



Utdragen och eskalerande gråzonsproblematik – hybridhot 2.0

Gränlandet mellan krig och fred

Dokumenttyp: Planeringsförutsättningar

Antaget av: Kommundirektören

Status: 2024-02-29

Giltighetstid: Tillsvidare



| | |
|-----------------------------------|--|
| Diarienummer: KS 2021-948 | |
| Dokumentansvarig: Anders Jolby | |
| Adresserat till: | |
| Tidpunkt för aktualitetsprövning: | |
| Tidpunkt för senaste revidering: | |
| Relaterade styrdokument: | |
| Sökord: | |



Innehåll

| | | |
|----------|--|-----------|
| 1 | Inledning | 5 |
| 2 | Bakgrund | 5 |
| 3 | Hot och hotbild | 8 |
| 4 | Planeringsförutsättningar | 11 |
| 4.1 | Situation och händelseförlopp | 12 |
| 4.2 | Förutsättningar för att värna civilbefolkningen | 15 |
| 4.3 | Förutsättningar för att säkerställa de viktigaste samhällsfunktionerna | 15 |
| 4.4 | Förutsättningar för att stödja Försvarmakten och allierade | 17 |
| 5 | Referenser | 17 |

1 Inledning

Detta dokument är planeringsförutsättningar för kommunens arbete med krisberedskap och civilt försvar. Förlagan är Totalförsvarets forskningsinstitut (FOI) hotbildsunderlag i utveckling av civilt försvar, hotbildsunderlag typfall 5¹, Säkerhetspolisens årsbok 2023-2024, MUST årsöversikt 2023, Försvarsberedningens rapport Kraftsamling DS 2023:34, Försvarsmaktens budgetunderlag för 2025, FM2023-24770:10 samt Försvarsberedningens rapport Stärkt försvarsförmåga – Sverige som allierad DS 2024:6.

Syftet med dokumentet är att öka medvetandet och kunskapen gällande det hot som gråzonsproblematiken utgör för kommunens verksamhet. Dokumentet kan även användas som underlag för övning och kontinuitetsplanering av kommunens kris- och krigsorganisation. Dokumentet hanterar ämnet generiskt och omfattas därmed inte av sekretess.

Dokumentet är ett komplement till *Linköpings kommuns planeringsförutsättningar för kommunens krigsorganisation* som utgår från hotbildsunderlag i utveckling av civilt försvar typfall 4² som är klassad begränsat hemligt och sekretessbelagd enligt OSL 15 kap. 2 §.

2 Bakgrund

Försvarsberedningen framhåller att ett väpnat angrepp mot Sverige eller våra allierade inte kan uteslutas. Det kan inte heller uteslutas att militära maktmedel eller hot om sådana kan komma att användas mot Sverige eller våra allierade.

Rysslands fullskaliga invasion av Ukraina den 24 februari 2022 innebär det mest omfattande och brutala konventionella krig Europa upplevt sedan andra världskriget. Ett krig i Europa, med potential att på kort tid eskalera ytterligare, är idag en realitet och utgör ett direkt hot mot såväl EU- och Natomedlemmar som andra länder. Därför, konstaterar Försvarsberedningen, har förutsättningarna för svensk säkerhetspolitik förändrats i grunden. Ett aggressivt Ryssland, med såväl förmåga som vilja att föra krig under lång tid, ska således utgöra den huvudsakliga dimensioneringsgrunden för utvecklingen av det svenska totalförsvaret. Försvarsberedningen framhåller att det inte är den troligaste händelseutvecklingen som är viktigast i relation till uppgiften att dimensionera totalförsvaret, utan de händelseutvecklingar som skulle få allvarliga konsekvenser om de inträffade.

Natomedlemskapet ökar säkerheten för Sverige och stärker Nato som helhet och innebär att Sverige har ingått ömsesidigt bindande försvarsåtaganden. Sveriges försvarsförmåga utgör enligt artikel 3 i nordatlantiska fördraget en del i det kollektiva försvaret. Natomedlemskapet medför även i övrigt långtgående politiska och praktiska konsekvenser för Sverige. Den nationella

¹ FOI Memo 6338

² FOI Memo 5089

totalförsvarsförmågan ska inriktas mot att enskilt och med allierade försvara Sverige och våra allierade mot väpnat angrepp. Förberedelserna, beredskapen och förmågan inom hela totalförsvaret, både det militära och det civila försvaret, måste därför öka skyndsamt. Insikten om detta behöver genomsyra alla delar av samhället och vara den främsta drivkraften för utvecklingen av totalförsvarets samlade förmåga de kommande åren.

Begreppet gråzon beskrivs som tillståndet mellan fred och krig där stater eller andra aktörer försöker påverka ett lands intressen, handlingsfrihet och förmåga i syfte att stärka sina egna intressen. I internationella sammanhang används även begreppet hybridhot eller skymningsläge.

Stater använder sig i större utsträckning av olika typer av antagonistiskt agerande som kan användas i stället för, i kombination med eller som förberedelse till militärt våld. Maktmedel såsom otillbörlig informationspåverkan, desinformation, politiska påverkansoperationer, ekonomiska åtgärder, cyberangrepp, illegal underrättelseinhämtning, utnyttjande av juridiska sårbarheter samt fysiskt sabotage används för att påverka andra staters politik och samhällen. Detta gör det svårt att dra en gräns mellan inre och yttre säkerhet samt mellan militära och icke-militära hot. Ofta kan det vara en kombination av olika aktiviteter. De kan ske öppet eller dolt. Aktiviteterna kan vara del i krigsförberedelser, men utförs i väsentligt högre utsträckning lågintensivt i fredstid och är därmed något som samhället måste kunna hantera även utan särskilda beslut om höjd beredskap. Angriparens mål är att främja sina intressen. Syftet kan också vara att testa, öva eller demonstrera vissa förmågor. Tillvägagångssättet som sådant har funnits i alla tider. Det som utmärker vår tid är att den samhällsliga och tekniska utvecklingen har skapat nya sårbarheter och därmed även nya angreppspunkter.

Försvarsberedningen konstaterar i sin rapport Kraftsamling att en mängd maktmedel används i dagens säkerhetspolitiska kriser och konflikter. Det kullkastar delvis antagandet om en tydlig eskalationstrappa med möjlighet till stegvis förstärkning av försvaret under längre tid. Den ryska fullskaliga invasionen av Ukraina visar också att en eskalering kan vara svår att bryta när beslut om angrepp väl fattats. Den ryska ledningen hade sannolikt planerat, förberett och beslutat den fullskaliga invasionen långt innan genomförandet.

EU har under de senaste åren utvecklat och vidtagit en rad viktiga åtgärder för att förbättra unionens förmåga att möta kriser och stärka motståndskraften. Inom Nato benämns motståndskraft (resilience) som ett nationellt ansvar och ett kollektivt åtagande. Nato konstaterar att nationell och kollektiv motståndskraft är centralt för trovärdigheten i alliansens avskräckning och försvar. Varje allierads individuella åtgärder för att upprätthålla och stärka den civila motståndskraften reducerar sårbarheten hos alliansen som helhet och höjer tröskeln för en angripare. Natos stats- och regeringschefer har upprepade gånger betonat att varje allierad måste vara tillräckligt robust och anpassningsbar för att hantera kriser som alliansen planerar att möta.

Inom Nato har de civila åtgärderna och förberedelserna (civil preparedness) inriktats mot tre kritiska funktioner:

- förmågan att upprätthålla politiskt beslutsfattande och centrala ledningsfunktioner,
- säkerställandet av viktiga samhällsfunktioner och
- civilt stöd till militära operationer.

Dessa tre kritiska funktioner har brutits ner i sju grundkrav (Baseline Requirements) för nationell motståndskraft mot vilka de allierade kan mäta sina åtgärder. Dessa är:

- 1) säkerställande av politiskt beslutsfattande och centrala ledningsfunktioner,
- 2) robust energiförsörjning,
- 3) effektiv hantering av okontrollerade befolkningsrörelser,
- 4) robusta system för livsmedels- och dricksvattenförsörjning,
- 5) hantering av masskadeutfall,
- 6) motståndskraftiga civila kommunikationssystem och
- 7) robusta transportsystem.

En totalförsvarsplanering för krig kommer även att förbättra möjligheterna att förebygga och hantera kriser och hybridangrepp i fredstid. Det samlade totalförsvaret ska också stödja Natos gemensamma operationer inklusive lämna nödvändigt stöd till allierade stridskrafter som baseras på, transporteras genom eller försörjs via svenskt territorium. Sverige blir ett viktigt bas-, logistik och uppmarschområde för Nato. Konkreta militära åtgärder, inom ramen för Natos kollektiva försvar, tar av geografiska och andra rent praktiska orsaker tid även då de är en del i den gemensamma operationsplaneringen. Det kan gå relativt snabbt att förstärka de allierade styrkor som redan i fredstid finns i ett operationsområde med flygstridskrafter. Marinstridskrafter tar troligen längre tid och arméstridskrafter tar längst tid att få på plats i relevant omfattning. Undantaget är de amerikanska förband som har förhandslagrad materiel i till exempel Norge. För dessa styrkor handlar det om dagar till veckor. Med Sverige som allierad blir också Natos och enskilda allierades försörjningsvägar genom landet viktiga. Sverige kommer till exempel att vara centralt för att säkerställa Finlands försörjning och för att säkerställa försörjningen av allierade förband i Finland. Det gäller såväl land- som luft- och sjötransporter. Försörjningen av Norge och Baltikum kan till del också förväntas gå via Sverige.

De svenska beredskapsåtgärderna blir delar i EU:s och Natos samlade beredskapsåtgärder. Därför kan de svenska åtgärderna för att trygga till exempel försörjningen inte bara ses i ett nationellt perspektiv. Det behöver också inkludera hur humanitärt och annat civilt stöd kan tas emot för att skydda civilbefolkningen och samhällets funktionalitet.

Inför och under ett krig ställs stora krav på beslutsfattande och agerande. Med ryktesspridning, motsägelsefull information, vilseledning och överraskning strävar angriparen efter att skapa en situation där beslut om motåtgärder försenas eller uteblir. Ett särskilt problem är behovet av

underrättelsebedömningar, tidig förvarning och förmåga att hantera de negativa effekter som uppstår bland annat vid falsklarm eller vilseledning. Det ställer bland annat krav på tydliga beslutsvägar och mandat för att möjliggöra tidiga beslut om beredskapshöjning och andra motåtgärder. Beslut måste kunna fattas även när läget är oklart. Vid krishantering är det ofta bättre att agera tidigt och kraftfullt, även med ett ofullständigt beslutsunderlag, även om det senare visar sig vara mindre allvarligt än vad man initialt bedömde. Det ställer också krav på att den ordinarie verksamheten kan möta antagonistiska hot i fredstid innan beslut om beredskapshöjande åtgärder tagits.

I formell och juridisk mening råder fred under gråzonstiden. För att mobilisera försvarsmakten och övriga delar av totalförsvaret krävs regeringens beslut om höjd beredskap. Detta sker först om ”Sverige är i krigsfara eller om det råder utomordentliga förhållanden pga. krig utanför Sverige eller att Sverige varit i krig eller krigsfara.”³ Således ska gråzonsproblematiken kunna hanteras av den fredstida krisorganisationen. Gråzonsproblematiken eller hybridkrigföringen kvarstår även under höjd beredskap och kan då hanteras med andra motmedel då ett särskilt regelverk för civilt försvar aktiveras.

3 Hot och hotbild

När man planerar motåtgärder och övar för att kunna möta gråzonsproblematiken är begreppen hot och hotbild centrala. Båda begreppen är avgörande för hur man ska förbereda och anpassa sin egen förmåga att hantera problematiken. En antagonists hot utgörs av dess avsikt och förmåga. Det vill säga både dess *vilja* och *kunnande*. *Vill* man mycket men inte har *kunnandet* är hotet litet, detsamma gäller om man *kan* mycket men inte *vill*. Däremot om man både *kan* och *vill* är hotet stort. Begreppet hotbild definieras som en möjlig händelseorienterad framtidsbild och används som ett strategiskt beslut- och planeringsunderlag.

I Säkerhetspolisens (Säpo) årsbok 2023-2024 pekas framför allt Ryssland men också Kina och Iran ut som de största hoten mot Sverige. Länder som verkar, och till viss del samverkar, för att förändra den nuvarande säkerhetsordningen. Intresset för nya områden ökar hos främmande makt. Arktis är ett exempel, vars råvaror och strategiska position påverkar svenska intressen. Samtidigt får en tilltagande kapprustning och militarisering av rymden även konsekvenser för Sverige då stora delar av säkerhetskänsliga och samhällsviktiga verksamheter är beroende av rymdtjänster. Den snabba tekniska utvecklingen, inte minst inom artificiell intelligens, AI, medför möjligheter men också att nya hot och sårbarheter uppstår.

I den Militära underrättelsetjänstens (Must) årsöversikt för 2023 framgår att Ryssland alltjämt är den säkerhetshotande aktör som Försvarsmakten dimensionerar sin verksamhet utifrån. Ryssland har en operativ militär planering som innefattar Sverige och närområdet, vilket gör att rysk underrättelseverksamhet riktas mot stora delar av Försvarsmakten,

³ Lag (1992:1403) om totalförsvaret och höjd beredskap

totalförsvaret och försvarsindustrin. Den svenska planeringen inför Natomedlemskapet samt svenskt och västerländskt stöd till Ukraina är också prioriterade mål för inhämtning. Dessutom riktas underrättelseverksamhet mot civila förmågor och civil infrastruktur som Försvarsmakten är beroende av.

Rysk doktrin lägger stor vikt vid att underblåsa sociala konflikter och oro som ett sätt att bedriva subversion. Troligen finns en långsiktig rysk strategi att påverka opinionen i Väst och i förlängningen minska den politiska viljan att stödja Ukraina. Ryssland genomför också löpande aktiviteter för att skapa förutsättningar för att vid behov kunna genomföra sabotage, med egna resurser eller via ombud eller agenter. Det handlar om underrättelseinhämtning, etablering av stödjepunkter och rekrytering av potentiella ombud för att möjliggöra sabotage vid ett senare tillfälle. I detta ingår även att utveckla förmågan att genomföra cyberattacker. Det ligger i ryskt intresse att aktivt motverka västligt stöd till Ukraina, där sabotage är ett möjligt verktyg.

Som en effekt av kriget i Ukraina har kontakterna mellan Kina och Ryssland fördjupats, inte minst ekonomiskt och politiskt, samtidigt som det ryska ökade beroendet av Kina skapar förutsättningar för det kinesiska kommunistpartiet att flytta fram sina positioner inom områden som berör Sveriges närområde och intressen. För att nå målsättningarna om en globalt ledande roll nyttjar partiet en stor bredd av öppna och dolda maktmedel för att påverka andra länder och det internationella systemet. Svensk innovationskraft är av intresse för Kina. Landet tar till sig utländsk högteknologi bland annat genom strategiska uppköp och forskningssamarbeten. Kinas kommunistiska parti (KKP) kartlägger och försöker påverka svensk åsikts- och opinionsbildning samt bedriver olovlig underrättelseverksamhet. I Sveriges närområde har Kina även strategiska intressen kopplade till bland annat Arktis och rymdindustri. Kina har också en väl utvecklad cyberförmåga som används mot både militära och civila mål.

Försvarsberedningen konstaterar att rysk planering och förberedelser för ett anfall mot Sverige pågår redan idag. Det innebär dock inte nödvändigtvis att det finns en avsikt att genomföra ett anfall på Sverige. Genom planeringen och förberedelserna skapar Ryssland en möjlighet, en option, att anfälla Sverige och alliansen om de egna strategiska intressena i en given säkerhetspolitisk situation, enligt deras bedömning, skulle kräva det. En sådan situation skulle manifesteras i en större säkerhetspolitisk kris. En allvarlig säkerhetspolitiska kris kan ha ett långvarigt förlopp, kanske över flera år, eller vara mycket hastig under dagar till veckor.

Ryssland använder sig i stor utsträckning av olika typer av antagonistiskt agerande som kan användas i stället för, i kombination med eller som förberedelse för militärt våld. Ett väpnat angrepp kan föregås av att en angripare under kortare eller längre tid genomför upptrappad aktiv, ofta subversiv, hybridverksamhet utan att utlösa ett krigstillstånd. Användandet av allt för kraftiga hybrida aktiviteter riktade mot någon eller flera av Natos medlemsstater måste dock vägas mot risken för Natos samlade motåtgärder inklusive militära beredskapshöjningar. Vilseledning är därför också ett viktigt

instrument även i hybridoperationer i fredstid. Tidiga och tydliga indikationer på angreppsförberedelser i fredstid är viktigt för vår möjlighet att besluta om motåtgärder. Underrättelsebedömningen kan bidra till att skapa förutsättningar för att tidigt kunna fatta nödvändiga beslut rörande olika former av motåtgärder och beredskapshöjningar. Detta skulle kunna bidra till att det handlingsutrymme angriparen skapat med de hybrida aktiviteterna minskar och ytterst begränsar möjligheterna att framgångsrikt genomföra en militär operation. Tydliga beredskapshöjande åtgärder i ett tidigt skede skulle även kunna förhindra ett angrepp genom att göra operationen för kostsam och allvarligt försvåra möjligheten att uppnå de målsättningar som satts.

Underrättelseinhämtning genom tekniska hjälpmedel är ett allvarligt hot mot svenska säkerhetsintressen. Den information som eftersöks finns ofta lagrad digitalt vilket gör att teknisk inhämtning, som både är personal- och kostnadseffektiv, kan användas. Det går dock att försvåra motståndarens möjligheter till inhämtning genom att följa säkerhetsföreskrifterna och genom noggranna säkerhetskontroller av personal och system. En trend inom cyberområdet är att utnyttja svagheter i leverantörskedjorna och på så vis komma åt information. Därför är det viktigt att alla som hanterar skyddsvärd information ser till att informationsägare i alla led säkrar upp sina system.

De flesta stater är i dag beroende av satellittjänster, exempelvis för väderprognoser och klimatforskning, för positionering, navigering och tidshållning, men även för vissa militära- och samhällskritiska funktioner. Därför kan bortfall av satellittjänster leda till kumulativa effekter som kan påverka både samhällets robusthet och staters militära förmåga, vilket i förlängningen kan skaka maktdynamiken i det internationella systemet. Infrastruktur för rymdverksamhet, på marken, i rymden samt kommunikationen dem emellan, betraktas därför allt oftare som kritisk infrastruktur i behov av skydd. Ett förstörande angrepp kan få långtgående konsekvenser för samhällsviktig verksamhet och ett flertal länder har uppvisat förmåga att slå ut satelliter via robotangrepp. Det finns även risk för förstörande cyberangrepp mot satelliter vilket till exempel kan innebära läckage av stulen information eller att satelliten som sådan förstörs.

Från ett hotperspektiv kommer främmande makt att stå för den mest avancerade och sofistikerade användningen av AI-modeller. Men även andra aktörer har visat prov på användning av sådana verktyg. Genom AI sänks trösklarna och höjs lägstanivån ytterligare. Aktörer som idag har en låg förmåga kan med relativt enkla medel höja den och utföra mer komplexa handlingar, exempelvis få tillgång till instruktioner, få hjälp med att utföra cyberangrepp och sprida desinformation.

Utöver en bred utveckling av redan existerande förmågor kan AI även innebära hot som förfalskade bilder, videor eller ljud, nyttjande av självkörande fordon och fiendlig maskininlärning. AI-verktyg kan också användas för att förbättra och automatisera förmågan att utföra cyberangrepp. Användning av AI-verktyg för att producera och sprida innehåll i informationspåverkanssyfte är ett av de mest uppmärksammade och omskrivna sätten som hotaktörer kan nyttja AI på. En kraftig ökning av social mediemanipulering, desinformation och allmänt

icke-autentiskt material på digitala plattformar kan göra det svårt att säkerställa trovärdigheten i den information som ges. Det finns redan exempel på hur främmande makt och våldsbejakande extremister använder AI för att generera propaganda- och påverkansmaterial. Denna typ av förmåga kan innebära ett hot mot enskilda beslutsfattares integritet och säkerhet, liksom ett bredare hot mot demokratin, i den mån allmänhetens förtroende för politiska företrädare och processer tar skada.

Försvarsberedningen anser att förmågan att genomföra defensiva och offensiva cyberoperationer samt förmågan att upptäcka, identifiera och avvärja cyberhot mot svenska intressen är av central vikt för hela totalförsvaret.

Försvarsberedningens rapport Kraftsamling konstaterar beredningen att statliga eller statsunderstödda aktörer har både kompetens och resurser för att genomföra kvalificerade it-intrång. Flera statsaktörer har byggt upp avsevärda förmågor i syfte att kunna verka offensivt genom bland annat cyberattacker. Även enskilda aktörer har visat vilja och förmåga att orsaka skada. FRA:s, Musts och Säpos erfarenheter visar att främmande makt har både avsikt och förmåga att utföra cyberangrepp som kan skada centrala samhällsfunktioner.

Försvarsberedningen bedömer att effekterna av ett cyberangrepp kan få lika stora konsekvenser för samhällsviktiga funktioner och kritiska it-system som ett konventionellt väpnat angrepp. Ett cyberangrepp kan därför i vissa fall vara att betrakta som ett väpnat angrepp.

Nato har aviserat att cyberangrepp under vissa förutsättningar kan likställas med ett väpnat angrepp och leda till att artikel 5 om kollektivt försvar kan åberopas. Nato konstaterar även att svagheter inom cyberområdet hos en allierad kan drabba andra allierade och betonar därför att samtliga allierade ska stärka sin cyberförsvarsförmåga.

4 Planeringsförutsättningar

Kapitel 4 bygger på beskrivningar i FOI Memo 6338 – Typfall 5: Utdragen och eskalerande gråzonsproblematik samt ÖB:s typfall hämtade ur ÖB Budgetunderlag för 2025 från 2024-03-01

Det råder en ansträngd säkerhetspolitisk situation i närområdet men det föreligger inledningsvis inget direkt konkret militärt hot mot Nato eller Sverige som motiverar höjd beredskap. De inledande händelserna innebär en rad utmaningar för samhället men utgör också en larmklocka för den svenska regeringen och Försvarsmakten inför en möjlig eskalation. Händelseförloppet är tämligen utdraget i tid och de säkerhetspolitiska spänningarna i närområdet ökar över tiden för att i scenariots avslutande faser inbegripa begränsade stridshandlingar i något av de nordisk-baltiska grannländerna.

Både regeringen och myndigheter, liksom allmänheten, utsätts för direkta påfrestningar via påverkade samhällsfunktioner, liksom informationspåverkan, samtidigt som det initialt är oklart vad det egentligen är som sker. Antagonistens syfte med aktiviteterna är också oklara, åtminstone

inledningsvis. Givet att den säkerhetspolitiska situationen är ansträngd och eskalerar mot en eventuell regional konflikt skulle syftet exempelvis kunna vara att lamslå svenskt beslutsfattande, att bryta ner den svenska försvarsviljan, att få Sverige att avbryta bilaterala och internationella militära samarbeten, att förhindra att Sverige tar emot och ger stöd till allierade förband samt att skapa handlingsutrymme för ett militärt ingripande mot Sverige eller något nordiskt-baltiskt grannland. De parallella utmaningarna att hantera störningar, klargöra läget, återställa samhällsfunktionalitet, stödja och skydda allierade förband med värdlandsstöd samt mildra de negativa effekterna av störningarna, liksom att förstå antagonistens mål, karaktäriserar denna typ av scenario.

4.1 Situation och händelseförlopp

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 cyberangrepp och fysiska sabotage på samhällsfunktioner där man försöker dölja spåren och/eller rikta misstankarna åt annat håll. Angreppen förefaller ske främst mot ”låg hängande frukter” såsom lokala försörjningssystem samt enstaka samhällsaktörer och företag, men även mot elförsörjning och telekommunikationer inom och mellan länder.

Förekomsten av förvrängd information och korrupta data i system som används av beslutsfattare, operatörer och specialister inom en rad samhällssektorer ökar, vilket tyder på avancerade dataintrång. Påverkan på samhällets funktionalitet är begränsad men bland allmänheten sprider sig ändå viss oro. Spridandet av propaganda via internetaktiviteter och alternativa medier, som sedan ibland oreflekterat sprids vidare i svenska traditionella medier, förmedlar en skev bild av Sverige.

Den svenska allmänheten utsätts för mångtydiga fakta och ibland ren desinformation i frågor som berör bl.a. ordning och trygghet, migration och integration, traditionella värderingar, krisberedskap och försvar samt utrikes- och säkerhetspolitik. Dessa informationsoperationer, som i första hand utnyttjar vårt öppna samhälles informationsinfrastruktur i termer av internets sociala medier och bloggar, liksom indirekt TV, radio och tidningar, får negativ påverkan på allmänhetens förtroende för myndigheter och politiker.

Främmande makts underrättelseverksamhet i Sverige och dess grannländer ökar. Det gör även en allt mer konfrontativ diplomatisk retorik i kombination med spridning av propaganda via statskontrollerade medier. 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.

Försörjningslinjerna störs vilket påverkar tillförseln av varor. Sabotage mot järnvägslinjer i norra Sverige hindrar exporten av järnmalm. Myndighetsbeslut drar ut på tiden pga. försvårad informationsdelning beroende på störda IT-system. 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. Primärvården belastas av lokala utbrott av magsjuka. Räddningstjänsten belastas av en ökning av bränder pga. att människor använder uttjänta eldstäder samt lagar mat över öppen eld på exempelvis balkonger, när värme- och elsystem fallerar. Polisen belastas av ökade ordningsstörningar och ökad gängkriminalitet liksom av alltmer våldsamma uppgörelser mellan olika gäng som helt plötsligt förefaller blivit tyngre beväpnade. Vidare kan en markant ökning av den organiserade brottslighetens aktiviteter på den ekonomiska arenan konstateras, såsom bidragsfusk, skattebrott och penningtvätt. Särskilt drabbad är bank- och finanssektorn som utsätts för cyberrelaterade utpressningsförsök via s.k. ransomwareattacker.

Ett falskt pressmeddelande som ser ut att komma från Säkerhetspolisen, avseende ökat terrorhot mot Sverige, får stor spridning i sociala medier. Dessutom förekommer motsvarande inlägg på sociala medier som kan tolkas som att de kommer från pålitliga källor såsom Sveriges Radio och Krisinformation.se. Detta skapar oro och förvirring och tar myndigheternas kommunikationsresurser i anspråk.

När den ansträngda situationen har varat i ungefär ett halvår blir främmande makts diplomatiska utspel allt mer aggressiva med indirekta hot om militärt våld. Påverkansoperationer på den internationella nivån intensifieras för att förhindra en gemensam hållning, främst inom EU. Denna påverkan sker bl.a. via diplomatiska framstötter, ekonomiskt bistånd, fördelaktiga handelsavtal, hot om indragna energileveranser och personliga kontakter. Sverige och de nordisk-baltiska grannländerna vill gemensamt med EU peka ut och vidta sanktionsåtgärder mot antagonisten men EU är politiskt splittrat.

Nato etablerar ledningsresurser och basområden för flyg på svenskt territorium, bland annat berörs Norrköping och Linköping. Sverige tillhandahåller värdlandsstöd i form av exempelvis transport och logistiktjänster (livsmedel, drivmedel, sjukvård, infrastruktur, etc.) samt skydd. Förstärkning av förband i Finland och på Nordkalotten innebär att allierade logistikflöden och transporter genom svenskt territorium, på land och till sjöss ska skyddas.

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 pga. höjda försäkringspremier. Produktionen i viss tillverknings- och förädlingsindustri har dock redan stagnerat pga. 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 följeffekter 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. Därtill är det osäkert om hela VMA-systemet fungerar som planerat. Försök till påtryckningar mot olika beslutsfattare ökar via e post, brev och hembesök. Här drabbas inte bara myndighetspersoner utan även nyckelpersonal inom privat samhällsviktig verksamhet. Företag med leveransavtal med Försvarmakten förefaller vara hårdast drabbat av hot om våld och sabotage. Det rapporteras från ett nordiskt-baltiskt grannland om sociala oroligheter mellan olika etniska grupper samt att några slags beväpnade lokala miliser gör sporadiska angrepp mot myndighetskontor och polisen.

Samtidigt ökar främmande makts militära övningsverksamhet och omdispositioner i närområdet, liksom kränkningar av svenskt luftrum och sjöterritorium. 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. Solidariteten med andra i närmiljön är dock stor och många människor hjälper varandra i denna ansträngda situation medan andra inriktar sig på att skydda sina egna resurser, med våld om så är nödvändigt. 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 Försvarmakten och dess utländska samarbetspartners. Upplopp och plundring förekommer i flera svenska städer.

Vaga nyhetsrapporter, samt en flodvåg av tvetydig information på sociala medier, om stridshandlingar i det nordiskt-baltiska grannlandet når den oroliga svenska allmänheten och de utarbetade svenska beslutsfattarna. Främmande makt varnar den svenska regeringen för att besluta om höjd beredskap, och därigenom ytterligare öka spänningen i närområdet.

4.2 Förutsättningar för att värna civilbefolkningen

Trots att de inledande händelsernas påverkan på samhällets funktionalitet är begränsad finns risk för att oro och rädsla breder ut sig, vilket exempelvis kan öka sjukfrånvaron. Informationskampanjer, desinformation, falska meddelanden och annan psykologisk påverkan kan i sin tur påverka allmänhetens förtroende för samhällets styrning och därmed försvarsviljan.

Ökningen av olyckor påverkar direkt civilbefolkningen men ökar också arbetsbelastningen för polis, räddningstjänst och akutsjukvård, vilket indirekt minskar möjligheten att värna civilbefolkningen.

Störningar i el- och värmesystem som inträffar under de kalla årstiderna kan ha direkt påverkan på civilbefolkningens hälsa. Behov av evakuering av särskilt utsatta kan behövas. Elavbrott i kombination med störningar i leveransen av reservkraftsbränsle påverkar exempelvis sjukvård och avloppsrening, vilket också kan drabba civilbefolkningens hälsa. Avsaknad av varmvatten kan medföra sämre hygien och därmed ökad risk för smittspridning och eventuella sjukdomsutbrott.

Störningar i betalningssystemen påverkar människors möjligheter att anskaffa förnödenheter och därmed deras fysiska hälsa. Om det inte är möjligt att anskaffa förnödenheter på normal väg kan snatterier, småstöldar och inbrott komma att öka. Detta kan till viss del direkt drabba civilbefolkningen men också arbetsbördan för ordningsmakten, vilket i sin tur indirekt kan påverka möjligheterna att värna civilbefolkningens säkerhet.

Störningar som drabbar data- och telekommunikationer skapar följd effekter som direkt kan påverka människors hälsa, exempelvis att läkemedel inte går att hämta ut. Om det inte går att nå ut med VMA kan det innebära allvarliga fysiska risker för civilbefolkningen. Där spelar bl.a. mediesektorns funktionalitet en viktig roll. Mediernas förmåga att nå ut med saklig och opartisk information är överhuvudtaget en viktig beståndsdel i det psykologiska försvaret. Begränsad möjlighet till pålitlig nyhetsförmedling kan skapa oro och otrygghet, öka ryktesspridning samt öka möjligheten att medvetet sprida falsk information. En annan viktig del i ett psykologiskt försvar är att identifiera, analysera och möta informationskampanjer, vilket försvåras av störningar i informationsinfrastrukturen. Å andra sidan försämras då även möjligheten att iscensätta informationskampanjer och sprida falsk information. I typfallets senare eskalerade faser med stora störningar på nationell infrastruktur, akut livsmedelsbrist och förekomst av våldsbrott finns uppenbara risker för civilbefolkningens fysiska välmående.

4.3 Förutsättningar för att säkerställa de viktigaste samhällsfunktionerna

Även om samhällets funktionalitet tekniskt sett endast marginellt påverkas i förloppets inledning så kan den påverkas om människor pga. oro och rädsla sjukskriver sig eller uteblir från jobbet. Även mindre störningar i lokal och regional elförsörjning, liksom i data- och telekomsystemen, bidrar till förstärkta störningar i andra system, exempelvis livsmedelsförsörjningen,

betalningssystemen, vatten- och avloppssystemen, fjärrvärmens och transportlogistiksystemen, som i sin tur får ytterligare spridningseffekter. Ett exempel är elavbrott som medför att tankstationer inte fungerar, vilket efter kort tid försvårar transporter av exempelvis livsmedel, postförsändelser, reservdelar, sjukvårdsmateriel och personal.

Även samhällsfunktioner med reservkraft kan påverkas av mindre men återkommande elavbrott om nytt bränsle inte hinner fyllas på i tid innan nästa elavbrott uppstår. Det kan exempelvis gälla avloppsreningsverk, trafikledningscentraler, sjukhus, jordbruksanläggningar och lager i livsmedelskedjan.

Större störningar som drabbar nationell elförsörjning samt data- och telekommunikation kan skapa omfattande följd effekter i en rad sektorer. Det kan exempelvis gälla det elektroniska recepthanteringssystemet för utskrivna läkemedel, bankers internetservicefunktioner, livsmedelskedjornas beställningssystem och lagersaldon, den spårbundna kollektivtrafikens signalsystem samt informations- och nyhetsförmedlingen. Även begränsningar av importflödena till Sverige får svåröverskådliga följd effekter eftersom detta inte bara omfattar färdiga produkter utan även insatsvaror till exempelvis livsmedels- och tillverkningsindustrin samt inte minst reservdelar och underhålls- och reparationsmateriel.

Att hantera stora infrastrukturella störningar samt att återställa funktionalitet är en utmaning oavsett händelseförlopp. Sådana insatser måste kunna ledas och försörjas med materiella resurser samt kompetens och arbetskraft. Till skillnad från vid en ”naturlig” kris kan en antagonist på olika sätt försöka att ytterligare försvåra hanterings- och återställningsarbete, exempelvis genom att störa ledningsfunktioner.

Vissa uppgifter som åläggs polis, räddningstjänst och akutsjukvård kan komma att nedprioriteras om dessa aktörer överbelastas av kraftig ökning av olyckor. I ett skede där särskilt utsatta människor är i behov av extra resurser från redan hårt belastad kommunal vård- och omsorgspersonal kan andra kommunala funktioner komma att nedprioriteras.

Desinformation som måste dementeras tar myndigheternas resurser i anspråk och undergräver också myndigheternas trovärdighet i att kommunicera läget framöver, då en faktisk höjning av hotnivån kan bli aktuell. Att nå ut med korrekt och saklig information kan i sin tur mildra indirekta effekter av störningar, exempelvis hamstring av livsmedel och drivmedel. Påverkan och påtryckningar mot beslutsfattare inom privat samhällsviktig verksamhet kan exempelvis beröra godstransporter, apotek och läkemedelstillverkning, banker, energi, mobiltelefoni och internet, dagligvaruhandel samt privat hälso- och sjukvård.

Oavsett anledning till eventuella sjukdomsutbrott drabbas indirekt samhällets funktionalitet av sjukfrånvaro då samhällsfunktioner blir underbemannade.

Bemanningen av samhällsviktiga funktioner försvåras också om människor som tillhör resursstarka grupper, med hänsyn till sin egen och sina familjers säkerhet, väljer att lämna sina boendeorter eller resa utomlands.

4.4 Förutsättningar för att stödja Försvarmakten och allierade

Det bör noteras att eftersom det inte råder höjd beredskap i detta typfall är det kanske i första läget så att det förväntas att Försvarmakten ska stödja krisberedskapen och det civila samhället, snarare än att Försvarmakten ska motta stöd. Försvarmaktens stöd till det civila samhället kan exempelvis handla om flygtransporter av reservdelar och reparationsmateriel för återställning av infrastruktur eller att hemvärnsförband bistår polis och räddningstjänst. Försvarmaktens stöd till samhället måste hela tiden vägas mot utförandet av de egna uppgifterna och detta kan leda till behov av samordning mellan militära och civila resurser.

Det är rimligt att anta att det i typfallets senare eskalerade delar börjar förberedas för eventuell höjd beredskap och därmed också det civila samhällets stöd till Försvarmakten och allierade förband (värdlandsstöd).

Upprätthållandet av Försvarmaktens och allierade förbands förmågor är beroende av tjänster som produceras i civila sektorer. Det handlar bland annat om el, drivmedel, transporter av personal och materiel, tele- och datakommunikationer, livsmedel, läkemedel och sjukvård, samt finansiella tjänster. Dessa sektorer bemannas av människor ur civilbefolkningen, vars relativa välmående och möjligheter att ta sig till sina arbetsplatser och där kunna utföra sina arbeten är förutsättningar för att stöd till Försvarmakten och våra allierade ska kunna ges alt. erbjudas.

Fysiska störningar och angrepp mot dessa samhällsfunktioner, liksom eventuell underbemanning, påverkar givetvis möjligheten för det civila samhället att tillgodose Försvarmaktens behov. Även påtryckningar och hot mot privata aktörer med leveransavtal mot Försvarmakten kan både direkt och indirekt påverka dessa aktörers förmåga att stödja Försvarmakten.

5 Referenser

- Försvarsberedningens rapport *Kraftsamling*, DS 2023:34
- Försvarsberedningens rapport *Stärkt försvarsförmåga – Sverige som allierad*, DS 2024:6
- FOI Memo 6338
- FOI Memo 4769
- Säkerhetspolisens årsbok 2023-2024
- Militära underrättelsetjänstens årsöversikt 2023
- Försvarmaktens budgetunderlag för 2025, FM2023-24770:10