna kan beskrivas som skickliga omvärldsbevakare i den bemärkelsen att de är snabba på att upptäcka nya affärs- eller brottsmöjligheter, ofta genom att identifiera svagheter i lagstiftning och utnyttja myndigheternas kontrollrutiner. De använder dessutom myndigheters servicevillighet för att utveckla brottsuppläggen. Genom mer avancerade upplägg och användande av att manipulera personers mänskliga beteenden (på engelska *social engineering*) kan vägar för infiltration öppnas som ger tillgång till myndigheters och företags känsliga information. Detta kan sedan nyttjas i framtida brottsupplägg, ekonomisk brottslighet eller otillåten påverkan.

Kriminella aktörer använder äkta, falska eller manipulerade identiteter och intyg som brottsverktyg. Användandet av artificiell intelligens är en trend som eskalerat kraftigt i takt med att den tekniken utvecklas. Det är en utmaning att se igenom denna typ av upplägg. En möjlig motåtgärd att införa i den egna verksamheten är ett korrekt taktiskt operativt uppträdande, vilket exempelvis kan innebära användandet av överenskomna kodord eller överenskommet uppträdande vid videosamtal i syfte att säkerställa att det verkligen är rätt person som deltar i samtalet. Detta försvåras om bedragaren på andra sidan har god kännedom om företagets eller myndighetens rutiner och arbetssätt och därmed kan uppträda på ett än mer övertygande sätt.

4.5.2 Internetrelaterad brottslighet

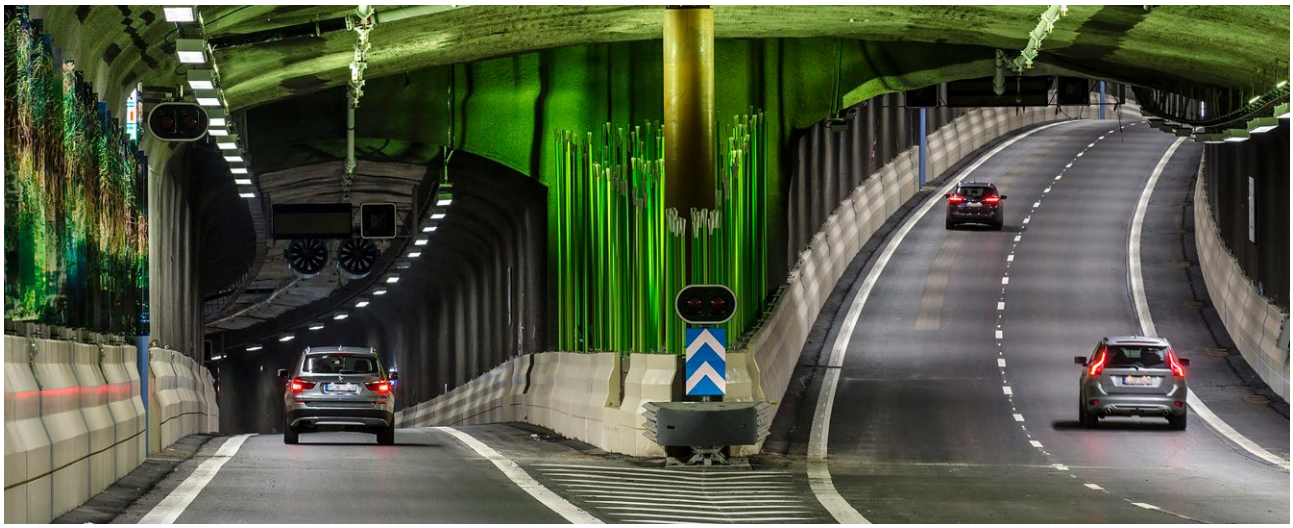
Cyberangrepp från hotaktörer och kriminella nätverk belyses särskilt i rapporten Cybersäkerhet i Sverige[138]. Där beskrivs hur cyberangreppen har förändrats över tid:

> **Spridningen av utpressningstrojaner har skiftat från att riktas brett och urskillningslöst, till att istället riktas mot specifika företag. Förhoppningen är att gå från flera små, till färre och istället större betalningar. Denna strategiska skiftning har varit framgångsrik vilket bekräftas av den rapportering som finns i öppna källor, exempelvis diverse säkerhetsföretags årliga rapportering.**

Sveriges nationella cybersäkerhetscenter rapporterar att det finns ett större mörkertal kring de cyberrelaterade brott som skedde under pandemin. På Europanivå identifierades en uppgång i denna typ av brott. Cyberkriminaliteten riktar sig mot såväl enskilda individer som privata och offentliga verksamheter.

Cybersäkerheten påverkas av ett antal sårbarheter som kan ha olika ursprung och manifestera sig inom ett antal områden. EU strävar efter att stärka motståndskraften och har till stöd infört nya samt stärkt befintliga regleringar. NIS 2-direktivet innebär t.ex. skärpta krav på berörda aktörer jämfört med NIS-direktivet och omfattar betydligt fler aktörer[139].

Transportsektorns aktörer behöver således, mot bakgrund i en möjlig roll i dessa direktiv, beakta antagonisters drivkraft, tillvägagångssätt och val av mål. Trenden, baserat på inträffade händelser, visar att hotaktörer har en tendens att använda de verktyg som fungerar för stunden och att antagonisten väljer att förfina existerande metoder snarare än att använda nya och avancerade metoder[140]. Det blir därigenom allt svårare för användare att upptäcka förfalskningar och bedrägerier.



138 Cybersäkerhet i Sverige 2022 Del 1: Hot, metoder, brister och beroenden. Nationellt Cybersäkerhetscenter, 2022.

139 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag. Regeringens proposition 2025/26:28. Regeringskansliet, 2025.

140 Cybersäkerhet i Sverige 2022 Del 1: Hot, metoder, brister och beroenden. Nationellt Cybersäkerhetscenter, 2022.

4.5.3 Klimataktivism

En av vår tids största utmaningar och samhällsfrågor är den pågående globala klimatkrisen. Ett flertal IPCC-rapporter menar på att utvecklingen går åt fel håll och att klimatrelaterade utmaningar nu och i framtiden kommer att påverka stora delar av jordens befolkning. I framför allt västvärlden har dessa rön och den här utvecklingen resulterat i skapandet av klimataktivistgrupperingar med olika syften och mål.

En gemensam nämnare för flera av dessa är tillvägagångssättet med civil olydnad genom olaga intrång, skadegörelse eller blockering av trafik. Ofta är dessa manifestationer eller demonstrationer av fredlig karaktär, men det är likväl lagbrott och skapar stor påverkan på eller leder till ökat resursbehov för rättsvårdande myndigheter och transportsektorns aktörer.

Transportsektorn har påverkats när aktioner riktade mot flaskhalsar i vägtrafiknätet har genomförts. Aktioner kan skapa en kedja av störningar inom transportsektorn som direkt eller indirekt kan orsaka skada eller andra konsekvenser för flera av sektorns aktörer. Den mediala rapporteringen har visat att opinionen kanske inte fullt har fallit ut i den riktning som aktivisterna har avsett med blockering av motorvägar. Under våren 2024 meddelade därför en organisation att denna typ av aktiviteter inte längre skulle genomföras.

Inga av dessa aktioner har i nuläget visat på ett aggressivt uppträdande. På lång sikt kan dock inte risken förbises att nya grupper med mer radikaliserade inslag eller våldsverkande element bildas, om en frustration eskalerar eller ett missnöje kring att makthavare inte upplevs ta till tillräckliga åtgärder för att motverka klimatförändringar. Dessa grupper kan också komma att utgöra mål för statsaktörers påverkan och infiltration.

Transportsektorns aktörer behöver vara medvetna om aktivistmiljön och den aktuella situationen kring den. Det kan underlätta för responsplanering och för utbildning av egen personal i händelse av att verksamheten störs av pågående aktion.

4.6 Sabotage och organiserade stölder

Transportsektorn är omfattande och mängden möjligheter som en sabotör har att tillgå är enorm. Det gör att det är svårt att helt motverka sabotage utfört av en kreativ antagonist. Det kan dessutom vara svårt att bekräfta att det rör sig om ett sabotage beroende på incidentens natur.

> **Making a faulty decision may be simply a matter of placing tools in one spot instead of another. A non-cooperative attitude may involve nothing more than creating an unpleasant situation among one's fellow workers, engaging in bickering's, or displaying surliness and stupidity**[141].

Organiserade omfattande stölder av till exempel metaller, drivmedel och byggnadsmaterial åsamkar såväl driftstörningar, utdragna processer och ökade kostnader samtidigt som de kan medföra ökade säkerhetsrisker för personal. Denna form av brottslighet betecknas som frekvent. Det kan inte uteslutas att en ökad efterfrågan kan skapas med koppling mot det pågående kriget i Ukraina.

Detta kan innebära ett förstärkande eller samverkande hot mot en verksamhet, det vill säga att tidigare förekommande hot kan eskaleras om verksamheten i någon mån är en del av exempelvis stödet till Ukraina. Om man därutöver hanterar material eller utrustning av stort ekonomiskt värde som används till att genomföra stödet så kan dessa faktorer sammanfalla. Det kan då vara av större intresse för organiserade kriminella att stjäla från organisationen om man utöver det stulna godset samtidigt kan få betalt av en statsaktör.

Problematiken för transportsektorns aktörer ligger mycket i att analysera inträffade incidenter även ur perspektivet av hur de kan vara sammanlänkade företeelser och alltså kan utgöra en helhetsbild där incidenterna hänger ihop.

Transportsektorns aktörer uppmanas samverka och dela information med varandra i syfte att tydliggöra hotbild och kunskap och för att bibehålla en hög säkerhetsnivå. Med fördel sker detta i de upparbetade samverkansforum mellan privata och offentliga aktörer som finns i dag. Beredskapsfrågor inom transportsektorn hanteras i dag inom Beredskapssektor Transporter Privat Offentlig Samverkan, BT-POS, under ledning av Trafikverket.

4.6.1 Förberedelser och märkliga incidenter

I detta kapitel, inom ramen för organiserade stölder, är det av värde att särskilt belysa den situation som kan uppstå om det som inledningsvis ser ut som en enkel stöld har en eller annan svårbegriplig komponent. Exempelvis i en situation där förberedelse för till exempel stöld av utrusning eller materiel tycks ha gjorts utan att något egentligen har stulits. I detta skede väcks frågan vad gärningspersonen har att vinna på att bara förbereda stölden vid det första besöket, för att sedan återvända till brottsplatsen vid ännu ett tillfälle och därmed fördubbla risken för upptäckt.

Mot bakgrund av det som tidigare beskrivits om gråzonen, hybrida metoder och statsaktörers modus och användande av kriminella kan en av många förklaringar vara att koordinera en insats. Det avbrott eller den olägenhet som angreppet innebär skulle kunna ha ett dubbelt syfte där den kriminelle får betalt för utförandet och samtidigt behåller det som stjäls samtidigt som avbrottet som sådant tjänar en statsaktörs syfte.

Det föreligger redan i dag rapporteringsskyldighet för vissa typer av händelser exempelvis genom säkerhetsskyddsförordningen (SFS 2021:955), men det vore olyckligt att fastna i en egenvald intellektuell begränsning utan att förstå att det kan finnas sammanhang i en större helhet. Säkerhetspolisen ger följande uppmaning i sin lägesbild 2024–2025[142]:

> **Utöver att anmäla säkerhetshotande händelser i enlighet med säkerhetsskyddsförordningen, uppmanas verksamhetsutövare att även rapportera andra typer av incidenter som inte berör säkerhetskänslig verksamhet men som avviker från normalbilden till Säkerhetspolisen.**

Det är därför ytterst viktigt att uppmärksamma och rapportera denna typ av händelser så att en samlad lägesbild kan tas fram på rätt strategisk nivå inom den egna organisationen, inom sektorn eller inom landet, beroende på situationen.

141 Simple sabotage field manual-Strategic services field manual No. 3. Office of Strategic Services, 1944. Declassified by Central Intelligence Agency, 2008.

142 Lägesbild 2024–2025. ISBN: 9789186661274. Säkerhetspolisen, 2025.

5 Litteratur och referenser

Följande källor ligger i olika hög grad till grund för detta dokument.
Referenslistan kan även ses som en fördjupande litteraturhänvisning:

- Acta Publica. Ryska intressen – En fördjupad studie av svenska bolag med rysk koppling. Rapport 2025:1. Acta Publica, 2025.
- Brottsförebyggande rådet. Otillåten påverkan från kriminella och extremistiska grupperingar Påverkansförsök mot förtroendevalda och kommunal förvaltning. Rapport 2025:4. Brottsförebyggande rådet, 2025.
- Brottsförebyggande rådet. Möjliggörare för kriminella nätverk – Om möjliggörare i kommunal, statlig och privat sektor. Rapport 2024:2. Brottsförebyggande rådet, 2024.
- Carnegie Mellon University. DensePose From WiFi. Geng J, Huang D, och F. De la Torre. Carnegie Mellon University, 2025.
- Center mot våldsbejakande extremism. PM Januari 2021. Våldsbejakande högerextrem accelerationism. Center mot våldsbejakande extremism, 2021.
- Ds 2023:19. Allvarstid. Försvarsberedningens säkerhetspolitiska rapport 2023.
- Europaparlamentet. Ghiretti, F, Gökten, M, Gunter, J, Pindyuk, O, Sebastian, G, Tonchev, P, Zavarská, Z, 2023, Research for TRAN Committee – Chinese Investments in European Maritime Infrastructure, European Parliament, Policy Department for Structural and Cohesion Policies, Brussels. Europaparlamentet, 2023.
- Europol. European SOCTA 2021 – Serious and organised crime threat assessment. ISBN 978-92-95220-23-2. Europol, 2021.
- European Union Agency for Law Enforcement Cooperation. European union terrorism situation and trend report 2023. ISBN 978-92-95220-91-1. European Union Agency for Law Enforcement Cooperation, 2023
- Forsvarets Efterretningstjeneste. Opdateret vurdering af truslen fra Rusland mod Rigsfællesskab. Forsvarets Efterretningstjeneste, 2025.
- Försvaret av Sverige. Jonsson, 2024. ISBN 9789180025003. Mondial ,2024.
- Försvarets radioanstalt. FRA årsrapport 2022: Året då kriget kom till Europa. Försvarets radioanstalt, 2023.
- Försvarets radioanstalt. FRA årsrapport 2023: Fler hot och större osäkerhet. Försvarets radioanstalt, 2024.
- Försvarsmakten. MUST årsöversikt 2024. Försvarsmakten, 2025.
- Försvarsmakten. MUST årsöversikt 2023. Försvarsmakten, 2024.
- Försvarsmakten. MUST årsöversikt 2022. Försvarsmakten, 2023.
- Försvarsmakten och Myndigheten för samhällsskydd och beredskap. Utgångspunkter för totalförsvaret 2025–2030. Försvarsmakten och Myndigheten för samhällsskydd och beredskap, 2025.
- Försvarsmakten. Skyddsvärden för försvaret av Sverige – Att identifiera säkerhetskänslig verksamhet. Militära underrättelse- och säkerhetstjänsten, MUST. Försvarsmakten, 2025.
- Försvarsmakten. Överbefälhavarens militära råd – Svensk försvarsförmåga inom ramen för Natos kollektiva försvar. FM2023-23092:14. Försvarsmakten, 2023.
- Global Threat Landscape Report 2025. FortiGuard Labs, 2025.
- Göteborgs tingsrätt. Mål B 18567-20.
- Honungsfällan. Berge & Gordh Humlesjö, 2024. ISBN 9789100185015. Albert Bonniers Förlag AB, 2024.
- Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Översikt och terminologi. ISO/IEC 27000:2018. SS-EN ISO/IEC 27000:2020.
- Eurasia Daily Monitor. Ukraine's Cyber Powerhouse: How the Military Security Service (HUR) Turned Traffic Cameras into a Battlefield Advantage. Jamestown Foundation. Eurasia Daily Monitor, vol. 20, nr 3, 10 januari 2023.
- Myndigheten för psykologiskt försvar. Årsredovisning 2023. MPF2024:90. Myndigheten för psykologiskt försvar, 2024.
- Myndigheten för samhällsskydd och beredskap. Cyberangrepp mot samhällsviktiga informationssystem – 25 rekommendationer för stärkt skydd mot cyberangrepp. ISBN: 978-91-7927-459-7. Myndigheten för samhällsskydd och beredskap, 2024
- Myndigheten för samhällsskydd och beredskap. Erfarenheter från Ukraina – Initiala lärdomar för det civila försvaret – Delredovisning av regeringsuppdrag Fö2023/01325. ISBN: 978-91-7927-438-2. Myndigheten för samhällsskydd och beredskap, 2023.
- Myndigheten för samhällsskydd och beredskap. Cyberangrepp mot samhällsviktiga informationssystem – 25 rekommendationer för stärkt skydd mot cyberangrepp. ISBN: 978-91-7927-459-7. Myndigheten för samhällsskydd och beredskap, 2024
- Myndigheten för samhällsskydd och beredskap. EU förändrar cybersäkerhetsområdet Årsrapport it-incidentrapportering 2023. ISBN: 978-91-7927-494-8. Myndigheten för samhällsskydd och beredskap, 2024.
- Myndigheten för samhällsskydd och beredskap. Om krisen eller kriget kommer. ISBN: 978-91-7927-527-3. Myndigheten för samhällsskydd och beredskap, 2024.
- Nationellt Cybersäkerhetscenter. Cybersäkerhet i Sverige 2024. Nationellt Cybersäkerhetscenter, 2025.
- Nationellt Cybersäkerhetscenter. Cybersäkerhet i Sverige 2022 Del 1: Hot, metoder, brister och beroenden. Nationellt Cybersäkerhetscenter, 2022.
- Nationellt Cybersäkerhetscenter. Cybersäkerhet i Sverige 2022 Del 2: Rekommenderade säkerhetsåtgärder. Nationellt Cybersäkerhetscenter, 2022.
- Nationellt centrum för terrorhotbedömning. Helårsbedömning 2025. Nationellt centrum för terrorhotbedömning, 2025.
- Nationellt centrum för terrorhotbedömning. Våldsbejakande misantropi. Nationellt centrum för terrorhotbedömning, 2025.
- Nationellt centrum för terrorhotbedömning. Helårsbedömning 2024 Sammanfattning. Nationellt centrum för terrorhotbedömning, 2024.
- Nationellt centrum för terrorhotbedömning. Helårsbedömning 2022. Nationellt centrum för terrorhotbedömning, 2022.
- Polismyndigheten. Fördjupad modusrapport – Systematisk penningtvätt inom den rysktalande organiserade brottsligheten. Finanspolissektionen, NOA. Polismyndigheten, 2024.
- Polismyndigheten. Professionella penningtvättare – Branscher, modus och kopplingar till kriminella nätverk. Finanspolissektionen, NOA. Polismyndigheten, 2024.

- Polismyndigheten. Korruption i Sverige – En lägesbild. Årsrapport från Nationella Antikorruptionsgruppen. Polismyndigheten, 2024.
- Polismyndigheten. Myndigheter i samverkan mot den organiserade brottsligheten 2024. Polismyndigheten, 2025.
- Polismyndigheten. Myndighetsgemensam lägesbild om organiserad brottslighet 2025. Polismyndigheten, 2025.
- Polismyndigheten. Myndighetsgemensam lägesbild om organiserad brottslighet 2023. Polismyndigheten, 2023.
- Polismyndigheten. Myndighetsgemensam lägesbild om organiserad brottslighet 2021. Polismyndigheten, 2021.
- Office of Strategic Services. Simple sabotage field manual – Strategic services field manual No. 3. Office of Strategic Services, 1944. Declassified by Central Intelligence Agency, 2008.
- Regeringskansliet. Gemensamt meddelande om EU:s rymdstrategi för säkerhet och försvar. Faktapromemoria 2022/23:FPM67. Regeringskansliet, 2023.
- Regeringskansliet. På upplyst grund – en ESO-rapport om myndigheternas remissarbete. Expertgruppen för studier i offentlig ekonomi 2024:5. Berglöf, E., Settergren, O & Sundström, G. Regeringskansliet, 2024.
- Regeringskansliet. Försvaret av Sverige – Starkare försvar för en osäker tid, DS 2014:20. ISBN 978-91-38-24119-6. Regeringskansliet, 2014.
- Regeringskansliet. Motståndskraft och handlingskraft – en nationell strategi mot organiserad brottslighet, Skr: 2023/24:67. Regeringskansliet, 2024.
- Regeringskansliet. Nationell säkerhetsstrategi. Skr: 2023/24:163. Regeringskansliet, 2024.
- Regeringskansliet. Nya regler om cybersäkerhet, SOU 2024:18. Delbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven. ISBN 978-91-525-0879-4. Regeringskansliet, 2024.
- Regeringskansliet. Rymdens roll i ett nytt säkerhetspolitiskt läge – Sveriges försvars- och säkerhetsstrategi för rymden. Regeringskansliet, 2024.
- Regeringskansliet. Stärkt försvarsförmåga – Sverige som allierad, DS 2024:6. ISBN 978-91-525-0917-3. Regeringskansliet, 2024.
- Regeringskansliet. Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag. Regeringens proposition 2025/26:28. Regeringskansliet, 2025
- Regeringskansliet. Sveriges strategi för den arktiska regionen. Regeringskansliet, 2020.
- Semperis. Ransomware risk report 2025. Semperis, 2025.
- SFS 2023:560. Lag om granskning av utländska direktinvesteringar.
- SFS 2022:524. Förordning om statliga myndigheters beredskap.
- Snällast vinner. Hansson, 2024. ISBN 9789189740662. The Book Affair, 2024.
- Statskontoret. SOU 2021:25. Struktur för ökad motståndskraft. Statskontoret.
- Statskontoret. Den statliga värdegrunden – gemensamma principer för en god förvaltning. ISBN 978-91-88865-23-6. Statskontoret, 2019.
- Sveriges radio. Gräns, avsnitt 144. Sveriges Radio, 2025.
- Säkerhetspolisen. Personlig säkerhet, fjärde upplagan. ISBN: 9789186661212. Säkerhetspolisen, 2021.
- Säkerhetspolisen. Lägesbild 2024–2025. ISBN: 9789186661274. Säkerhetspolisen, 2025.
- Säkerhetspolisen. Årsrapportering 2023–2024. ISBN: 9789186661250. Säkerhetspolisen, 2024.
- Säkerhetspolisen. Årsrapportering 2022–2023. ISBN: 9789186661236. Säkerhetspolisen, 2023.
- Säkerhetsskyddsanalys i teori och praktik. Söderlund & von Zeipel, 2024. ISBN 9789139027058. Norstedts Juridik, 2024.
- Södertörns tingsrätt. Brottsmål B 2595-24. Stämningsansökan – Ärende AM-137440-24/Handling 123. Södertörns tingsrätt, 2024.
- TCO. Tyst förvaltning – Tjänsteman i offentlig förvaltning – om roller, reformer och konsekvenser för demokratin. TCO, 2025.
- Totalförsvarets forskningsinstitut. Attacking and Deceiving Military AI Systems, FOI-R--5396—SE. Totalförsvarets forskningsinstitut, mars 2023.
- Totalförsvarets forskningsinstitut. Gråzonsproblematik och hybrida hot i transportsystemet. FOI-R-5118. Totalförsvarets forskningsinstitut, 2021.
- Totalförsvarets forskningsinstitut. Gråzonsläge i krig och fred. FOI-R-5447. Totalförsvarets forskningsinstitut, juni 2023.
- Totalförsvarets forskningsinstitut. Kinesiska bolagsförvärv i Sverige: en kartläggning, FOI MEMO 6903. Totalförsvarets forskningsinstitut, 2019.
- Totalförsvarets forskningsinstitut. Typfall 5: Utdragen och eskalerande gråzonsproblematik, FOI MEMO 6338. Totalförsvarets forskningsinstitut, 2018.
- Totalförsvarets forskningsinstitut. Ryska investeringar och ekonomiska intressen i Sverige. FOI-R-5377. Totalförsvarets forskningsinstitut, december 2022.

Trafikverket, Box 810, 781 28 Borlänge. Besöksadress: Rödavägen 1
Telefon: 0771-921 921, Texttelefon: 010-123 50 00
trafikverket.se