Gråzonsproblematik och hybrida hot i transportsystemet

Ester Veibäck, Ann-Sofie Stenérus Dover,
Anna McWilliams

FOI-R--5118--SE

Mars 2021

FOI

Ester Veibäck, Ann-Sofie Stenérus Dover,
Anna McWilliams

Gråzonsproblematik och hybrida hot i transportsystemet

Titel	Gråzonsproblematik och hybrida hot i transportsystemet
Rapportnr	FOI-R--5118--SE
Månad	Mars
Utgivningsår	2021
Antal sidor/Pages	50
ISSN	1650-1942
Kund	Trafikverket
Forskningsområde	Krisberedskap och civilt försvar
FoT-område	Inget FoT-område
Projektnr	E13701
Godkänd av	Malek Finn Khan
Ansvarig avdelning	Försvarsanalys

Bild/Cover: Anna McWilliams

Sammanfattning

Genom den återupptagna planeringen för totalförsvaret har ökat fokus lagts på gråzonsproblematik och hybrida hot. En antagonistisk strategi att påverka eller skapa oro utan att eskalera till konflikt är inte något nytt. Men i ett samhälle som kännetecknas av öppenhet, tvärsektoriella beroenden och digitaliserade arbetssätt har nya tillämpningar och ökade sårbarheter uppkommit. Oavsett om Sverige i juridisk mening befinner sig i krig eller fred så behöver vi kunna möta den typen av hot. De sårbarheter och hot som diskuteras i rapporten är:

- 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

Avslutningsvis konstateras att ett väl fungerande civilt samhälle står för en betydande del av den tröskeleffekt som kan ha en avskräckande effekt på en antagonist. Transporter är en viktig del vårt samhälle, och av avgörande betydelse när samhället utsätts för påfrestningar. Robusta försörjningssystem är en viktig grund och medvetandet om antagonistiska hot behöver höjas för ökad motståndskraft.

Nyckelord: civilt försvar, gråzon, gråzonsproblematik, sårbarhet, hotbild, hybrida hot, tröskel, förmåga, transport, tåg, flyg, fartyg, lastbil, trafik

Summary

In the recent plans for the Swedish total defence, there has been an increased focus on grey zone and hybrid threats. An antagonist's strategy to influence or cause unrest without creating an escalated reaction is not in itself something new. However, in a society based on openness, digitisation and dependencies between different societal functions, these threats make society all the more vulnerable. The vulnerabilities and threats that are discussed in this report cover the following areas:

- Market conditions set the playing field for companies as well as antagonists
- The transport system's openness and accessibility can be used by an antagonist
- Intrusion and interference could affect operations and systems
- Security risks occur during public tending and using goods and services
- Dependencies create vulnerabilities
- Challenges for the development of coherent defence readiness

Finally, this report concludes that a well-functioning society creates a threshold effect that deters a possible antagonist from acting. Transportation is a vital part of a functioning society, and is of crucial importance in a situation where we are faced with a threat. Having robust supply systems is an important base, in war as well as in peace. It is important to raise the awareness of antagonist threats in order to achieve resilience.

Keywords: civil defence, grey zone, vulnerability, threat, grey zone scenario, hybrid threat, threshold, defence capability, transport, train, aeroplanes, ships, trucks, traffic.

Förord

Föreliggande rapport redovisar en studie som har utförts på uppdrag av Trafikverket. Trafikverket driver ett utvecklingsarbete med utgångspunkt i myndighetens ansvar för att utveckla och samordna arbetet med krisberedskap och planering för höjd beredskap inom hela transportområdet. Kopplat till detta har Trafikverket lagt ett uppdrag på FOI att ta fram ett kunskapsunderlag avseende gråzonsproblematik och hybrida hot.

Under arbetets gång har coronapandemin utbrutit och påverkat hela samhället på flera sätt. Den har också påverkat hur arbetet inom detta projekt har kunnat bedrivas och begränsat möjligheten till datainhämtning. Trots dessa utmaningar har vi fortsatt arbetet med vissa förändringar i arbetssättet. Inom studien har information och synpunkter inhämtats såväl från företag i transportsystemet som från myndigheter via ett antal workshoppar och digitala möten. Vi vill tacka för all värdefull input. Eventuella felaktigheter som smugit sig in står författarna för.

Ester Veibäck, projektledare

Innehållsförteckning

1 Inledning

Det alltmer osäkra säkerhetspolitiska läget har under de senaste åren lett till en ökad instabilitet och oförutsägbarhet i omvärlden. Riksdagen beslutade 2015 om att återuppta planering för hela totalförsvaret (även den civila delen), efter att den hade varit vilande en tid. Beslutet innebär att aktörer inom krisberedskapen ska arbeta för att samhället ska höja sin förmåga att hantera ett väpnat angrepp mot Sverige och så kallad gråzonsproblematik. Den återupptagna planeringen för totalförsvaret har resulterat i ett förnyat arbete där ökat fokus har riktats mot det som brukar kallas hybrida hot och gråzonsproblematik. Innebörden av dessa begrepp kan dock tyckas oklar och beskrivs ibland svepande. Beskrivningar på en abstrakt och övergripande nivå är till föga hjälp för aktörer inom enskilda branscher och verksamheter. Istället behöver begreppen sättas i ett sammanhang och kopplas till mer specifika situationer.

Benämningen gråzonsproblematik används när ett samhälle i fredstid utsätts för påfrestningar såsom exempelvis statsinitierad antagonism, desinformationskampanjer, sabotage, cyberattacker och maktdemonstrationer, men under den tröskel som skulle leda till att en reaktion hos motparten eskalerar förloppet.[1] Gråzonsproblematik och bredden av de maktmedel och metoder som en stat eller aktör kan använda i gråzonen eller i en öppen konflikt, så kallade hybrida hot, kommer att fördjupas i denna rapport, orienterat till transportområdet.

FOI forskar om hybrida hot och gråzonsproblematik inom flera tillämpningsområden och sektorer, till exempel energiförsörjning, polisiär verksamhet, sjukvård och industriella informationssystem. Under 2018 publicerades rapporten ”Gråzonsproblematik och hybridkrigföring – påverkan på energiförsörjning”, vilken är en viktig utgångspunkt för denna studie. Föreliggande rapport, med fokus på transportområdet, bygger vidare på de erfarenheter och slutsatser som har dragits genom arbetet kopplat till energiområdet, liksom den bredd av kompetens som har byggts upp vid FOI inom andra studier.[2]

Forskning avseende hur transportsektorn påverkas av gråzonsproblematik har visat sig vara begränsad, vilket gör den här studien extra angelägen. Inte bara för transportsektorn i sig, utan också för den svenska totalförsvarsplaneringen generellt.

[1] Jonsson (2018) sid. 40

[2] Se till exempel Jonsson (2018), Stenérus Dover (2019), Lindahl m.fl. (2020), Appelgren m.fl. (2020), Svenonius m.fl. (2020)

1.1 Syfte

Syftet med denna studie är att beskriva en gråzonshotbild för transportsystemet för att konkretisera på vilket sätt den här typen av hot kan uppfattas och vilka konsekvenser de kan leda till, kopplat till transporter. Vilka hot, aktiviteter och sårbarheter är relevanta att uppmärksamma och vilka medel kan en antagonist förväntas använda? En konkretiserad hotbild kan användas som utgångspunkt i planeringen och i dialog mellan myndigheter och branschaktörer. Den kan också vara till stöd i vidareutvecklingen av en omvärldsbevakning som innefattar gråzon, samt utgöra underlag för planering av beredskapsåtgärder.

1.2 Genomförande

Genomförandet av denna studie bygger på metodik och teori från FOI-rapporten ”Gråzonsproblematik och hybridkrigföring – påverkan på energiförsörjning”.[3] Arbetet inleddes med en litteraturgenomgång avseende sårbarheter, hybrida hot och gråzonsverksamhet, med koppling till transportsystemet. Litteraturstudien gav en inledande övergripande bild, men tydliggjorde också att forskningen är relativt begränsad vad gäller perspektivet gråzonsproblematik kopplat till transportsektorn. Den forskning som bedrivits tidigare har ofta fokuserat på säkerhetsaspekter, exempelvis fraktsäkerhet och hamnsäkerhet, och har på så sätt snarare haft fokus på hur man skyddar varor i stället för hur man kan upprätthålla *funktionen* transport. Den har även fokuserat på enskilda komponenter i transportsystemet, som hamnar, flygplatser, containrar, snarare än det övergripande systemets funktion.[4] Forskningen och kunskapen avseende enskilda delar i hotbilden är relativt omfattande, exempelvis terrorism med koppling till transportmedel och olika cyberhot, men tunnare när det kommer till en sammansatt strategi.

För att beskriva en hotbild som känns angelägen och trovärdig bestämdes redan vid planeringen av projektet tillsammans med uppdragsgivaren att workshoppar med aktörer inom transportområdet skulle genomföras. Datainsamling genom fysiska möten har varit grundläggande. En workshop med privata aktörer inom transportområdet genomfördes i mars 2020. Mötet hölls i skyddade lokaler för att möjliggöra förtroendeskapande diskussioner och erforderlig fördjupning om detaljer som förknippas med sekretess. För att kunna använda den data som samlades in, trots att vissa delar bedömdes vara känsliga, användes ett arbetssätt som beskrivs kapitel 1.3 nedan. De exempel på hot som presenterades under workshopen kategoriserades därefter i sex analysdimensioner som fördjupades med stöd av tidigare forskning och erfarenheter från inträffade händelser.

[3] Jonsson (2018)
[4] Johansson m.fl. (2017)

Arbetet fortsatte genom en serie digitala möten[5] där analysdimensionerna och valda delar av materialet presenterades och diskuterades dels med företrädare från transportmyndigheterna Sjöfartsverket, Transportstyrelsen, Luftfartsverket och Trafikverket, dels med representanter från tre länsstyrelser. Under mötena med de centrala myndigheterna och länsstyrelserna diskuterades även arbetet med att utveckla totalförsvaret mot bakgrund av den uppmålade hotbilden, och viktiga reflektioner avseende detta presenteras i rapportens avslutande kapitel.

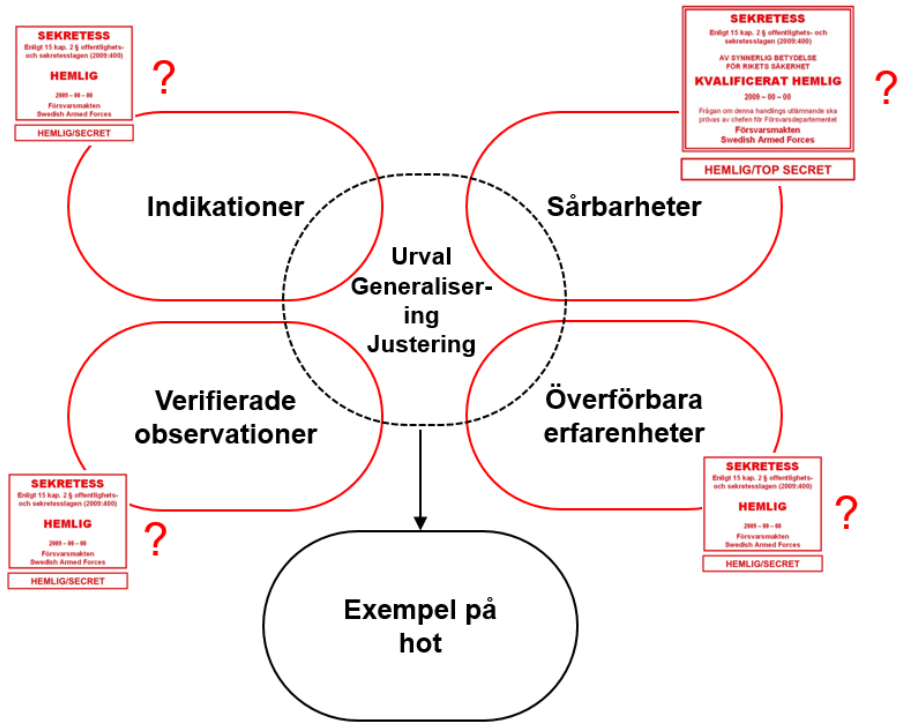
1.3 Om att hantera känsliga uppgifter

Målet med denna rapport är att ge en bild av hur hybrida hot och gråzonsverksamhet kan användas av en antagonist inom transportområdet, och eventuella konsekvenser av detta. För att uppnå detta på ett trovärdigt sätt har exempel på hot och sårbarheter som framkommit genom diskussionerna med branschföreträdare använts, liksom kända och i media uppmärksammade fall av påverkan inom transportområdet.

Det blir en balansgång mellan att ge tillräckligt konkreta resonemang för att hot och situationer ska kunna förstås, och att inte lämna ut detaljer som kan utnyttjas i fel sammanhang. I diskussionerna och datainsamlingen har vi utgått från följande kategorier av exempel:

- Indikationer: något har hänt, men det finns inte någon tydlig helhetsbild av huruvida händelsen är en medveten handling eller inte, eller vem som egentligen ligger bakom.
- Verifierade observationer: det finns en klar bild av vad som har hänt och vem antagonisten med hög sannolikhet är.
- Sårbarheter: kända och förmodade nuvarande eller framtida sårbarheter som skulle kunna exploateras av en antagonist.
- Överförbara erfarenheter: Tänkbara händelser eller analyser kopplat till verksamheter i andra sektorer eller i jämförbara system.

[5] Den ursprungliga planen innebar att genomföra en hel workshopserie i säkra lokaler, men den fick av uppenbara (corona-)skäl revideras när pandemin svepte in i Sverige under våren 2020, och ersattes med digitala möten.



Figur 1: Metod för urval av exempel på hot, med hänsyn tagen till sekretess.

Specifika detaljer om exempel inom respektive kategori kan vara förknippade med sekretess. Genom att göra urval bland de exempel som ges samt att generalisera och justera beskrivningar kan vi återge en helhetsbeskrivning som inte utelämnar känsliga detaljer. Till exempel tar vi inte upp händelser som drabbat specifika organisationer utan beskriver fenomen generellt. Analysen har sedan utgjorts av arbete med att ställa detta material mot fynd från litteraturen och att hitta relevanta analyskategorier som återspeglar innehållet.

1.4 Läsanvisningar

Första kapitlet ger en bakgrund till projektet, dess syfte och det valda arbetssättet. Andra kapitlet beskriver övergripande beredskapsarbetet inom transportområdet. I det tredje kapitlet ges en beskrivning av hybrida hot och gråzon generellt och kopplat till transportsystemet. I det fjärde kapitlet analyserar vi hur gråzonsproblematik, hybrida hot och sårbarheter kan ta sig uttryck inom transportsystemet. Det femte kapitlet diskuterar hantering av hot på ett övergripande plan och i det avslutande sjätte kapitlet dras övergripande slutsatser avseende utmaningar kopplat till gråzon och hybrida hot. Dessa slutsatser är också till stor del överförbara till andra områden.

2 Transportsystemet och utvecklingen av krisberedskap och civilt försvar

Transportsystemet utgör en central del av samhällets funktion. Transporter pekas ut av Myndigheten för samhällsskydd och beredskap (MSB) som en samhällssektor med samhällsviktig verksamhet.[6] Tillgänglighet och möjlighet att transportera både gods och människor är en viktig del i dagens samhälle, såväl i normalläge som i kriser och ansträngda situationer. Det är av avgörande betydelse att infrastrukturen och transportsystemets funktionalitet kan upprätthållas om samhället på något sätt hotas, oavsett om det gäller naturhändelser och olyckor eller om det är antagonistiska hot. I detta kapitel redogörs övergripande för ansvarsstrukturer inom transportsektorn och hur beredskapen är organiserad. Kapitlet avslutas med en historisk tillbakablick över hur den hotbild som har legat till grund för beredskapsplanering utvecklats de senaste hundra åren, för att sätta det arbete som görs idag i perspektiv.

2.1 Ansvar för beredskap inom transportsektorn

Myndigheterna inom transportsektorn har ansvar för olika delar i transportsystemets funktion och utveckling. Själva trafiken är i många fall i privat regi och företagen agerar på en konkurrensutsatt marknad. I sitt uppdrag ska Trafikverket anta ett trafikslagsövergripande perspektiv och ansvara för den långsiktiga infrastrukturplaneringen. Därutöver har Trafikverket i uppdrag att bygga och ansvara för driften av statliga vägar och järnvägar.[7] Sjöfartsverket följer upp hur sjöfarten utvecklas i förhållande till de transportpolitiska målen och utför uppgifter kopplat till sjöfarten, till exempel lotsning, sjöräddningstjänst och upprätthållande av farleder.[8] Luftfartsverket har i huvuduppgift att tillhandahålla flygtrafiktjänster (såsom flygtrafikledning) för civil och militär luftfart.[9] Transportstyrelsens huvuduppgift är att svara för regelgivning, tillståndsprövning och tillsyn inom hela transportområdet.[10] Luftfartsverket och Sjöfartsverket är statliga affärsverk, vilket innebär att verksamheten i stor utsträckning finansieras genom avgifter på verksamheter.

[6] MSB (2019) Vägledning för identifiering av samhällsviktig verksamhet
[7] SFS 2010:185. Förordning med instruktion för Trafikverket
[8] SFS 2007:1161. Förordning med instruktion för Sjöfartsverket
[9] SFS 2010:184. Förordning med instruktion för Luftfartsverket
[10] SFS 2008:1300. Förordning med instruktion för Transportstyrelsen

Trafikverket har sedan 2017 ett breddat uppdrag att vidta åtgärder i syfte att utveckla och samordna krisberedskapen och planeringen för höjd beredskap inom transportområdet. Det ska göras med utgångspunkt i ett trafikslagsövergripande perspektiv och i samverkan med andra aktörer.[11]

Alla fyra myndigheter är dock bevakningsansvariga myndigheter, vilket innebär att de har ett särskilt ansvar för krisberedskapen och för att vidta åtgärder inför och vid höjd beredskap. Det handlar dels om att planera för sin egen verksamhet och då beakta totalförsvarets krav, dels om att följa utvecklingen och kunna vidta åtgärder vid en kris, samt för Trafikverkets del att verka för att transportområdet som helhet utvecklar förmågor för detta. Alla statliga myndigheter ska verka för att minska sårbarheten i samhället och utveckla en förmåga att hantera sina uppgifter även under kriser och vid höjd beredskap.[12]

De fyra myndigheterna samverkar också med andra myndigheter med koppling till transporter inom Samverkansområde Transporter (SOTP) som drivs av MSB.[13] Därutöver leder Trafikverket projektet Transportsektorns samverkan inför samhällsstörningar (TP SAMS), som är ett samverkansforum för aktörerna inom transportsektorn. TP SAMS samlar ett 20-tal myndigheter och branschorganisationer inom transportsektorn för att förbättra samarbetet inför störningar med samhällspåverkan. Huvudsyftet med forumet är att stärka transportsektorns samlade förmåga att hantera samhällsstörningar genom utökad samverkan kring frågor som relaterar till krisberedskap och åtgärder inför och vid höjd beredskap.[14]

2.1.1 Fredstida krisberedskap

Krisberedskapsarbetet syftar till att stärka samhällets förmåga att förebygga och hantera kriser, olyckor och hot. Svenska myndigheters agerande under en samhällsstörning eller kris regleras av förordning (SFS 2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap, vilken ställer krav på svenska myndigheters agerande under samhällsstörning eller kris för att säkerställa förmågan till verksamhet, och att säkerställa samhällsviktiga funktioner även vid samhällsstörningar och stora påfrestningar.

[11] SFS 2010:185. Förordning med instruktion för Trafikverket
[12] SFS 2015:1052. Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap samt förordning (SFS 2015:1053) om totalförsvar och höjd beredskap
[13] Samverkansområde Transporter är ett av sex samverkansområden för myndigheterna inom krisberedskap och civilt försvar. Vilka dessa är framgår av bilaga till förordning (SFS 2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. I SOTP deltar Luftfartsverket, MSB, Sjöfartsverket, Energimyndigheten, Trafikverket och Transportstyrelsen.
[14] Trafikverkets websida om TP SAMS.

Det finns flera institutionella system för att förbereda och skydda mot olika typer av hot i fredstid. Säkerhetsskyddet syftar till att skydda säkerhetskänslig verksamhet och är uppdelat i tre områden: informationssäkerhet, fysisk säkerhet och personalsäkerhet.[15] Säkerhetsskyddet har stöd genom säkerhetsskyddslagen (SFS 2018:585) och säkerhetsskyddsförordningen (SFS 2018:658) med ytterligare förtydligande i Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2019:2) och MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6). Alla myndigheter måste utföra en säkerhetsskyddsanalys för att identifiera skyddsvärd information och annan skyddsvärd verksamhet samt vidta åtgärder för att skydda dessa.[16]

Genom risk- och sårbarhetsanalyser (RSA) ska varje myndighet arbeta för att minska sina sårbarheter och förbättra sin förmåga att förebygga, motstå och hantera samhällsstörningar och hot.[17] I RSA:erna utgår man från vad som är samhällsviktigt inom respektive verksamhetsområde, men det är svårt att ge en exakt definition av vad som är samhällsviktiga transporter. Det handlar både om transporter som är viktiga i sig, och om att upprätthålla flöden som är en förutsättning för andra samhällsviktiga tjänster, till exempel livsmedelsförsörjning eller sjukvård.[18]

Att ha en god förståelse för vilka hot samhället och dess aktörer står inför, samt hur dessa kan verkställas, är en viktig grund både för att bygga robusta system och för planeringen för krisberedskap och civilt försvar. Förståelse för hur hoten – om de realiseras – kan påverka den verksamhet som ska skyddas samt hur olika former av antagonism kan påverka samhället som helhet ger möjlighet till att stärka medvetenheten och motståndskraften. Genom att förbereda organisationer inför uppgiften att upptäcka, försvåra och hantera skadlig inverkan mot den egna verksamheten säkerställs robustheten mot olika typer av hot, även antagonistiska.

2.1.2 Totalförsvarsplaneringen

Utgångspunkten för totalförsvarsplaneringen är de så kallade försvarsbesluten som riksdagen fattar ungefär var femte år och som fastställer mål för försvarsområdet under de närmaste åren. I försvarsbeslutet 2020 fattades beslut om nytt mål för det civila försvaret (se textruta nedan). Transportsektorn har en avgörande betydelse för flera av delarna i målet, till exempel för att säkerställa de viktigaste samhällsfunktionerna, att upprätthålla nödvändig försörjning och att bidra till det militära försvarets förmåga vid väpnat angrepp. Transporters betydelse för samhällets funktionalitet såväl i fred som vid kris som vid krig

[15] Svenonius och Strindberg (2020) sid. 30
[16] SFS 2018:658 2. Kap. §1
[17] SFS 2015:1052. Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap
[18] Helmbring och Arvidsson (2015) sid. 8

betonas särskilt av Försvarsberedningen som också föreslår väsentliga satsningar på området för att ges möjlighet att utveckla sin förmåga.[19]

> Målet för det civila försvaret ska vara att ha förmåga att:
>
> – värna civilbefolkningen,
> – säkerställa de viktigaste samhällsfunktionerna,
> – upprätthålla en nödvändig försörjning,
> – bidra till det militära försvarets förmåga vid väpnat angrepp eller krig i vår omvärld,
> – upprätthålla samhällets motståndskraft mot externa påtryckningar och bidra till att stärka försvarsviljan,
> – bidra till att stärka samhällets förmåga att förebygga och hantera svåra påfrestningar på samhället i fred, och
> – med tillgängliga resurser bidra till förmågan att delta i internationella fredsfrämjande och humanitära insatser.
>
> (Prop. 2020/21:30 *Totalförsvaret 2021-2025*)

Försvarsberedningen konstaterar att möjligheterna att förebygga och hantera fredstida kriser, och gråzonsproblematik också förbättras genom en trovärdig totalförsvarsförmåga. Alltså förmåga att bedriva en sammanhållen planering, ledning, beredskap samt nödvändiga resurser för att kunna hantera krig.[20] Regeringen har fördelat förstärkta ekonomiska ramar till det civila försvaret i budgetpropositionen, samt gett förtydliganden och ställt ett återrapporteringskrav i särskilda anvisningar.[21]

Regeringens intention är att utvecklingen av det civila försvaret så långt som möjligt ska bygga på strukturer och processer som används inom krisberedskapen. Förmågan att hantera fredstida kriser i samhället förväntas ge en grundläggande uthållighet och förmåga att hantera krigssituationer, samtidigt som utvecklingen av det civila försvaret förväntas stärka förmågan att förebygga och hantera svåra påfrestningar på samhället.[22]

Det är ännu inte fastlagt hur strukturen för uppbyggnaden av det civila försvaret ska se ut, med ansvariga myndigheter för utpekade områden. Den 1 mars 2021 lämnade utredningen för civilt försvar (Ju 2018:05[23]) sitt betänkande med förslag på en struktur med statliga myndigheter indelade i beredskapssektorer med sektorsansvariga myndigheter. Bland annat föreslås att Trafikverket blir

[19] Ds 2017:66 sid. 175f
[20] Prop. 2020/21:30 sid. 127
[21] Regeringsbeslut II:14 2020-12-17
[22] Prop. 2020/21:30 sid. 127
[23] Dir 2018:79 och 2019:98

sektorsansvarig myndighet inom beredskapssektorn för transporter, och att Transportstyrelsen, Sjöfartsverket och Luftfartsverket ingår i beredskapssektorn. Myndigheter som har ansvar inom en eller flera viktiga samhällsfunktioner, bedriver verksamhet med särskild betydelse för krisberedskapen eller totalförsvaret föreslås benämnas beredskapsmyndigheter. Kommitténs förslag ska nu skickas ut på remiss innan regeringen tar ställning till förslagen.[24]

[24] SOU 2021:xx *Struktur för ökad motståndskraft*

2.2 Utveckling av hotbilden – kort historik

Gråzonsproblematik och hybrida hot är egentligen inga nya fenomen, men begreppen har fått ökad uppmärksamhet och är närvarande såväl i den allmänna debatten som i politiken.[25] I detta avsnitt görs en kort tillbakablick över de senaste hundra åren och vilken hotbild som har varit styrande för beredskapsplaneringen under perioder. Historiskt har hotbilderna varierat, och de har ofta utvecklats utifrån tidigare erfarenheter eller inträffade händelser.

Under 1900-talets första hälft dominerade hotet om långvariga handelsstörningar med omfattande brist på till exempel livsmedel (utifrån erfarenheter från första världskriget). Det ledde till att man satsade på robusta försörjningssystem och lagring av strategiska varor. Efter andra världskriget breddades dock hotbilden till att omfatta fyra delar: militära angrepp, angrepp mot civila mål, psykologisk krigföring och angrepp mot folkförsörjningen. Det var alltså betydligt bredare än ett ensidigt fokus på kriget som hot. Under 70-talet kom hotbilden att komplicera ytterligare, till exempel förmodades att handelsstörningar eller internationella konflikter skulle kunna leda till avspärrningar mot Sverige (och därmed störningar i transportflöden och varubrist).[26]

Efter Berlinmurens fall och Sovjetunionens upplösning tonades snart de militära hoten ned. Vid inledningen av 2000-talet innebar det att Försvarsmakten ominriktades från att fokusera på territoriellt försvar till ett smalare och mer specialiserat insatsförsvar inriktat på internationella insatser. Totalförsvarsplanering upphörde i princip helt och civila myndigheter inriktades på uppgifter inom fredstida krishantering och krisberedskap. I praktiken hade Sverige avskaffat drygt tre av fyra av det gamla totalförsvarets hotbilder – varken militär, psykologisk eller ekonomisk krigföring ansågs längre aktuell. EU-inträdet 1994 ansågs också ha stärkt Sveriges försörjningstrygghet, samtidigt som Ryssland ansågs utvecklas i en demokratisk och fredlig riktning. Många upparbetade samarbeten avseende beredskapsfrågor mellan offentliga aktörer och företag avvecklades successivt.[27]

Perioden från slutet av 1990-talet och fram till försvarsbeslutet 2015 brukar omnämnas som den ”strategiska timeouten” avseende det civila försvaret. Då frångick de flesta aktörer hotbilder som innefattade antagonism, och fokuserade istället på fredstida sårbarheter, kriser, olyckor och naturhot såsom översvämningar och stormar. Fokus lades också på samhällets beroenden inom och mellan sektorer, samt det ökande beroendet av it-system. Även terrorism fanns med i hotbilden efter 11 septemberattackerna 2001.[28] Man kan också tala om en strategisk timeout för det militära försvaret då fokus flyttades allt mer till

[25] Jonsson (2020) sid. 2
[26] Jonsson m.fl. (2019)
[27] ibid.
[28] ibid.

fredsbevarande internationella insatser och fokus på det nationella försvaret minskade. Detta varade dock under en betydligt kortare period.

Under kalla kriget antogs agerande från andra stater följa ett mönster där maktdemonstrationer och uppvisningar var en del i ett maktspel. Idag är snarare osäkerheten och svårigheterna i att förstå vad som händer och varför en del av den nya hotbilden. Det är en sorts gråzon där olyckor, stölder, intrång, falska rykten och sabotage kan ses som isolerade incidenter, men också kan vara en del i en påverkan från annan nation.[29] I nästa kapitel beskriver vi närmare innebörden av gråzonsproblematik och hybrida hot, samt vad som är utmärkande för den, i förhållande till krissituationer och höjd beredskap.

[29] Jonsson m.fl. (2019)

3 Gråzon och hybrida hot

Den återupptagna planeringen för totalförsvaret har sedan 2015 resulterat i ett förnyat arbete med att beakta hela hotskalan, efter att i flera år haft fokus på framför allt fredstida kriser och terrorism. Ett område som har fått ökad fokus som del av denna planering för totalförsvaret är hybrida hot och gråzonsproblematik men dessa begrepps innebörd och användning kan tyckas oklar.

3.1 Om begreppen gråzon och hybrida hot

Ofta används termerna gråzonsproblematik och hybrida hot synonymt för att beskriva hot som ligger under gränsen för väpnad konflikt. Detta öppnar upp för ett brett område där många av de aktiviteter som innefattas är dolda, som subversion, underrättelseoperationer, informationspåverkan eller användning av ombud. Den här typen av hot är svåra att upptäcka eller att attribuera till en särskild aktör. Det gör dessa aktiviteter också svåra att definiera, vilket lätt kan skapa en viss begreppsförvirring.[30] Denna osäkerhet i begreppsanvändningen noterar även regeringen i den försvarspolitiska propositionen, och använder där framförallt begreppet hybridhot avseende situationer då en angripare använder en kombination av olika maktmedel för att nå vissa syften och för att undvika en eskalering till en väpnad konflikt.[31] Försvarsberedningen lägger å andra sidan stor vikt vid osäkerheten som kan uppstå då en antagonist agerar i gränslandet mellan fred och krig och att denne medvetet kan skapa sådan problematik (gråzonsproblematik) genom att agera så nära gränsen för upptäckt som möjligt för att överraska och vilseleda försvararen och undvika beredskapshöjning.[32]

Gråzonsproblematik och hybrida hot kan särskiljas genom att en angripare som agerar i *gråzon* utnyttjar de sårbarheter som finns i samhället för att skapa osäkerhet och samtidigt undvika en eskalerad konflikt. *Hybrida hot* är de verktyg som antagonisten använder för att uppnå dessa mål. Antagonisten försöker att sänka försvarsförmågan och den politiska handlingskraften utan att använda militära medel.

Gråzon beskrivs ibland som ett tillstånd ”mellan krig och fred där stater och andra aktörer försöker att påverka Sveriges intressen, handlingsfrihet och förmåga”.[33] Linjen mellan vad som anses utgöra krig och fred kan dock vara diffus. Något som kännetecknar gråzonen är antagonistens möjlighet att utnyttja en demokratisk stats öppna samhälle och att helt lagligt ägna sig åt olika former

[30] Appelgren m.fl. (2020)
[31] Prop. 2020/21:30 sid. 61
[32] Ds 2017:66 sid. 66
[33] Olsén m.fl. (2020) sid. 15

av antagonism som desinformation, strategiska uppköp eller legal underrättelseinhämtning. Det finns även möjlighet att förbereda illegal verksamhet eller krig utan att för den delen begå ett brott, t.ex. genom subversion, finansiering av ytterlighetsrörelse och kartläggning av sårbarheter eller nyckelpersonal. Just begreppens fokus på förhållanden mellan krig och fred kan få många aktörer att se detta som ett område som inte berör dem. I stället kan aktiviteter som innefattas i begrepp som t.ex. it- och cyberattacker, terrorhot, sabotage, elektromagnetisk störning, informationspåverkan eller ekonomisk påverkan kännas mer relevanta även om det är just denna typ av aktiviteter som är en del av hotbilden.

Att använda begreppen gråzon och hybrida hot kan ha en viktig funktion i att förmedla hur olika typer av händelser, som för sig själva inte pekar på något allvarligt, kan vara del av en koordinerad strategi. Tillsammans kan de då vara del av en större, och möjligen även långvarig, påverkan med negativa följder för den egna verksamheten. Ofta är det först när flera aspekter läggs ihop som bilden av vad som händer blir tydlig. Beskrivningen ”mellan krig och fred” kan också bli missvisande då hybrida hot kan vara ett reellt hot i såväl krig som fred.[34] Antagonistens strategi kan vara just att verka på ett sådant sätt att den kan skapa oro, rädsla och belastning utan att eskalera händelsen till fullskalig konflikt. På så sätt kan antagonisten agera utan att det blir tydligt att det rör sig om en koordinerad strategi.

En antagonist kan även agera genom ombud till exempel genom att på olika sätt uppmuntra till att agera på ett visst sätt eller begå brott, ibland till och med utan att ombuden är medvetna om att en statlig antagonist ligger bakom. Detta kan gälla allt ifrån cyberattacker till kopparstölder, och är särskilt svåra att identifiera som ett antagonistiskt angrepp som en del av en övergripande strategi. Det är först efter att en lägesbild har skapats som det kan gå att koppla ihop olika typer av händelser, brott och incidenter och ett samband kan ses mellan dem. Genom sättet på vilket antagonisten agerar för att undvika upptäckt uppstår det ett utrymme för tolkning om vad som hänt, vem som ligger bakom och varför. Detta skapar osäkerhet i hur den som utsatts ska agera och vilka motåtgärder som ska vidtas.[35]

Det ligger en svårighet i att hitta begrepp och benämningar som passar alla branscher, med olika bakgrund och verksamheter. Kanske är det inte avgörande vilket begrepp som används men däremot finns en risk för missförstånd om skilda aktörer har olika förståelse för de begrepp som används. När vi talar om gråzonsproblematik, hybrida hot och andra närliggande begrepp avses statsinitierad antagonism med olika tillgängliga verktyg och maktmedel som sammantaget uppfattas ligga under krigströskeln – som genomförs med eller utan icke-statliga

[34] Olsén m.fl. (2020) sid. 15
[35] Jonsson, m.fl. (2019)

ombud – med syfte att vinna politiska, psykologiska, ekonomiska eller militär-strategiska fördelar (eller indirekt försvaga motståndaren inom motsvarande domäner). Det viktiga är att de som ska arbeta med planering för dessa hotbilder förstår vilka problem och konsekvenser de kan leda till. Det är inte önskvärt att fastna i diskussioner om vilka begrepp som ska användas.[36]

3.1.1 En kategorisering av hybrida hot

Syftet för en antagonist med att påverka vårt samhälle i stort skulle kunna vara att få Sverige ”att justera sin handels-, utrikes-, säkerhets- eller försvarspolitik, att hindra Sverige från att ta emot eller komma andra till hjälp, att försvaga landet från att ta emot eller komma andra till hjälp, att försvaga landet inför en militär konflikt eller att belasta internationella samarbeten”.[37] En antagonist kan använda olika medel för detta, till exempel ges en övergripande kategorisering i militärstrategisk doktrin 2016:[38]

- Diplomatiska medel – kan innebära handlingar som restriktioner, fientlig retorik, utvisning av diplomater, avbrutna kontakter eller hot om våld i ett försök att påverka beslutsfattare och befolkning.
- Politiska medel – kan innebära handlingar som politisk infiltration, subversiv verksamhet eller stöd till ytterlighetsrörelser.
- Ekonomiska medel – kan innebära handlingar som marknadspåverkan, sanktioner, avbrutna handelsförbindelser, uppköp eller ökat inflytande över strategisk infrastruktur samt angrepp på samhällskritisk infrastruktur.
- Psykologiska medel – kan innebära handlingar som hot om användning av militära maktmedel, cyberaktivism eller påtryckningar mot enskilda beslutsfattare samt skapa oro.
- Information medel – kan innebära att man använder tekniska förutsättningar för att störa infrastrukturer som är beroende av internet, detta kan inkludera cyberattacker mot samhällsfunktioner, cyberspionage, propaganda och desinformationskampanjer.
- Subversiva medel – kan innebära handlingar som, iscensättning av kriminalitet och social oro, kompromettering av beslutsunderlagsdata eller illegal underrättelseinhämtning.
- Militära medel – kan innebära handlingar som sabotage, gränskränkningar, angrepp genom ombud eller blockader.

Många av dessa hot överlappar till viss del och olika typer av hot kan därför falla inom flera av de ovan nämnda kategorierna. En cyberattack kan till exempel falla

[36] Appelgren m.fl. (2020) sid. 14
[37] Jonsson (2018) sid. 21
[38] Försvarsmakten (2016)

inom nästan alla kategorier ovan då den kan påverka ekonomiskt genom inverkan på samhällskritisk infrastruktur, psykologiskt och subversivt genom att skapa oro, politiskt genom att påverka förtroendet för staten och dess förtroendevalda och informationsmässigt genom cyberspionage eller genom att sprida desinformation. Det ligger också i antagonistens intresse att handlingar kan ge så stor påverkan som möjligt inom olika delar av samhället. Ett annat sätt att nå detta är även att använda flera av de ovan nämnda hoten tillsammans. För antagonisten kan det därför ses som särskilt framgångsrikt om de sker i olika delar av samhället och visar få tecken på att vara en samordnad strategi. På så sätt kan antagonisten skapa oro och försvaga samhället utan att det blir uppenbart att en aktör ligger bakom och kan på så sätt undvika upptäckt. När saker sker i olika delar av samhället och av oklara orsaker blir det dessutom svårt att förstå hur stort hotet verkligen är och på så sätt veta var på hotskalan man befinner sig. Det vill säga, ligger vi närmare definitionen av fred eller börjar vi närma oss krig?

3.2 Gråzon och transportsystemet

Transportmyndigheterna tillhör de beredskapsansvariga myndigheter som ska vara del av uppbyggnaden av det civila försvaret. Enligt Samverkansområdet Transporter avser transportsystem ”människor som använder systemen, fordon, den tekniska och fysiska infrastrukturen samt regler och information som stödjer systemet och som krävs för att genomföra transporterna”.[39] Transportsystemet kan påverkas av hybrida hot antingen direkt eller indirekt. I en direkt attack är transportsystemet måltavla. Transportsystemet kan påverkas indirekt genom påverkan mot resurser som är viktiga för transporterna, som t.ex. elförsörjning eller informations- och kommunikationssystem.[40] Det kan också röra sig om händelser som leder till indirekta utmaningar som kan ge en påverkan på transportsektorn, till exempel vid storskalig utrymning.[41] Då är det inte transportsektorn som utgör själva målet, men den påverkas indirekt.

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) har varit aktiv i diskussionen om hybrida hot inom området kritisk infrastruktur, framför allt genom en serie workshops. Här har fokus legat på att definiera vilka områden som bör innefattas i detta samt att skapa internationella samarbeten.[42] Mycket av detta arbete har hittills fokuserat på hybridkrigföring snarare än andra typer av hot.[43]

En studie av utredningar, rapporter och litteratur inom transportsektorn som tar upp termerna gråzon eller hybrida hot visar att termerna inte användas i någon

[39] Helmbring och Arvidsson (2015) sid. 8
[40] Jonsson (2020)
[41] Helmbring och Arvidsson (2015) sid. 57, MSB (2014) sid. 22
[42] Savolainen (2019)
[43] Lohela och Schatz (2019)

större utsträckning. Däremot går det att hitta litteratur som kopplar ihop gråzon och hybrida hot och transport utan att uttryckligen beskriva det i dessa termer. Framför allt gäller detta rapporter som kopplar transport till det civila försvaret eller totalförsvaret.

En rapport som nämner gråzon är Trafikverkets egen utredning: *Redovisning av regeringsuppdrag till bevakningsansvariga myndigheter att inkomma med underlag för den fortsatta inriktningen av det civila försvaret – Gemensamt svar för transportområdet: Trafikverket, Transportstyrelsen, Luftfartsverket och Sjöfartsverket.*[44] Här beskrivs hur gråzon kan komma att påverka samhället genom t.ex. ”ökad kriminalitet, sabotage och störningar i olika vitala system utan att en fiende är utpekad”.[45] Rapporten beskriver områden som transportmyndigheterna gemensamt anser behöver prioriteras inom civilförsvaret för transportsektorn t.ex. anslagsfinansieringar, förtydligande av roller och ansvar och att ”förstärka säkerhetsskydd, informationssäkerhet och säkra kommunikationssystem som bygger på nationella samordnade lösningar”.[46]

Sårbarheter i transportsystemet PM 2018:6 har tagits fram av Trafikanalys för att kartlägga olika definitioner av sårbarheter i trafiksystemet.[47] Rapporten nämner inte gråzonsproblematik eller hybrida hot utan använder begreppet antagonistiska hot vilket beskrivs som: väpnat angrepp, terrorism, it-angrepp eller cyberbrott, elektromagnetiska störningar och andra störningsproblem. Att hantera hot utifrån dessa separata kategorier är det vanligaste inom transportsektorn även om det förefaller finnas en förståelse för att dessa ibland kan hänga ihop. Det är också vanligt att säkerhet och hot diskuteras utifrån transportområdets olika delar: järnväg, vägtrafik, luftfart och sjöfart även om Trafikverket och Transportstyrelsen har mer övergripande roller för området i stort.

De delar inom transportområdet som förefaller ha störst medvetenhet rörande antagonistiska hot generellt finns inom luftfartssektorn och den maritima sektorn. Detta kan till viss del bero på att det finns mer omfattande krav och regleringar utifrån ett trafik- och driftsäkerhetsperspektiv inom dessa sektorer.[48] För flygsektorn kan man även se 11-septemberattackerna som en orsak för det ökade säkerhetsperspektivet, här direkt kopplat till hybridhot.

It-brott och cyberattacker har fått större fokus i och med det så kallade NIS-direktivet som trädde i kraft den 1 augusti 2018. Direktivet innebär att verksamheter som levererar samhällsviktiga tjänster och digitala tjänster måste arbeta med informationssäkerhet och rapportera incidenter. Detta direktiv omfattar alla trafikslag inom transportsektorn.

[44] Trafikverket, Transportstyrelsen, Luftfartsverket och Sjöfartsverket (2019)
[45] Ibid sid. 11
[46] Ibid sid. 11-12
[47] Trafikanalys (2018) sid. 21
[48] Helmbring och Arvidsson (2015) sid. 3

Samverkansområdet Transporter har publicerat flera rapporter om hur transportsektorn kan påverkas av kriser och samhällsstörningar.[49] Dessa rapporter innefattar såväl diskussioner kring specifika krissituationer som kan påverka transportsektorn såsom översvämningar,[50] snöoväder[51] och pandemier[52] som övergripande diskussioner om hur kriser kan påverka transportsektorn mer allmänt.[53] Andra rapporter inom området har även fokus på ansvar och roller inom transportsektorn för krisberedskap.[54] Flera av dessa har använts för diskussion i kapitel 4.

En rapport från Försvarshögskolans Centrum för totalförsvar och samhällets säkerhet (från ett arbete på uppdrag av Livsmedelsverket) presenterar konsekvenserna för livsmedelsförsörjningen ur ett leveransperspektiv av det omfattande snöovädret i Stockholm 2016.[55] Även om denna studie är baserad på ett snöoväder i stället för en antagonist blir det tydligt hur sårbar transport- och leverenskedjan är. Konsekvenserna var vid detta tillfälle begränsade på grund av att störningen bara pågick några dagar. Men en mer långvarig störning, något som är ett tänkbart gråzonscenario, skulle få betydligt större konsekvenser för samhället.

3.3 Vad skiljer gråzon från krissituation?

Det finns med andra ord redan mycket kunskap om hur samhällsstörningar kan hanteras inom transportsektorn. Det är dock viktigt att vara medveten om att det finns skillnader mellan att hantera incidenter under krissituationer och under gråzonssituationer. Till viss del kan det handla om samma typer av händelser, t.ex. störningar i elnät, men i en gråzonssituation är det inte säkert att det stöd som behövs för att hantera en händelse finns tillgängligt. Detta beror på att en ökad mängd incidenter, eller vad som kan se ut som olyckor, skulle sätta stor press på polis, räddningstjänst och andra samhällsviktiga aktörer och funktioner, vilket leder till att mindre akuta ärenden nedprioriteras. Eftersom andra delar av samhället också skulle vara under stor press och personal och material blir svåra att få tag på, särskilt om störningarna blir utdragna eller många incidenter inträffar på flera håll, kan assistans som reparationer etc. ta betydligt längre tid än vad vi är vana vid. Även för system där det finns reservkraft kan en utdragen situation eller upprepade incidenter leda till att reservsystemen inte hinner fyllas på innan nästa störning inleds.

[49] MSB websida för Samverkansområdet transporter.
[50] Trafikverket (2012).
[51] Luftfartsverket (2004).
[52] Sjöfartsverket (2006).
[53] Trafikverket (2013), Trafikverket (2014), Banverket (2007).
[54] Helmbring, K., Arvidsson, U. (2015), Skoog (2012).
[55] Kumlien (2018).

Skillnaden ligger också i att antagonisten i en gråzonssituation kan agera på ett sätt för att ytterligare försvåra hanteringen eller återställningen av en incident, t.ex. genom att störa ledningsfunktioner. En antagonist kan även utnyttja krissituationer som naturkatastrofer eller olyckor för att öka på störningen eller oron i samhället.

För att förtydliga hur eskalerande gråzonsproblematik skulle kunna se ut har FOI på uppdrag av MSB utvecklat ett scenario, Typfall 5, som grund för planering av civilt försvar (se utdrag ur scenariot i textruta nedan).[56] Typfallet innehåller inget sekretessbelagt material utan är öppet tillgängligt. Tanken är att Typfall 5 ska kunna anpassas till olika verksamhets- eller ansvarsområden och på sätt kunna användas som planeringsmaterial. Scenariot är uppbyggt genom att de inledande händelserna får en hel del konsekvenser för samhället samtidigt som det är oklart vad som sker. Händelseförloppet eskaleras över tid för att innefatta fler och mer omfattande händelser. Det blir tydligt hur en utdragen gråzonsproblematik med flera olika typer av händelser påverkar samhället i hög grad. Flera tidigare scenarier som har tagits fram, bland annat i relation till transportsektorn, har fokuserat på incidenter eller händelser som inte är lika utdragna i tid.[57] Det är också viktigt att analysera hur en situation kan utveckla sig över längre tid, något som också blivit tydligt under den rådande pandemin.

[56] Jonsson (2018)
[57] Trafikverket (2012), Luftfartsverket (2004), Sjöfartsverket (2006).

Det inledande skedet

I Sverige, liksom i de nordisk-baltiska grannländerna, har under senare tid ett tämligen stort antal svårförklarliga olyckor inträffat. Detta bidrar till en ökad arbetsbelastning för polis, räddningstjänst och akutsjukvård. Därtill sker en rad dolda angrepp såsom mindre cyberangrepp och fysiska sabotage på samhällsfunktioner där man försöker dölja spåren och/eller rikta misstankarna åt annat håll. Angreppen förefaller ske främst mot ”lågt hängande frukter” såsom lokala försörjningssystem samt enstaka samhällsaktörer och företag, snarare än mot strategiska mål.

Efter några månader

De upprepade infrastrukturella störningarna, som nu pågått i flera månader, sliter på samhället. Verksamheter når övertidstak för anställda, får brist på reparationsmaterial och överskrider budget. De periodvisa störningarna i lokal och regional elförsörjning, liksom i data- och telekomsystemen, bidrar till förstärkta störningar i andra försörjningssystem och samhällsfunktioner. Eftersom även Sveriges grannländer är drabbade förstärks problemen ytterligare av gränsöverskridande effekter.

Den upplevda otryggheten bland människor leder till indirekta effekter såsom exempelvis att det råder brist på vissa livsmedel pga. hamstring. Fler övergår också till att använda kontanter pga. störningar i betalkortssystemen, vilket leder till kontantbrist på vissa håll.

Efter ett halvår

När den ansträngda situationen har varat i ungefär ett halvår blir främmande makts diplomatiska utspel allt mer aggressiva med indirekta hot om militärt våld. Sverige och de nordisk-baltiska grannländerna vill gemensamt med EU peka ut och vidta sanktionsåtgärder mot antagonisten men EU är politiskt splittrat.

Ökningen av fartygsrelaterade incidenter, svårförklarliga olyckor och konstaterade sabotage gör att redare i allt större utsträckning undviker hamnar och farleder i anslutning till Östersjön, inte minst på grund av höjda försäkringspremier. Produktionen i viss tillverknings- och förädlingsindustri har dock redan stagnerat på grund av brist på insatsvaror och komponenter till följd av IT-relaterade störningar i transportlogistiksystemen.

Ett omfattande cyberangrepp inträffar. Detta drabbar såväl Sverige som de närmaste grannländerna och under några dagar fungerar inte betalningssystemen, ledningssystemen för flyg- och tågtrafik samt mobiltelefonin. Den svenska krisberedskapen prövas hårt då också de fysiska sabotagen mot de nationella försörjningssystemen eskalerar. Störningarna som drabbar just el- och drivmedelsförsörjningen skapar stora följdeffekter i andra system, exempelvis påverkas både primärproduktionen av livsmedel och kylkedjan vid transporter, vilket får stora konsekvenser för möjligheten att distribuera färskvaror och frysta livsmedel.

Störningarna påverkar därmed försörjningen av såväl inhemskt producerade som importerade livsmedel. Vissa skador som följd av sabotagen kommer att ta lång tid att reparera och därmed att återställa funktionalitet. Det är svårt att leda och samordna verksamheter och åtkomsten till elektroniska styrsystem är mycket begränsad.

Efter nio månader

Efter nio månaders störningar och svår samhällsansträngning är nu rädslan allmänt utbredd inom den svenska befolkningen och många som har möjlighet lämnar städerna och beger sig till släktingar eller fritidshus ute i landet. Vissa väljer till och med att lämna Sverige. Detta inte minst på grund av att en snar akut livsmedelsbrist kan skönjas. Ransonering förbereds men hamstringen av det som fortfarande finns tillgängligt eskalerar, liksom priserna.

Befolkningen i allmänhet känner stor frustration och uttrycker starkt missnöje, vilket underblåses av främmande makts intensifierade propaganda och ryktesspridning, som bl.a. förmedlar bilden av att förnödenheter undanhålls befolkningen till förmån för Försvarsmakten och dess utländska samarbetspartners. Upplopp och plundring förekommer i flera svenska städer.

Sverige erbjuds humanitärt bistånd, och då i synnerhet vissa svårt drabbade kommuner vid Östersjökusten, i form av direktinförsel av förnödenheter, drivmedel, reparationsmateriel och teknisk personal.

4 Gråzonsutmaningar för transportsystemet

Första steget för att stärka skyddet mot olika typer av hot är att öka medvetenheten om dem och att skapa förståelse för hur en antagonist kan agera. För att skapa en förmåga att sätta sig in i motståndarens perspektiv behövs en förståelse för vilka sårbarheter som finns i samhället, inte enbart kunskap om hotbilden.[58] Termerna sårbarhet och hot är nära kopplade till varandra men de har en viktig skillnad i betydelse. En sårbarhet är något som ligger inom det egna samhället eller den egna verksamheten, en svaghet som kan bero på både interna eller externa faktorer. Ett hot ligger däremot hos antagonisten och i hur denne kan utnyttja verksamheters sårbarheter för att skada eller skapa oro. Att förstå sina egna svagheter är därför ett viktigt steg i att skapa skydd mot antagonistiska hot genom att minska sårbarheter eller öka beredskapen just vid dessa svagare punkter.

I detta kapitel ger vi en bild av hur hoten som beskrevs i föregående kapitel kan komma till uttryck inom transportområdet, samt relevanta sårbarheter avseende transportsystemet. Vi presenterar och diskuterar utmaningar i sex olika kategorier. Dessa utgör exempel på hur hot kan realiseras inom transportområdet eller sårbarheter som en antagonist skulle kunna exploatera. Hotbilden är i många delar överförbar även på andra delar i samhället. Kategorierna utgörs av följande:

- 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

I metodavsnittet (kapitel 1.2) beskrevs hur vi har gått tillväga för att samla in underlag till och beskriva hoten i detta kapitel, samt hur vi har förhållit oss till att viss information kan vara känslig i sitt sammanhang. Texten nedan innehåller generaliserade beskrivningar av ”exempel på hot”, samt omständigheter som skapar förutsättningar för att realisera hot (snarare än konkreta sårbarheter, såvida de inte är allmänt kända och uppenbara). Analysen baseras på den forskning som bedrivs vid FOI avseende gråzon och hybrida hot, särskilt det explorativa arbete som genomfördes åt Energimyndigheten 2018, se ”Gråzonsproblematik och hybridkrigföring – påverkan på energiförsörjning”.

[58] Ds 2017:66

4.1 Marknadsförhållanden skapar spelplanen för företag och antagonister

Att vi har ett öppet samhälle gör att möjligheten för en antagonist att realisera vissa hot finns inbyggda i de grundförutsättningar som samhället vilar på. Det handlar till exempel om marknadens förutsättningar med näringsfrihet, den fria ägande- och etableringsrätten och andra villkor för att bedriva affärsverksamhet. Det är viktigt att komma ihåg att en marknad alltid är utsatt för ett maktspel, men syftet för en antagonist med att försöka påverka marknaden kan till exempel vara att skapa strategiska fördelar genom att påverka priser eller olika företags position och inflytande.

Transportsystemet bygger på en konkurrensmarknad, vilket bland annat gör att det inte finns någon övergripande samordning. Transportslagen är i många fall utbytbara i förhållande till det som ska transporteras, men intresset för att hänvisa till alternativa transportsätt kan vara lågt av konkurrensskäl. Det finns flera inbördes beroenden mellan olika trafikslag och även mellan aktörerna.

Det som komplicerar förståelsen för om ett visst agerande ska ses som marknadskonkurrens eller ett antagonistiskt agerande är att det inte finns några ”motståndare” på marknaden, utan alla är marknadsaktörer dvs. konkurrenter och samarbetspartners. Det kan dock förekomma ageranden som skapar förutsättningar för iscensättande av hot i framtiden, även om det i nuläget inte alls ses som ett hot. Potentiella ombud för framtida antagonistiska aktiviteter kanske i dagsläget inte ens är medvetna om att de är tilltänkta ombud. Det kan exempelvis handla om nya ägarskapsförhållanden, uppköp av infrastruktur eller etablering av leverantörsberoenden. Sådana aktioner är fullt rimliga marknadsageranden som görs i vinstdrivande syften men kan vara aktioner med syfte att understödja en framtida antagonistisk strategi där en samarbetspartner kan utsättas för påtryckningar att agera som ombud.[59]

Avsaknaden av helhetsperspektiv hos enskilda aktörer kan göra det svårt för dem att inse hur viktiga de är i systemet, och på vilket sätt de därmed kan bli utsatta för antagonistisk påverkan i syfte att komma åt andra delar av transportsystemet och inte skada enbart den egna verksamheten. Det kan handla om kommunikationsnoder för ledningar för dataöverföring och informationssystem eller kabeldragningar som hanteras av enskilda men som används av långt fler aktörer, även utanför transportsektorn.

De internationella marknadsprinciperna är i någon mening överordnade nationell lagstiftning. Utländskt inflytande över svensk kritisk infrastruktur är idag oundvikligt. Ett totalförsvarsperspektiv kan i viss mån sägas handla om en strävan

[59] Jonsson (2018)

efter oberoende – att ha egen förmåga att upprätthålla de viktigaste samhällsfunktionerna. Fungerande samhällsfunktioner förutsätter fungerande försörjningssystem, och då krävs att transporttjänster kan utföras. Försörjningssystemen levererar om marknaderna fungerar och inte alltför enkelt kan påverkas på ett otillbörligt sätt. Strävan efter oberoende kan dock inte drivas av de enskilda privata aktörerna på transportmarknaden, frågan ligger på en högre nivå. De enskilda företagen har en viktig roll i totalförsvaret men huvuddelen av själva ansvaret kan inte läggas över på dem.

Frågan om risker med utländska direktinvesteringar har de senaste åren varit aktuell i Sverige liksom inom EU. Europaparlamentet lade i mars 2019 grunden för att kunna granska utländska direktinvesteringar i unionen[60], och i augusti samma år gav regeringen i uppdrag åt en särskild utredare att lämna förslag på hur ett svenskt system för granskning av utländska direktinvesteringar inom skyddsvärda områden kan utformas.[61]

I FOI:s rapport om utländska direktinvesteringar[62] (som har gjorts på uppdrag av Utrikesdepartementet i syfte att stödja den ovan nämnda utredningen) konstateras att svenska myndigheter tolkar säkerhetsrisker och skyddsvärda verksamheter relativt brett. Utländska direktinvesteringar bedöms medföra risker om de negativt kan påverka att den territoriella integriteten kan upprätthållas och att demokratin och rättsstaten fungerar. Det finns också säkerhetskänsliga verksamheter som, om en antagonistisk handling utförs mot dem, kan innebära skada på nationell samhällsviktig verksamhet eller skada för Sveriges ekonomi.[63]

De branscher som under de senaste tio åren har haft störst utländska direktinvesteringstillgångar[64] är finans och försäkring; raffinerad petroleum, kemiska produkter och läkemedel; handel, serviceverkstäder för motorfordon; el, gas, vatten och avfallshantering; livsmedel, dryck och tobak samt transportmedel. I flera av dessa har värdet av utländska direktinvesteringar också ökat betydligt under dessa år.[65] Två av dessa branscher (indelade i grupper efter svensk näringsgrensindelning, SNI) berör transportområdet på ett direkt sätt: serviceverkstäder och transportmedel. Men samtliga områden berör transportområdet indirekt, till exempel finansiering av infrastruktur och företag, försäkring av fordon, drivmedel till fordon osv.

[60] Europaparlamentets och rådets förordning (EU) 2019/452 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen.
[61] Dir. 2019:50, SOU 2020:11.
[62] Petersson, m.fl. (2020).
[63] ibid. Sid. 20
[64] Direktinvesteringstillgångar mäts av SCB och visar Sveriges tillgångar och skulder gentemot utlandet.
[65] SCB ”Direktinvesteringar, tillgångar efter bransch SNI 2007, år 2008-2018”, statistiken återgiven och beskriven i Petersson m fl. (2020) sid. 39

Ökat potentiellt antagonistiskt inflytande över strategisk infrastruktur och verksamheter genom direkt eller indirekt ägarskap över produktions-, distributions- eller driftsresurser som medför ett starkt beroendeförhållande kan ses som en förberedelse inför en konflikt (det vill säga aktiviteter i en gråzon). Antagonistiskt inflytande kan också ske genom påverkan via tredje land och skapa förutsättningar för att få bättre effekt av annan otillbörlig marknadspåverkan. Exempel på hur internationellt samarbete har påverkats av olika länders agerande har vi sett under hanteringen av coronapandemin. Då europeiska länder stängde sina gränser påverkade det inledningsvis en stor del av varutransporterna. Det är viktigt att komma ihåg att det inte bara är själva infrastrukturen som är strategisk. Informationsinhämtning och påverkan på företag och aktörer i syfte att skapa instabilitet kan ske på andra sätt, exempelvis genom att ha koll på positionen av fordon och fartygsmotorer som kan vara uppkopplade mot tillverkarna.

Internationalisering av samhället i stort, och även av transportsektorn, har länge setts som en naturlig utveckling. Flygmarknaden avreglerades under 1980- och 90-talen i hela Europa, sjöfarten blev allt mer internationell särskilt under 90-talet och SJ:s monopol på järnvägsverksamhet togs bort i slutet av 2000-talet. Ägande av kritisk infrastruktur har sedan 1980-talet allt mer förflyttats till privata aktörer. Kontrollen av den kritiska infrastrukturen har i allt högre grad pekats ut som en potentiell riskfaktor som kan utnyttjas för att påverka ett annat land såväl i krig som i ett gråzonsläge.[66] Antagonistiskt inflytande genom ägande via ombud skulle kunna innebära att beslut fattas som minskar transportsystemets tillgänglighet, eller att ägandet fungerar som ett potentiellt politiskt påverkansmedel.

Sjöfarten kan idag betraktas som helt internationell och man kan fråga sig om det går att tala om ”svensk sjöfart”, även om det finns helägda svenska rederier. Sjöfarten lyder under internationella konventioner som den svenska lagstiftningen har anpassats till. Tidigare har Sverige haft egna regler för den svenskflaggade sjöfarten, både vad gäller miljö och säkerhet. Men internationaliseringen av marknaden har tvingat fram en harmonisering av regelverken, i vissa fall på bekostnad av att även regler för ökad säkerhet har fått tas bort. En anledning är att rederierna är snabba på att flagga om sina fartyg om det land vars flagg man seglar under ställer krav som är alltför svåra eller dyra att leva upp till.[67] Även tillsyn och kontrollverksamhet har internationaliserats och privatiserats avseende sjöfarten genom att den till stor del utförs av internationella klassificeringssällskap.[68]

[66] Se till exempel Försvarsberedningens betänkande (Ds 2017:66) Motståndskraft– Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021-2025, sid 78.
[67] Workshop den 20 mars 2020.
[68] International Association of Classification Societies webbsida, iacs.gov.uk

4.2 Transportsystemets öppenhet och tillgänglighet kan utnyttjas av en antagonist

Tillgängligheten är en viktig aspekt för att varutransporter såväl som persontransporter ska fungera på ett bra sätt. Samtidigt kan tillgängligheten till tågstationer, tåg, räls, hamnar och fartyg öka sårbarheten, framför allt för sabotage och terrorattacker. Tillgängligheten till rälsområden leder regelbundet till sabotage i form av kopparstölder och skador på bland annat elledningar. Även i den icke-publika delen av transportsystemet, som till exempel kontorslokaler, finns en kultur med fokus på öppenhet som har beskrivits som tidvis naiv.[69] Här kan man se en skillnad mellan olika typer av transportslag där säkerheten har större prioritet inom vissa. Inom flygindustrin har säkerheten stramats upp ordentligt, framför allt sedan terrorattacken den 11 september 2001 i USA där möjligheten att fysiskt närma sig flygplan eller annan infrastruktur är betydligt mer begränsad. Samtidigt kan man ställa detta i kontrast mot de attacker som har skett mot tågtransporter utan att detta har lett till mer restriktioner.

Öppenhet är viktigt för att transportsektorn ska kunna fungera och attrahera kunder och resenärer. Dessutom är offentlighetsprincipen styrande som en viktig aspekt för att skapa insyn och öka tillgång till information. Balansen mellan öppenhet och säkerhet blir därför svår. Fokus har länge legat på att systemet ska vara tillgängligt och fungera smidigt snarare än på säkerhet. Här kan ytterligare studier bli viktiga för att öka förståelsen och medvetenheten för hot samtidigt som man tar till vara behovet av öppenhet och tillgänglighet.

Digitalisering och Internet of Things (IoT) har även möjliggjort en helt annan typ av öppenhet, en digital öppenhet. Det finns till exempel digitala applikationer som tillåter allmänheten att följa flyg- och båttrafik i realtid. Försök med liknande appar och tjänster där det går att följa tågtrafiken i sin helhet har också gjorts, men i Sverige ligger i dagsläget inte sådan information tillgängligt helt öppet. Transportsystemet är byggt för att vara tillgängligt och effektivt, vilket gagnar alla som vill använda det, oavsett syfte.[70]

Med ökad digital teknik finns det även ökade möjlighet för kunder att ha en bättre insyn i transportflödet, något som uppskattas av kunder och som i många fall är en förutsättning för att transportflödet ska kunna fungera. Denna typ av insyn i hur produkter transporteras efterfrågas allt mer och konsumenter kan även vara villiga att betala mer för detta. Genom att följa varornas väg genom dess digitala spår blir det möjligt för konsumenter att kontrollera var varor har tillverkats och hur transporterna från produktion till konsument ser ut, vilket kan

[69] Workshop den 20 mars 2020.
[70] Trafikanalys (2018)

vara viktigt i ett hållbarhetsperspektiv. För aktörerna inom transportsektorn innebär transparens i leveranskedjan också flera effektiviseringsfördelar. Bland annat har användandet av blockkedjor[71] använts för att säkra leveranser, följa transporter, hantera identiteterna på aktörerna i försörjningskedjan och effektivisera administration.[72] Men ökad transparens betyder även att det finns risk för att dessa system utnyttjas i syfte att störa eller skada.

Även om digital teknik kan öka säkerheten för många processer kan öppenhet inom leverenskedjor och körscheman också betyda ökad risk för hot. Dessa system kan störas av en IT- eller cyberattack, men en attack mot en organisations kommunikation kan också betyda att felaktig information sprids, att falska pressmeddelanden sprids eller att webbsidor läggs upp som ser ut som legitima organisationers webbsidor i syfte att skicka ut felaktig information och på så sätt skada och ifrågasätta samhällets förtroende för organisationen. Öppenheten är en förutsättning i en demokrati där fri och öppen debatt är del av den demokratiska kärnan. Den kan dock utnyttjas av en antagonist i syfte att skapa oro och osäkerhet eller sprida konspirationsteorier. Desinformation kan röra allt ifrån den politiska nivån, om hur transportsektorn ska styras och regleras, till att enstaka avgångar har påverkats av problem.

Framför allt kan desinformationsattacker användas i kombination med andra typer av attacker för att hävda att ett företag eller organisation inte har situationen under kontroll. Dessa attacker kan ske både i kris och under normalläge. Även olyckor som inte har orsakats av någon antagonist kan utnyttjas för att öka oro och skada tilliten till organisationen eller myndigheten som ansvarar för hanteringen av den. Öppenheten är viktig för att skapa tillit men den kan även vara en sårbarhet om en antagonist med syfte att skada just denna tillit utnyttjar situationen.

I kontrast till öppenheten står skyddet av säkerhetsskyddsklassificerad information, som i många fall kan skapa svårigheter att samverka och att kommunicera sårbarheter och utmaningar, särskilt mellan myndigheter, företag och organisationer.

Trots att it-angrepp och cyberhot har ökat betyder det inte att fysiska sabotage inte längre är ett reellt hot. Eftersom transportmedel har använts för terrorism är medvetenheten om sådana typer av hot relativt hög. Ett viktigt exempel är serien av samordnade attacker med hjälp av flygplan i USA den 11 september 2001. Fyra flygplan kapades varav två flögs in i de två skyskraporna i World Trade Centre i New York, ett i försvarshögkvarteret Pentagon i Virginia, medan det fjärde störtade i ett fält i Pennsylvania. Nästan tre tusen personer omkom i attackerna och sex tusen skadades. Ett av de mest omfattande dåden som har

[71] Blockkedja är ett öppet (publikt) och distribuerat verifieringssystem för digitala transaktioner. (www.ne.se)
[72] Sternberg (2017)

genomförts med hjälp av tåg utfördes under rusningstid vid pendeltågstrafiken i Madrid den 11 mars 2004 med explosioner i tågvagnar vid tre olika stationer. Nästan två hundra personer omkom i dådet och drygt två tusen personer skadades.

Det finns flera exempel på attentat där transportmedel eller transportinfrastruktur har använts på platser där många personer befunnit sig. I Sverige och Europa har det bland annat skett attacker med skåpbil (Barcelona 2017) och med lastbil (Nice och Berlin 2016, London och Stockholm 2017). Explosivämnen har detonerat på en tågstation (Bryssel 2017) och på flygplats och på tunnelbanetåg (Bryssel 2016).[73]

Även stöld eller sabotage vid transport av farligt gods ses som ett hot vilket kan utnyttjas av bland annat terrorister. För farligt gods finns särskilda regler om transportskydd.[74]

4.3 Intrång och störningar kan drabba anläggningar och system

Intrång är i sig inte något nytt men det har skett en ökning i antalet olika tillvägagångssätt som en antagonist kan använda sig av. Tidigare handlade det först och främst om fysiska intrång, nu kan intrången ske både på plats och utföras på distans genom till exempel digitala intrång, insiderbrott eller elektromagnetiska störningar.[75] Syftet bakom intrånget kan variera från sabotage, stöld och informationsinhämtning till att skapa oro. Det kan också handla om att plantera skadlig mjukvara som till exempel så kallad malware eller ransomware[76]. Vilket syfte antagonisten har påverkar hur tillvägagångssättet ser ut.

Det fysiska och det digitala intrånget ska inte ses som helt separata områden utan en antagonist kan använda bägge delar i genomförandet av en attack. Till exempel kan ett digitalt intrång vara en del av förberedelsen för ett fysiskt intrång och ett fysiskt intrång kan vara en del av förberedelsen för ett framtida cyberangrepp.[77] Det har funnits en naivitet i det att digitala intrång såsom cyberattacker inte har bedömts få fysiska följder, de beskrivs ofta som icke-våldsamma.[78] I

[73] Trafikanalys (2018)
[74] MSB websida för Transportskydd.
[75] Elektromagnetiska hot utgörs av elektromagnetisk strålning eller av den utrustning som orsakar strålning, och som allvarligt kan skada utrustning och ge negativ påverkan på en verksamhet. Odell m.fl.(2020)
[76] Malware är ett samlingsbegrepp för oönskade datorprogram som utvecklats i syfte att störa it-system eller för dold informationsinhämtning. Ett ransomware är en typ av skadlig programvara vars syfte är utpressning, ofta genom att kryptera filer på den angripnes dator.
[77] Jonsson (2018)
[78] Applegate (2013)

stället behöver man förstå förhållandet mellan de fysiska och de digitala systemen för att förstå helheten och vilka konsekvenser en attack mot en del av systemet kan få för andra delar.

I januari 2008 lyckades till exempel en polsk tonåring programmera om en fjärrkontroll för att kontrollera växlarna i spårvagnsystemet i staden Łodz och kunde därmed dirigera trafiken. Detta ledde till att ett spårvagnståg spårade ur och krockade med passerande tåg. Fyra tåg spårade ur eller krockade med varandra och mer än tolv personer skadades. Detta var den första cyberattacken inom transportsektorn som orsakade skador mot människor.[79] För att kunna programmera om fjärrkontrollen hade tonåringen tagit sig in i depån för spårvagnstågen och stulit de delar som behövdes. Många uttryckte efteråt stor förvåning över lättheten med vilket systemet kunde hackas.[80]

Sedan 2008 har it-brott, cyberattacker och elektromagnetiska störningar blivit allt vanligare och det har sedermera lett till att säkerheten har ökats markant för dessa hot. Särskilt tydligt framstår medvetenheten om cyberhot mot flygindustrin och den maritima transporten även om cyberhot mot tågindustrin också framkommer, om än inte lika mycket. Ett exempel på det ökade intresset på området är den första konferensen för transportcybersäkerhet som hölls i Lissabon i januari 2019.[81] Europeiska unionens cybersäkerhetsbyrå (ENISA) har även tagit fram riktlinjer och råd om till exempel hot mot kritisk infrastruktur och funktioner (Critical Infrastructures and Services, CIS)[82] samt dokumentation om cybersäkerhet för den maritima sektorn.[83] Europeiska sjösäkerhetsbyrån (EMSA) har publicerat en serie nätbaserade kurser för att utbilda och upplysa om cybersäkerhet från ett maritimt perspektiv.[84] Även från nationellt perspektiv har frågor om säkerheten för den maritima transporten lyfts. FOI har till exempel på uppdrag av Sjöfartsverket tagit fram scenarier som stöd till planeringen för totalförsvaret. Här diskuteras gråzon och flera hot inom det området.[85]

Elektromagnetiska hot kan också betraktas som en typ av intrång eftersom det kan användas för att störa ut utrustning och system inom och mellan organisationer. Exempel på elektromagnetiska hot som kan påverka transportsektorn är: störningar mot globala satellitnavigationssystem som kan påverka pålitligheten i positioneringsdata, störning av automatiserade spärr- och gränskontroller vilket

[79] Applegate (2013)
[80] Richards, G. (2008)
[81] 1st Transport Cybersecurity Conference. Dokument med summering av resultaten från konferens. Konferensen arrangerades av organiserad av European Union Agency for Network Information Security (ENISA), Europeiska Kommissionen (DG MOVE), European Union Aviation Safety Agency (EASA), European Maritime Safety Agency (EMSA) och EU Agency for Railways (ERA).
[82] ENISA websida a)
[83] ENISA websida b) ENISA (2020)
[84] EMSA websida
[85] Olsson och Odell (2020)

kan skapa stora problem och förseningar på bland annat flygplatser, radarteknik som kan slå ut annan eller koppla in på annan utrustning eller bredbandiga störningar som bland annat kan påverka radiokommunikation. Störningar kan vara både avsiktliga eller oavsiktliga och det kan ibland vara svårt att avgöra vad eller vem som ligger bakom en störning.[86]

Även om möjligheterna att göra intrång utan att vara fysiskt på plats har ökat finns det fortfarande tillfällen när en ”insider” är bästa sättet för en antagonist att komma åt platser och system. Personer som agerar inom en verksamhet kan arbeta på uppdrag av en antagonist i syfte att inhämta information, förbereda och underlätta för cyberattacker eller förbereda för sabotage på verksamhetens system. Det kan även handla om underrättelseinhämtning eller kartläggning av nyckelpersoner och system som inte kan nås på något annat sätt.[87] Detta gäller inte bara personer som är fast anställda inom verksamheter utan även andra sätt att få in personer på ”insidan” som till exempel praktikanter, tillfälligt anställda, underentreprenörer, leverantörer, samarbetspartners eller personer på studiebesök.[88]

Andra brott och incidenter som vanligtvis framstår och behandlas som separata, till exempel stöld, social oro eller våldsbrott skulle kunna vara del av en koordinerad strategi av en antagonist för att skapa oro och för att underminera förtroendet för myndigheter eller verksamheter inom transportsektorn. Här krävs framför allt samarbete mellan olika myndigheter inom transportområdet och med polismyndigheterna som arbetar för att skapa bättre förståelse för brott som ligger inom gråzonen.[89]

4.4 Säkerhetsrisker uppkommer vid upphandling och användning av varor och tjänster

Att få insyn i en verksamhet och utöva inflytande över den genom ägarskap är, som beskrivs i kapitel 4.1, ett sätt på vilket en antagonist kan agera för att påverka och utöva makt. Ett annat sätt att få tillgång till information och kunna påverka en verksamhet är genom de varor och tjänster som köps in och används i verksamheten. För alla aktörer som verkar inom transportsystemet finns det komponenter och kompetenser som aktörerna själva inte tillverkar eller innehar och därmed måste upphandlas från olika underleverantörer. Med användningen

[86] Odell m.fl. (2020)
[87] Jonsson (2018) sid. 58
[88] Ibid. sid. 58-59
[89] Svenonius (2020)

av komponenter, hårdvara och teknikstöd från underleverantörer följer dock potentiella säkerhetsrisker.

Komponent- och underleverantörsmarknaden är idag global. Många tekniska komponenter tillverkas i utlandet och säljs av internationella aktörer. Även entreprenörer med teknisk och andra former av specialistkompetens verkar på en internationell marknad och är inte alltid hemmahörande i Sverige. Aktörer inom transportsystemet är därmed beroende av varor och tjänster som har sitt ursprung i utlandet, ett beroende som kan innebära utmaningar för verksamhetens säkerhetsskydd. För enskilda aktörer kan det vara svårt att ha överblick över varornas ursprung inklusive alla delkomponenter. Exempelvis kan en modul från ett väletablerat utländskt företag bestå av komponenter som tillverkas i tredje land, som i sin tur innehåller integrerad datorkod från en mjukvaruleverantör i fjärde land, som i sin tur har skrivits av programmerare i femte land. Bristen på överblick över vilka komponenter som ingår i en vara, och var och av vem dessa har producerats, gör det svårt att ha överblick över potentiella säkerhetsbrister i komponenterna. Säkerhetsbrister kan uppkomma av misstag men kan också tillkomma avsiktligt (med ett mer eller mindre specifikt bakomliggande syfte). Oavsett deras ursprung kan en antagonist dra fördel av potentiella säkerhetsbrister som en aktör kanske är omedveten om att denne har i sina system.

Vid sidan av latenta säkerhetsrisker med de upphandlade varorna i sig kan också själva upphandlingsförfarandet medföra potentiella säkerhetsrisker. Bolag kan exempelvis lämna offerter endast i syfte att inhämta information om den upphandlande aktören. Upphandlingsunderlaget kan innehålla information som kravställningar rörande nivåer av säkerhetsskydd eller kritiska systemfunktioner, information som kan vara av intresse för en antagonist. Sådan information kan förvisso även vara intressant för andra aktörer, exempelvis ur ett konkurrensperspektiv, utan att det egentligen finns något bakomliggande antagonistiskt motiv. Det kan vara svårt att särskilja om en offererande aktör drivs av affärsmässiga intressen eller om det kanske finns andra bakomliggande drivkrafter.

Jämte varor finns också potentiella säkerhetsrisker med nyttjandet av kompetenser i form av teknikstöd, entreprenörer, (utländska) gästforskare etc. Beroende på uppgift kan dessa få mer eller mindre tillgång till en aktörs skyddade verksamhet. Inom transportsystemet finns flera säkerhetskänsliga anläggningar samtidigt som många aktörer är beroende av att ta in (tillfällig) extern kompetens för olika uppgifter. Ur ett gråzonsperspektiv innebär det en utmaning, då det, liksom för varor, kan vara svårt att ha en insyn i underleverantörer av kompetens i alla led. Ett nyligen redovisat exempel på den utmaningen är upptäckten av två personer utan arbets- och uppehållstillstånd som arbetade innanför säkerhetsspärrarna vid Arlanda. Bristen uppdagades vid en stickprovskontroll och i det ena fallet rörde det sig om en rysk medborgare som arbetade som flygplanstekniker,

och i det andra fallet om en sydamerikansk man som arbetade vid en restaurang.[90] För säkerhetsklassade anläggningar behövs ett fungerande system med säkerhetskontroll, något som den här händelsen har visat på svagheterna i.

Outsourcing[91] medför en i sammanhanget närbesläktad säkerhetsrisk. Outsourcing kan exempelvis resultera i att en aktör, avsiktligt eller omedvetet, ger externa parter tillgång till verksamhetens skyddade system och att aktören förlorar kontrollen över känslig information. Ett exempel är då Transportstyrelsen hade för avsikt att överlåta driften av myndighetens it-system till ett företag med underleverantörer utomlands. I samband med det beslutades om avsteg från bland annat Säkerhetsskyddslagen, vilket ledde till omfattande kritik och till dåvarande generaldirektörens uppsägning.[92]

För aktörer inom transportområdet medför resonemanget ovan en rad avvägningar. Avvägningarna står mellan att å ena sidan potentiellt göra kostnadsbesparingar genom outsourcing och genom att anlita konsulter och entreprenörer istället för att ha egen personal, samt genom att köpa in tekniska system och produkter istället för att utveckla dem själva, och å andra sidan de potentiella säkerhetsrisker som det också medför.

4.5 Beroenden skapar sårbarheter som kan utnyttjas av en antagonist

Likt alla samhällsviktiga funktioner är transportsystemet beroende av olika former av resurser för att upprätthålla sin funktionalitet. Det handlar exempelvis om interna resurser som egen personal och styrsystem, och externa resurser som drivmedel, elektricitet och elektroniska kommunikationer. Beroenden utgör i sig en potentiell sårbarhet för en verksamhet och kan vid störningar påverka hela verksamhetens förmåga att fungera. Det är något som en antagonist kan tänkas utnyttja. Men, störningar i leveransen av de resurser som en verksamhet är beroende av behöver inte nödvändigtvis medföra negativa konsekvenser. Vissa beroenden kan till del elimineras eller mildras genom att exempelvis skapa redundans i verksamheten och förbereda för alternativa handlingssätt, som egna drivmedelslager, reservkraft och alternativa kommunikationssystem. På så sätt är det möjligt att skapa en mer robust organisation och ett minskat handlingsutrymme för en antagonist att påverka.

För transporter har det alltid funnits ett beroende av drivmedel. Idag befinner sig samhället i en övergångsfas där användningen av traditionella fossila bränslen såsom bensin minskar till förmån för användningen av alternativa (förnybara)

[90] SVT (2019)
[91] Outsourcing är ett företagsekonomiskt begrepp och innebär att en verksamhet läggs ut på en extern utförare.
[92] www.transportstyrelsen.se/sv/Om-transportstyrelsen/fragor-och-svar/

bränslen.[93] Detta sker i kombination med en snabbt ökande andel eldrivna fordon. Möjligheten att använda alternativa bränslen är positivt för transportsystemet i den bemärkelsen att det minskar beroendet av enskilda energislag, såsom oljeprodukter.[94] Samtidigt är kunskapen om de traditionella bränslena mer utbredd och det finns till del också beredskapslagring av petroleumprodukter att använda när försörjningen av drivmedel störs. För de nyare drivmedlen finns ännu inte samma beredskap och inte heller några tidigare erfarenheter från hantering av störningar eller bristsituationer av dessa drivmedel att utgå och lära från i uppbyggnaden av ett robust transportsystem. Övergången till nya drivmedel, som biodrivmedel och el, kan med andra ord initialt skapa sårbarheter som vi ännu inte är helt bekanta med, eller ens är medvetna om.

Det är inte bara på drivmedelssidan som det pågår omfattande omställningar. Samhället automatiseras och digitaliseras i allt högre grad, ofta med en drivkraft om ökad effektivitet och kostnadsbesparingar. För transportsystemet innebär utvecklingen ett ökat beroende av datoriserade system och elektronisk kommunikation i driften av olika verksamheter. Samtidigt sker till följd av automatiseringen och digitaliseringen en förändring vad gäller bemanning, dels minskar personalbehovet, dels skiftar arbetsuppgifterna fokus från att vara mer manuella till att bli mer digitaliserade. Men vad händer i verksamheten om exempelvis it-systemen slås ut och verksamheten inte längre kan styras digitalt? Ofta finns gamla manuella rutiner att plocka fram, men det kan vara få i personalen som varit med och driftat verksamheten manuellt och har kunskap om hur det praktiskt går till. Att hantera en verksamhet manuellt är dessutom mer omständligt och personalkrävande, personal som kanske inte finns tillgänglig till följd av de rationaliseringar som automatiseringen och digitaliseringen fört med sig. Även här för den tekniska utvecklingen med sig sårbarheter som en antagonist kan tänkas utnyttja.

4.6 Utmaningar finns i utvecklingen av en sammanhängande beredskap

Transportsektorn kan å ena sidan ses som en sammanhängande helhet eftersom transportsätten i många fall är utbytbara i förhållande till det som ska transporteras. Å andra sidan finns tydliga skiljelinjer, till exempel mellan godstransporter och persontransporter som har olika förutsättningar.

Trafikverkets uppgift enligt instruktionen är att ”… med utgångspunkt i ett trafikslagsövergripande perspektiv ansvara för den långsiktiga infrastrukturplaneringen för vägtrafik, järnvägstrafik, sjöfart och luftfart samt för byggande

[93] Energimyndigheten (2020)

[94] Sverige är i sammanhanget beroende av import av råolja men är samtidigt en nettoexportör av raffinerade oljeprodukter.

och drift av statliga vägar och järnvägar".[95] Enligt samma förordning har Trafikverket avseende krisberedskap och civilt försvar i ansvar att "… med utgångspunkt i ett trafikslagsövergripande perspektiv samverka med andra aktörer och därvid vidta åtgärder i syfte att utveckla och samordna krisberedskap och planering för höjd beredskap inom transportområdet. I detta ingår att bedriva omvärldsbevakning och analys samt att stödja andra myndigheter med expertkompetens inom området".[96] Trafikverkets uppdrag avseende att utveckla och samordna krisberedskapen och planeringen för höjd beredskap inom transportområdet är bredare än myndighetens egna expertområden och kräver ett nära samarbete med övriga myndigheter inom transportområdet.

Transportsystemet innefattar olika typer av resande och transporter, som ställer olika krav på tillförlitlighet och punktlighet samt är olika känsliga för störningar av skilda slag. När det gäller kollektivtrafiken uppfattas det som oklart vilken myndighet som har det övergripande ansvaret. Stora mängder människor reser kortare sträckor dagligen. Ansvaret för regional kollektivtrafik ligger på landets regioner, medan Trafikverket ska "… verka för en grundläggande tillgänglighet i den interregionala kollektivtrafiken".

Ansvaret för att se till att vissa transportförmågor – med alla ingående komponenter – över huvud taget finns är ett ansvar som ligger utanför de enskilda aktörerna inom sektorn, eller hos dem gemensamt. Det kan behöva analyseras vilka funktioner som är grundläggande för nationen att upprätthålla under kris och krig och precisera detta ansvar. Av myndigheterna inom transportområdet är det ingen som har uppdraget att se till *att branschen och transporterna fungerar*. Uppdragen består i allt från att bedriva tillsyn och se till att regelverken efterlevs samt att utveckla dessa, till att ansvara för utveckling och underhåll av infrastruktur osv. Sedan är det transportföretagen och efterfrågan som styr att transporterna sker. I vissa fall, till exempel där efterfrågan är låg, har Trafikverket särskilda uppdrag att upphandla trafik.

Att transportsystemet består av många aktörer och att mycket sker på lokal nivå innebär en utmaning för att utveckla en sammanhängande beredskap inom transportområdet. Det är viktigt att det finns ett gemensamt perspektiv i arbetet. Det gäller också att hitta en balans mellan vad som sker gemensamt och vad som kan begränsas inom en organisation eller bransch. Att skapa sammanhängande planeringsstrukturer har blivit allt mer komplext allteftersom fler aktörer är inblandade med flera lager av underleverantörer. För företag inom transportområdet är det en förutsättning att arbetet drivs på av myndigheterna för att skapa en beredskap och en robusthet i systemet.

Samtidigt som beredskapen nu byggs upp sker en parallell stark utveckling på miljöområdet som ger stor påverkan på transporter, till exempel genom att nya

[95] §1 SFS 2010:185. Förordning med instruktion för Trafikverket
[96] §3a SFS 2010:185. Förordning med instruktion för Trafikverket

bränslen och eldrift ersätter fossila bränslen och genom förändrade resmönster. Genom detta kan det uppstå målkonflikter mellan miljö och säkerhet. Men, det är också viktigt att uppmärksamma och utveckla de synergieffekter som finns och att arbeta för att utöka dessa. Det finns nu ett unikt tillfälle när båda dessa områden står inför stora omdaningar av samhället, att utnyttja möjligheten till positiv förändring i båda riktningarna. Perspektiven miljö och säkerhet ska inte behöva bli en fråga för avvägning, utan bör stärka varandra.

Att studera transportsektorn ur ett flödesperspektiv kan ge nya perspektiv på hur gråzon och hybrida hot kan ge konsekvenser både inom sektorn och för andra delar av samhället. Eftersom olika typer av flöden, som fysiska flöden och informationsflöden, är integrerade kan störningar få konsekvenser även i andra delar av flödet. För att ett fysiskt flöde ska kunna fungera är det beroende av informationsflödet.[97]

Utveckling som digitalisering, artificiell intelligens, massdata, automatisering av trafik och Internet of Things kommer att påverka transportsektorn i allt högre grad. En ökad integration mellan olika system och aktörer både inom och utanför transportsektorn gör att hela transportsystemet, flödet, har blivit betydligt mer omfattande. Detta ger stora fördelar genom att olika varor, tjänster, kunder och leverantörer kan flöda mer obehindrat mellan olika operatörer och områden men det betyder även att en antagonistisk påverkan i en del av systemet kan få stora konsekvenser även för andra delar. Vissa beroendeförhållanden är mer självklara, som transportsektorns beroende av importerad fossil bränsle eller elförsörjningen för tågtrafiken, medan andra inte omedelbart förefaller lika tydliga, som hur intrång i en underleverantörs it-system kan slå ut betalningssystem.

[97] Olsén, m.fl. (2020) sid. 14 med referens till boken, Oskarsson, B., Aronsson, H., och Ekdahl, B. (2013) Modern Logistik – för ökad lönsamhet.

5 Hantering av hybrida hot och gråzonsproblematik

I föregående kapitel presenterades en uppsättning hot och sårbarheter för transportsystemet utifrån ett hybridhots- och gråzonsperspektiv. En del hot och sårbarheter är av mer sektorsövergripande karaktär, medan andra är mer specifika för transportsystemet utifrån dess utformning och förutsättningar. Oavsett typ av hot och sårbarhet finns det skäl för att reflektera över hur en aktör ska förhålla sig till dem och på vilket sätt som de kan hanteras i verksamheten. Inom transportsystemet arbetas idag (mer eller mindre kontinuerligt) med krisberedskapsfrågor och hur olika former av störningar i den egna verksamheten kan hanteras. Det finns en medvetenhet om och både planering för och åtgärder mot en rad olika händelser. Det kan röra sig om allt från naturhändelser och olyckor, till anlagda bränder, stölder, insiders och attentat. En del aktörer genomför också kontinuerligt risk- och sårbarhetsanalyser. Därtill ställer Säkerhetsskyddslagen (SFS 2018:585) krav på genomförandet av säkerhetsskyddsåtgärder för informationssäkerhet, fysisk säkerhet och personalsäkerhet, för verksamheter som är av betydelse för Sveriges säkerhet – däribland verksamheter inom transportsystemet.

Sammantaget betyder det att det redan idag finns vissa förberedelser och viss motståndskraft i transportsystemet, och i samhället som helhet, för att hantera sådana påfrestande situationer som faller inom ramen för det som kan beskrivas som hybrida hot och gråzonsproblematik. Som nämns i avsnitt 3.3 finns det dock viktiga skillnader mellan ”vanliga” krissituationer och en gråzonsituation. Exempelvis finns det bakom hybrida hot och verkställandet av dessa per definition en antagonist att förhålla sig till, även om det kan vara svårt att identifiera vem det är. Antagonisten kan potentiellt påverka i vilken riktning som en händelse utvecklar sig. En gråzonssituation karaktäriseras också av att det parallellt kan ske flera olika händelser som tillsammans kan skapa påfrestning på hela samhället. I en sådan situation är det inte säkert att det stöd som behövs för att hantera en händelse finns tillgängligt, som det kanske hade varit under mer ”normala” omständigheter (i termer av reparationspersonal, expertstöd, materiel, etc.). Hybrida hot och gråzonsproblematik utgör därmed sammantaget en något annan typ av utmaning än den fredstida krisen, och fordrar därmed också troligen andra former av åtgärder.

Baserat på en genomgång av forskningslitteratur presenteras i en tidigare FOI-rapport av Svenonius och Strindberg[98] fyra olika delmoment som anses vara centrala när det kommer till hantering av hybrida hot:

[98] Svenonius och Strindberg (2019)

- att upptäcka dem,
- att medvetandegöra,
- att bygga motståndskraft och
- att skapa institutionella arrangemang där så behövs.

Nedan följer en översiktlig genomgång av delmomenten utifrån ett transportsystemperspektiv med resonemang, exempel och åtgärdsförslag som har lyfts under projektets workshopar, eller framkommit i tidigare relaterat arbete vid FOI.

Att upptäcka och medvetandegöra

I Säkerhetspolisens årsbok från 2019 beskriver myndigheten en i grunden förändrad hotbild mot Sverige där främmande makt bedriver öppen och dold påverkan i termer av breddad och fördjupad underrättelseverksamhet, spionage mot säkerhetskänslig verksamhet, avancerade cyberangrepp och stöld av teknologi, forskning och utveckling. Hybrida hot är med andra ord högst verkliga i dagens samhälle, och ett första steg mot att förhålla sig till dem är en ökad medvetenhet och förmågan att upptäcka deras existens.

För att kunna upptäcka om den egna verksamheten har drabbats av antagonistiska aktiviteter är det två aspekter som är särskilt viktiga. För det första behövs en förståelse för vad som är ett ”normalläge”, det vill säga hur verksamheten ser ut i normalfallet utan några störningar. Om aktörerna inom transportsystemet har en god förståelse för hur normalläget ser ut så är det lättare att upptäcka anomalier, det vill säga händelser som ligger något utanför det normala men som kanske inte automatiskt väcker larmklockor. För det andra behövs en medvetenhet hos personalstyrkan om potentiella hot mot verksamheten och hur dessa kan ta sig uttryck. Medvetenheten behövs för att anomalierna ska kunna uppmärksammas och kommuniceras vidare inom verksamheten. En sådan medvetenhet behöver finnas på alla nivåer inom en organisation. Om inte ledningen betraktar antagonistiska hot som något viktigt att ta hänsyn till i organisationens beredskapsarbete så kommer det inte heller att finnas varken resurser eller incitament för andra att prioritera det.

Att bygga motståndskraft

Avskräckning eller tröskelförmåga är begrepp som kan tolkas som att vi som samhälle har sådan gemensam styrka att vi klarar att motstå de yttre hot och påtryckningar som sker. En stor motståndskraft kan innebära att det krävs en allt för stor insats för antagonisten att genomföra sin tänkta verksamhet och att denne då väljer att avstå eller agera på annat sätt. Sett ur det perspektivet är Sveriges första försvarslinje just att upprätthålla samhällets funktionalitet. Här spelar transporter en avgörande roll. Robusthet i transportsystemet är därför en viktig aspekt i Sveriges totalförsvar, och det gäller att alla aktörer i systemet ser sin roll som en viktig del av totalförsvaret.

Att skapa ett robust transportsystem och att bygga motståndskraft handlar både om att vidta åtgärder för att förebygga att en aktör drabbas av antagonistisk påverkan, och om att vidta åtgärder för att minska skadeverkningarna i verksamheten i de fall den faktiskt drabbas.

Det finns flera förebyggande åtgärder som kan vidtas för att skapa robusthet och öka redundansen inom den egna, eller relaterade, verksamheter. Tekniska exempel på detta kan vara att sektionera verksamhetens it-system. Genom att hålla olika delar i systemen separata behöver en attack mot ett system inte påverka ett annat. Ett annat sätt att skydda verksamheten kan också vara att använda beprövade tekniska lösningar. Ofta ser vi förändring som något positivt, särskilt när det kommer till tekniska lösningar. Men nya system kan även betyda att verksamheten blir mer beroende av leverantörer och andra aktörer vilket kan skapa sårbarheter. Nya system kan också ha oprövade säkerhetslösningar, leda till fler uppkopplingspunkter och öka beroenden till andra interna eller externa system.

Även när det gäller fysiskt skydd finns det åtgärder som kan öka verksamhetens motståndskraft. Under de workshoppar och digitala möten som har varit en del av projektet har problem med olika verksamheters säkerhetskultur lyfts. Här gäller det att hitta sätt att skärpa verksamheters fysiska skydd som att exempelvis begränsa tillträdet.

Att öka informationsutbytet mellan aktörer inom transportsektorn kan även hjälpa till att skapa kunskap om incidenter som har inträffat hos andra organisationer och verksamheter. Detta måste dock ske på ett säkert sätt för att ta hänsyn till sekretess och känslig information.

Ett viktigt verktyg för att förebygga incidenter är att genomföra risk- och sårbarhetsanalyser. En grundlig utredning om vilka sårbarheter och hot som föreligger samt vilka konsekvenser en störning kan få är en viktig utgångspunkt för att skapa en beredskap.

Det är samtidigt viktigt att aktörer förbereder sig på hur man ska hantera en situation när en störning eller incident har inträffat för att på så sätt minska verkningarna av incidenten. Här handlar det framför allt om att hålla krisplaner uppdaterade och att öva organisationen i att hantera olika typer av störningar genom scenarier. Då störningar, särskilt om de blir långvariga, kan påverka personalförsörjning är detta något som måste planeras för. Det kan exempelvis handla om situationer där många inte kan ta sig till sina jobb eller måste stanna hemma för att exempelvis ta hand om sin familj. Att upptäcka vilka roller som är särskilt sårbara, framför allt specialiserade roller som är svåra att ersätta med annan personal, kan vara del av en viktig förberedelse. Här gäller det även att förstå att beroende av konsulter eller leverantörer kan utgöra en sårbarhet då dessa kan vara svåra att få tillgång till i en gråzonssituation med flera parallella händelser i samhället eller när ett utdraget förlopp ställer stora krav på experter eller specialister inom specifika områden. Kopplat till detta är även svårigheter

att få leveranser under en samhällsstörning, även i detta fall med ökad påverkan beroende av hur länge störningen pågår.

Att även ha en planering för vilka system som kan läggas över till manuella rutiner vid en stor samhällsstörning kan vara av stor vikt. Detta gäller exempelvis möjligheten till att gå över till manuella system för att upprätthålla kritiska leveranser med manuella logistiksystem, möjligen med hjälp av alternativa kommunikationssystem som det svenska säkra myndighetsnätet, SGSI, eller RAKEL. Ett exempel på övergång till manuellt system var den cyberattack som informationssystemet vid flygplatsen i Bristol utsattes för 2018. Då inga skärmar längre visade någon information fick man återgå till manuella metoder som att skriva upp information på tavlor.[99] Att förbereda för hur dessa situationer kan se ut redan på förhand ger en chans att utbilda personalen att hantera olika typer av händelser. Det ger också stöd och möjlighet till övning för beslutsprocessen att lägga om arbetet genom alternativa system, något som det kan vara svårt att fatta snabba beslut om under en kris.

En sista åtgärd som kan vara värd att fundera på som beredskap inför samhällsstörning eller gråzonsrelaterade hot är beredskapslagring. Detta område har fått förnyat utrymme i diskussioner om beredskap under Covid-19 pandemin men då har fokus framför allt legat på lagring av livsmedel, läkemedel och andra hjälpmedel för sjukvården, som respiratorer och munskydd. Som pandemin har visat är det dock inte bara dessa typer av materiel som snabbt kan sina under en samhällsstörning och när leveranskedjor störs kan det snabbt uppstå en brist som kan ytterligare påverkatransportsektorn såväl som samhället i stort. Har verksamheter dessutom drabbats av sabotage och behöver materiel för att reparera skador kan en brist få stora konsekvenser.

Institutionella arrangemang

Hantering av hybrida hot och gråzonsproblematik underlättas om det finns en samhälleligt sammanhängande och samordnad strategi för det, från sektors-, myndighets- och departementsnivå upp till ett internationellt plan. Frågor som rör hantering av hybrida hot behandlas idag både inom EU, av olika internationella organ, såsom Hybrid CoE i Helsingfors, och nationellt inom exempelvis Regeringskansliet. När det kommer till hybrida hot och gråzonsproblematik får man nog utgå från att enskilda aktörer inte kommer att ha en förståelse för och uppfattning om hela problembilden, utan sitta på enskilda pusselbitar. Samordning genom olika former av institutionella arrangemang är därmed en viktig del i hanteringen av hybrida hot och i arbetet med att gemensamt bygga den motståndskraft som behövs.

[99] BBC News den 16 september 2018 *Cyberattack led to Bristol Airport bland screens*

6 Avslutande reflektioner

Gråzonsproblematik är inte ett nytt fenomen, men det har fått ökad aktualitet på senare tid. Genom vårt allt mer digitaliserade och uppkopplade samhälle finns det möjlighet för antagonister att genomföra attacker och aktiviteter på bekvämt avstånd från målet, och de kan slå mot flera mål koordinerat parallellt med annan verksamhet inom hybridkrigföring. Att traditionella styrkedemonstrationer och militära konfrontationer bär med sig kostnader av ett helt annat slag bidrar sannolikt till valet av metod.

Att begreppet gråzon har blivit populärt innebär också att innebörden kan skilja sig åt i olika sammanhang, och beskrivningar tenderar att bli oprecisa. En anledning till detta är också den osäkerhet som naturligt sammanknippas med gråzonen – antagonistens strategi är sällan öppen och inkluderar att verka utan att bli upptäckt, och under den nivå som skulle kunna resultera i en eskalering hos motparten. Det är en del av antagonistens strategi att utnyttja motpartens önskan om att inte eskalera konflikten.

För enskilda aktörer kan det vara ett rimligt mål att ha förmåga att skydda sig mot enskilda företeelser som kan vara del av en antagonistisk strategi, såsom att skydda sig mot intrång eller påverkanskampanjer (vilket diskuteras i kapitel 5). Att hålla koll på vilka händelser som även är en del av en koordinerad antagonistisk strategi kan sägas höra till centrala myndigheters uppgifter, som har möjlighet att skapa en mer övergripande bild på nationell nivå. Men att ha kunskap och förståelse om en sådan bakomliggande strategi kan också vara en förutsättning för att upptäcka och identifiera hot och därmed kunna skydda sig mot dem.

Att civila samhället fungerar står för en stor del av tröskeleffekten

Man kan tala om en konfliktavhållande tröskeleffekt som innebär att en presumtiv angripare inte ska anse att det är lönt att försöka angripa ett land, på grund av att risken är stor att målet inte kommer att kunna uppnås, att det kommer att kosta för mycket eller att det riskerar att drabba angriparen själv.[100] Ur ett civilt perspektiv kan detta förstås som att samhället har en så pass god resiliens att insatsen för en angripare blir orimligt hög. Ett resilient samhälle – ur flera perspektiv såsom robusta försörjningssystem och motståndskraft mot påverkan och störningar – är en viktig del av tröskeleffekten mot både militära hot och gråzonsaktivitet. Angreppen biter då inte på försvararen utan kan till och med fungera som en larmklocka.[101] Dessutom är samhällets stöd till Försvarsmakten viktigt för att möjliggöra olika typer av militära försvarsåtgärder, vilket

[100] Dalsjö (2017)

[101] Jonsson och Veibäck (2020)

gör att samhällets resiliens ger en krigsavhållande effekt. Vår första försvarslinje kan alltså sägas vara de system som samhällets funktionalitet är beroende av.

Robusta försörjningssystem är en viktig grund i fred som krig och i gråzon

I ett resilient samhälle är robusta försörjningssystem en viktig byggsten, till exempel väl fungerande infrastruktur för transporter, energi, kommunikation och ekonomi. Detta gäller under alla förhållanden, oavsett vilken typ av hot samhället ställs inför. Att diskutera gråzonsproblematik tydliggör att det är svårt att planera för fungerande försörjningssystem eller samhällsviktiga verksamheter under störda förhållanden utifrån en enda dimensionerande hotbild. Genom den spännvidd och mångfald av hot som kan användas inom gråzonen ökas förståelsen för att gränsen mellan krig och fred inte är så skarp i praktiken.

Regeringens och centrala myndigheters styrning av totalförsvarsplaneringen bör också vara anpassad till en bredd av hotbilder och inte fastna vid befintliga begrepp i lagstiftningen såsom begreppet ”höjd beredskap”. De hot som vi beskriver som gråzons- eller hybrida hot kan inträffa både i fred och i krig. Oavsett om Sverige i juridisk mening befinner sig i fred eller krig så behöver vi kunna möta den här typen av hot och hantera de händelser som inträffar.

Förmågan att tala semi-hemligt behöver stärkas

Under den så kallade strategiska timeouten var det inte bara beredskapslager och kapitaldrivande resurser som avvecklades. Under tiden drogs både planering för, och övning av, olika situationer kopplat till höjd beredskap ner till ett absolut minimum. Samarbeten mellan det civila samhället och Försvarsmakten minskade. Detta sammantaget har också minskat förmågan och vanan att hantera och på ett säkert sätt förmedla hemlig information (eller information om informationen). Detta gäller såväl inom myndigheter som samhället som helhet. När sådan minskad förmåga och vana är utbredd och det enda som skyddas är information som förvaltas av få personer, så uppstår två saker: å ena sida en utbredd uppfattning om att det *inte finns behov* av skydd eftersom man inte känner till att det finns hemlig information som behöver skyddas. Å andra sidan en oförmåga att tala om viktiga aspekter av rädsla för att utlämna något som är känsligt.

Båda dessa tendenser skapar en farlig situation där skyddsvärd information riskerar att röjas på grund av att det saknas förståelse för att till exempel ett it-system behöver ha ett högt skydd. Och eftersom man inte har en vana av att tala om systemet som bärare av känslig information försvåras uppbyggnaden av förståelsen.

Uppdaterade regleringar såsom nya säkerhetsskyddslagen, NIS-direktivet och föreskrifter om informationssäkerhet och säkerhetsskydd har lagt ökat fokus på att även samhällets säkerhet och funktionalitet betraktas som del av Sveriges

säkerhet och att det här finns skyddsvärda funktioner. Sveriges säkerhet handlar inte bara om de primärt försvarsinriktade funktionerna.

Höja medvetandet om gråzon brett i organisationer och i samhället i övrigt för ökad motståndskraft

Medvetenheten om gråzonsproblematik och hybrida hot behöver höjas hos många aktörer och inom organisationer. Dock ligger det en svårighet i att på ett enkelt sätt förmedla information eftersom samlad information om hot och sårbarheter i regel är förknippade med sekretess. Men för att skapa en motståndskraft mot hoten är det en viktig grund att förståelsen för dem finns brett i samhället och särskilt i samhällsviktig verksamhet. Det lägger förutsättningen för att bygga en beredskap (såväl mental som fysisk). Här har bevakningsansvariga myndigheter en viktig roll gentemot respektive bransch att bedriva en väl avvägd informationsspridning. Den grad av öppenhet som behövs måste avvägas mot riskerna med att vi blottar delar av vår kunskap.

Lägga fokus på det utmärkande med att det finns en antagonist bakom hoten, inte fastna i definitioner

Riskmedvetenheten generellt är för flera branscher inom transportsektorn mycket god, även om det skiljer sig mellan olika aktörer. Men, för de flesta privata aktörer räknas inte att värna rikets säkerhet som en kärnverksamhet, och därmed ligger hot som påverkar den och totalförsvarets behov oftast utanför de riskanalyser som görs. En framkomlig väg för att höja kunskapen om hoten kan vara att börja arbeta mer med de olika hoten och även analysera vilken skillnad olika typer av hot ger skilda verksamheter.

Främja synergieffekter mellan miljö och säkerhet

Samtidigt som beredskapen byggs upp sker en stark utveckling på miljöområdet, som också påverkar transportsektorn. Genom detta finns det risk att det uppstår målkonflikter mellan miljö och säkerhet. Mycket handlar dock om att kunskapen om och beredskapssystemen för nya lösningar ännu inte är på plats, och här behöver energi läggas på att uppmärksamma och utveckla de synergieffekter som finns. Perspektiven miljö och säkerhet ska inte behöva bli en fråga för avvägning utan stärka varandra. Det gäller att nya lösningar blir långsiktiga hållbara ur flera perspektiv.

7 Referenser

Applegate, Scott, D. 2013. The Dawn of the Kinetic Cyber. Conference: 5th International Conference on Cyber Conflict. https://www.researchgate.net/publication/237065308_The_Dawn_of_Kinetic_Cyber

Appelgren, J., Bay, S., Malminen, J., Zouave, E. 2020. *Strategisk verktygslåda mot hybridhot – ett ramverk för gemensam problemförståelse*. FOI-R--4816--SE

Banverket 2007. *Öresundsstudien 2006*. Samverkansområdet transporter.

BBC News 16 september 2018 *Cyber attack led to Bristol Airport bland screens*. www.bbc.com/news/uk-england-bristol-45539841 (åtkomst 2021-01-13)

Dalsjö, R. 2017. *Fem dimensioner av tröskelförsvar*. FOI-R--4458--SE

Dir. 2018:79 *Ansvar, ledning och samordning inom civilt försvar* samt tilläggsdirektiv 2019:98

Dir. 2019:50 *Ett system för granskningar av utländska direktinvesteringar inom skyddsvärda områden*. Justitiedepartementet

Ds 2017:66 *Motståndskraft. Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021-2025*.

EMSA websida. http://www.emsa.europa.eu/we-do/safety/maritime-security/item/3477-cybersec.html

Energimyndigheten 2020. *Energiläget 2020*. ET 2020:1

ENISA 2020. *Cyber risk management for ports. Guidelines for cybersecurity in the maritime sector.*

ENISA 2019. 1st Transport Cybersecurity Conference. Dokument med summering av resultaten från konferens: https://www.era.europa.eu/sites/default/files/events-news/docs/1st-transport-cyber-security-conference-conclusions.pdf (åtkomst 2020-11-27)

ENISA webbsida a). https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services?tab=details

ENISA webbsida b). https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

Europaparlamentets och rådets förordning (EU) 2019/452 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen.

Försvarsmakten 2016. *Militärstrategisk doktrin – MSD 16*. FM2016-7616:1

Helmbring, K., Arvidsson, U. 2015. *Förstudie: Ansvar och roller i transportsektorn avseende arbete inom krisberedskapsområdet*. Konsultrapport från Combitech AB för Samverkansområdet Transporter.

International Association of Classification Societies websida: www.iacs.gov.uk (åtkomst 2020-10-06)

Johansson, J., Arvidsson, B., Tehler, H., 2017 *Kunskapsöversikt säkra flöden, försörjningssäkerhet och kritiska beroenden*. MSB1115 45-46

Jonsson, D. och Veibäck, E. 2020. *Nato och svensk civil beredskap – Ett kunskapsunderlag med fokus på NATO Baseline Requirements och svensk energiförsörjning*. FOI-R--4937--SE

Jonsson, D., Ingemarsdotter, J., Johansson, B., Rossback, N., Wedebrand, C. och Eriksson, C. 2019. *Civilt försvar i gråzon*. FOI-R--4769--SE

Jonsson, D. 2020. *Preparing for Greyzone Threats to the Energy Sector*. Occasional Paper, Royal United Services Institute for Defence and Security Studies.

Jonsson, D. 2018. *Gråzonsproblematik och hybridkrigföring – påverkan på energiförsörjning*. FOI-R--4590--SE:

Kumlien, U. 2018. *Snöovädret i Stockholm 2016. Konsekvenserna för livsmedelsförsörjningen ur ett leverensperspektiv.* Försvarshögskolans Centrum för totalförsvar och samhällets säkerhet.

Lindahl, D., Liljedahl, B., Waleij, A. 2020. *Cyberattacks in the healthcare sector during the first three months of the Covid-19 pandemic* FOI Memo 7062

Lohela, T. och Schatz, V. 2019. *Handbook on Maritime Hybrid Threats - 10 Scenarios and Legal Scans*. Hybrid CoE

Luftfartsverket 2004. *Rapport från Göteborgsstudien 2004*. Samverkansområdet transporter.

MSB websida för Samverkansområdet transporter: www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/samverkansforum/samverkansomraden/ (Åtkomst 2021-01-13)

MSB websida för Transportskydd: www.msb.se/sv/amnesomraden/skydd-mot-olyckor-och-farliga-amnen/brottsforebyggande/transportskydd/ (Åtkomst 2021-01-13)

MSB 2014. *Att planera och förbereda en storskalig utrymning*.

Odell, A. Zouave, E. och Jaitner, M. 2020. NCS3 – Elektromagnetiska hot mot trådlösa system. FOI-R--4838--SE.

Olsén, M., Melander, A., Eckersand, U. 2020. *Samverkan och ledning i gråzon – en identifiering av behov och verktyg* FOI-R--4959--SE

Olsson, M. och Odell, A. 2020. *Grundscenario Sjöfartsverket*. FOI Memo 7048

Petersson, M., Almén, O., Denward, C., Holmquist, E., Malmlöf, T. och Ädel, M. (2020) *Utländska direktinvesteringar i skyddsvärda verksamheter – En studie av risker, branscher och investerare*. FOI-R--5069--SE.

Prop. 2014/15:109 *Sveriges försvar 2016-2020*

Prop. 2020/21:30 *Totalförsvaret 2021-2025*

Regeringskansliet (Justitiedepartementet) 2020-12-17 *Anvisningar för det civila försvaret för försvarsbeslutsperioden 2021-2025* Ju2020/04658 (delvis)

Richards, G. 2008. Hackers vs slackers, *Engineering & Technology* 8-21 November 2008.

Savolainen, J. 2019. *Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?* Hybrid CoE

SFS 2007:1161. Förordning med instruktion för Sjöfartsverket

SFS 2008:1300. Förordning med instruktion för Transportstyrelsen

SFS 2010:184. Förordning med instruktion för Luftfartsverket

SFS 2010:185. Förordning med instruktion för Trafikverket

SFS 2015:1052. Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap

SFS 2015:1053. Förordning om totalförsvar och höjd beredskap

Sjöfartsverket 2006. *Rapport från Stockholmsstudien*. Samverkansrådet transporter.

Skoog, R. 2012. *Kommunerna, krisen och logistiken*. SOTP-rapport.

Sternberg, H. 2017. Blockkedjan hjälper oss att följa i godsets spår. *Transportnytt* Nr. 4.

Stenérus Dover, A-S. 2019. *NCS3 Studie: ICS och gråzonsproblematik* FOI memo 6699

SOU 2020:11 *Kompletterande bestämmelser till EU:s förordning om utländska direktinvesteringar*.

SOU 2021:xx *Struktur för ökad motståndskraft*. (SOU:n hade vid denna rapports publicering ännu inte publicerats i SOU-serien och därmed inte tilldelats något nummer.)

Svenonius, O. och Strindberg, A. 2020. *Hantering av hybrida hot - Utgångspunkter och val av strategi för Polismyndigheten*. FOI-R--4966--SE

SVT 2019. *Krismöte efter säkerhetsmiss på Arlanda: ”Vi har utmaningar”.* www.svt.se/nyheter/lokalt/stockholm/efter-krismote-pa-arlanda-vi-har-utmaningar (Åtkomst 2021-01-13)

Thunholm, P. 2020. *Polisen och hybrida hot – Exempel-, byggstens-, och scenariosamling*. FOI-rapport i prep.

Trafikanalys 2018. *Sårbarheter i transportsystemet*. PM 2018:6

Trafikverket 2012. *Översvämningar slår ut transporterna. Rapport från Norrlandsstudien 2012*. Samverkansområdet transporter.

Trafikverket 2013. *Hur gör vi när hjulen slutar rulla? Rapport från Mötesplats transporter 2013*

Trafikverket 2014. *Att hantera kriser i ett gränslöst Norden. Rapport från Nordisk trafiksamverkan inom krisberedskapen 2014*.

Trafikverket 2017. *Särskild redovisning om krisberedskap och totalförsvar – Underlagsrapport till Nationell plan för transportsystemet 2018-2029*. 2017:166

Trafikverkets webbsida om TP SAMS: https://www.trafikverket.se/for-dig-i-branschen/samarbete-med-branschen/transportsektorns-samverkan-infor-samhallsstorningar-tp-sams/ (åtkomst 2020-11-27)

Trafikverket, Transportstyrelsen, Luftfartsverket och Sjöfartsverket 2019. *Redovisning av regeringsuppdrag till bevakningsansvariga myndigheter att inkomma med underlag för den fortsatta inriktningen av det civila försvaret – Gemensamt svar för transportområdet: Trafikverket, Transportstyrelsen, Luftfartsverket och Sjöfartsverket*.

Transportstyrelsens webbsida: www.transportstyrelsen.se/sv/Om-transportstyrelsen/fragor-och-svar/ (åtkomst 2021-01-27)

ISSN 1650-1942