# Digitaliseringens fallgropar i gråzon och krig

Johan Bengtsson, Karin Mossberg Sonnek,
Vidar Hedtjärn Swaling

FOI-R--5522--SE

Januari 2024

FOI

Johan Bengtsson, Karin Mossberg Sonnek,
Vidar Hedtjärn Swaling

# Digitaliseringens fallgropar i gråzon och krig

| | |
|---|---|
| Titel | Digitaliseringens fallgropar i gråzon och krig |
| Title | The pitfalls of digital transformation in gray zone and war |
| Rapportnr/Report no | FOI-R--5522--SE |
| Månad/Month | Januari / January |
| Utgivningsår/Year | 2024 |
| Antal sidor/Pages | 66 |
| ISSN | 1650-1942 |
| Uppdragsgivare/Client | Försvarsdepartementet |
| Forskningsområde | Krisberedskap och civilt försvar |
| FoT-område | Inget FoT-område |
| Projektnr/Project no | A123205 |
| Godkänd av/Approved by | Malek Finn Khan |
| Ansvarig avdelning | Försvarsanalys |

Bild/Cover: Everett Collection Inc / Shutterstock

# Sammanfattning

Digitaliseringen inom samhällsviktiga verksamheter har pågått under en längre tid. Syftet har främst varit effektivisering och kostnadsbesparingar, men också att underlätta för anställda inom verksamheterna och för medborgare som tar del av verksamheternas tjänster. Digitaliseringen har många positiva följder, men innebär även utmaningar. Studier och utredningar har visat att exempelvis snabba teknikskiften, omogen teknik, avsaknad av nationell samordning samt bristfällig beställarkompetens gör att sårbarheter byggs in i IT-systemen. Detta är sårbarheter som kan utnyttjas av antagonister i en gråzon eller under ett krig för att förstöra IT-systemen, manipulera data eller sprida desinformation.

I denna studie har vi sammanställt problem med digitaliseringen som har identifierats i tidigare FOI-studier. Vi för en diskussion kring hur problemens karaktär kan ändras när fred övergår till gråzon eller krig. Utgångspunkten är att IT-systemen då i en högre grad blir utsatta för antagonistiska angrepp av en statsaktör eller dennes ombud. Vi presenterar också 15 fallgropar som representerar förhållanden som i fredstid är funktionella men som skapar problem i gråzon och krig. Sammanställningen av problem och fallgropar kan tjäna som ett underlag för beredskapsplanerare inom samhällsviktiga verksamheter i arbetet med att förbereda verksamheter att kunna fortgå även i gråzon och krig.

Nyckelord: Digitalisering, sårbarheter, problem, fallgrop, IT-system, gråzon, krig

# Summary

Digital transformation within vital societal functions has been going on for a long time. The aim has primarily been efficiency and cost savings, but also to make it easier for employees and for citizens who take advantage of the societal services. Digital transformation has many positive consequences, but also poses challenges. Studies and investigations have shown that, for example, rapid changes in technology, immature technology, lack of national coordination and insufficient customer competence mean that vulnerabilities are embedded into IT systems. These vulnerabilities can be exploited by antagonists in a gray zone or during a war, in order to destroy IT systems, manipulate data or spread disinformation.

In this study, we have compiled problems with digital transformation that have been identified in previous FOI studies. We discuss how the nature of the problems change when the threat level changes from peace to gray zone or war, when the IT systems are being exposed to a greater degree to antagonistic attacks by a state actor or his agent. We also present 15 pitfalls that represent conditions that are functional in peacetime but create problems in a gray zone and war. The compilation of problems and pitfalls can serve as a basis for contingency planners within vital societal functions in the work of preparing activities to be able to continue even in gray zone and war.

Keywords: Digitization, vulnerabilities, problem, pitfall, IT system, grey zone, war

# Innehåll

# 1 Inledning

Digitaliseringen rullar på snabbt i samhället och har sedan 1990-talet varit ett politiskt mål i sig. Det som förr gjordes manuellt klaras nu av med ett knapptryck på telefonen. Många minns hur det var att slå upp ett okänt ord i ett lexikon som tog några hyllmeter i bokhyllan. En del kommer också ihåg noteringshäftet som hörde till checkhäftet, i vilket man skrev ner sina uttag för hand och själv räknade ut hur mycket man hade kvar på kontot, liksom nödvändigheten att besöka Försäkringskassans kontor om man hade ett ärende dit. För dagens unga är Google det självklara valet när man undrar över något, banktransaktionerna klaras lätt av på datorn eller mobiltelefonen och det är inte tal om att passa myndigheternas öppettider, ärenden med dem klaras av digitalt, 24 timmar om dygnet.

Digitaliseringen har inte bara underlättat för oss som privatpersoner. Många samhällsviktiga verksamheter har också genomgått förändringar i och med digitaliseringen, i syfte att bli effektivare. Den smarta staden har gjort sitt intåg, och i och med det går det att placera ut mätutrustning och samla in data om exempelvis vattennivåer, trafikflöden och elförbrukning. Data analyseras och, om så behövs, skickas personal till den punkt där ett eventuellt problem behöver åtgärdas. Digitala beslutsstödsystem har blivit allt vanligare, och de hjälper såväl samhällsplanerare som läkare att fatta bättre beslut. Dialogen med medborgarna sker också i högre grad över Internet. Utöver effektiviseringen har i många fall kostnader kunnat sparas in eftersom det inte längre behövs en lika stor personalstyrka för att hålla verksamheten rullande.

Men det finns också baksidor med digitaliseringen. Tekniken är inte alltid mogen och det sker snabba teknikskiften som behöver hanteras. Ibland går digitaliseringstakten så snabbt att konstruktionsfel och säkerhetsluckor inte hinner upptäckas och åtgärdas. Dessa fel och brister blir då sårbarheter som kan leda till att IT-system angrips och blir oåtkomliga, eller till att en angripare med uppsåt manipulerar IT-systemen till att återge felaktiga värden. Under de senaste åren har en rad sådana incidenter inträffat. En annan sårbarhet är beroendet av att infrastruktur för IT-kommunikation och el fungerar, och i vissa fall även av konsulter som har rätt kompetens för att kunna designa och underhålla IT-systemen.

De digitala systemen som används av svenska aktörer fungerar för det mesta väl, även om de ibland drabbas av oönskade incidenter. Många verksamheter i Sverige har kunnat dra nytta av fördelarna som digitaliseringen har fört med sig. Men vad händer med det digitaliserade samhället om Sverige utsätts för större påfrestningar, exempelvis då vi befinner oss i en gråzon, eller rent av i krig? Är samhället tillräckligt motståndskraftigt? Vilka sårbarheter har vi byggt in som kan utnyttjas av angripare? Har digitaliseringen några fallgropar?

## 1.1 Syfte och målsättning

För att skapa en långsiktig motståndskraft i samhället är det viktigt att analysera olika samhällstrender, även de som i grunden ses som positiva, för att se om det finns sårbarheter förknippade med dem som kan utnyttjas av angripare i gråzon eller krig. Digitaliseringen är en sådan trend. Regeringskansliet har därför gett FOI i uppdrag att genomföra en studie om digitaliseringens fallgropar i gråzon och krig. Studien har genomförts inom projektet Sabek (Samhällets beredskap i kris och krig) och syftar till att förbättra förutsättningarna för att digitaliserade samhällsviktiga verksamheter ska kunna fortgå även i gråzon och i krig.

Studien har som målsättning att besvara följande frågeställningar:

1. Vilka fredstida problem har digitaliseringen i Sverige fört med sig?
2. Hur kan digitaliseringens fredstida problem uppträda i gråzon och krig?
3. Finns det några fallgropar med digitaliseringen som påverkar möjligheterna att genomföra verksamheter i gråzon och krig?

## 1.2 Fred, gråzon och krig

I rapporten presenterar vi problem som digitaliseringen har fört med sig, och som har gått att identifiera under fredstid. Vi diskuterar också hur problemen kan förväntas utvecklas i en gråzon och i krig. För att kunna följa diskussionen, om de för oss hypotetiska situationerna, måste man som läsare förstå vad vi i det här sammanhanget menar med fred, gråzon och krig.

Det finns inga allmängiltiga definitioner att falla tillbaka på, framför allt kan fred och gråzon förstås på olika sätt. Men hur olika aktörer tolkar de olika situationerna är inte heller viktigt för vår frågeställning.

Vårt syfte har varit att undersöka hur digitaliserade samhällsviktiga verksamheter klarar av kraftiga angrepp från en antagonistisk statlig aktör. Det vill säga angrepp som kan ge större påfrestningar än vad som orsakas av fredstida kriser såsom en skogsbrand, ett större elavbrott eller en hackerattack. Till vår hjälp när vi diskuterar digitaliserings problem har vi använt begreppen fred, gråzon och krig, och vi har då resonerat utifrån förhållanden som redovisas nedan.

### 1.2.1 Fred

Fred betraktas oftast som ett slags normaltillstånd, det tillstånd som råder när vi inte är i krig eller utsätts för krigsfara.[1] Även i normaltillståndet finns påfrestningar i form av kriser, som kan få negativa konsekvenser för samhällsviktiga verksamheter och för delar av befolkningen. Påfrestningarna kan ha sin grund i olyckor och naturliga förlopp som extrema väderhändelser, eller i medvetna

[1] Försvarshögskolan. 2023. Bilaga 2-5.

mänskliga handlingar. De senare kallas antagonistiska kriser och inkluderar kriminalitet, terrorism eller att enstaka personer vill skada samhället. I likhet med de antagonistiska kriserna beror även olyckor ofta på mänskliga handlingar, men dessa utförs då utan uppsåt att orsaka skada.

I fredstid råder den fredstida lagstiftningen. Det finns internationella samarbetsavtal och import och export fungerar generellt bra. Allmänheten har stor tilltro till myndigheterna och förväntar sig en hög tillgänglighet till tjänster och information. Inslaget av antagonism i fredstida krishantering är inte dominerande. I fredstid är det svenska samhället i stort robust, och har hittills klarat av att hantera kriser och återgå till ett normaltillstånd efterhand.

### 1.2.2 Gråzon

Den svenska beredskapslagstiftningen är en aning svartvit, på så vis att den drar en skarp gräns mellan fred och krig. Men i verkligheten är det är inte alltid självklart när det ena övergår till det andra. En fientligt sinnad stat kan försöka påverka Sverige även strax under tröskeln för krig, bland annat genom territoriella kränkningar eller begränsade fysiska angrepp såsom sabotage. Denna utmaning – att statlig antagonism behöver hanteras inom ramen för den fredstida lagstiftningen, med de mandat som regeringen och myndigheterna har inom dessa regelverk och under stor osäkerhet om händelseförloppet – fångas in genom begreppet *gråzon*.[2]

När vi använder begreppet gråzon i rapporten utgår vi från att det finns antagonistiska statliga aktörer som angriper Sverige. Den angripande aktören är just statlig, eller agerar på ombud av en stat, vilket skiljer sig från de antagonistiska kriser som hanteras under fredstid. Påfrestningarna kan vara stora, men når samtidigt inte en sådan omfattning att det bedöms råda krig. Angreppen riktas till största delen mot den civila delen av samhället och maskeras för att det inte tydligt ska framgå vem som står bakom dem, och i vilka syften de utförs. Angreppen kan därför framstå som olyckshändelser, eller utföras på ett sådant sätt att det är svårt att spåra vem som ligger bakom dem, alternativt att någon annan aktör framstår som skyldig.

Gråzonen präglas alltså i hög grad av osäkerhet kring vad som händer och varför.[3] Osäkerheten syftar till att förhindra den som angrips att kunna sätta in effektiva motåtgärder. Under gråzonen kan en antagonist använda sig av flera olika maktmedel. Exempel på sådana är desinformationskampanjer, cyberoperationer, strategiska uppköp, propaganda, illegal underrättelseinhämtning och sabotage.[4] I gråzonen måste konsekvenserna av dessa maktmedel istället fortfarande hanteras med hjälp av den fredstida lagstiftningen. Allmänhetens

[2] För en mer detaljerad beskrivning, se: Försvarsberedningen. (2017).
[3] Jonsson, Ingemarsdotter, Johansson, Rossbach, Wedebrand & Eriksson. 2019, s. 4.
[4] Jonsson, Eriksson, Ingemarsdotter, Rossbach & Wedebrand. 2023. s. 10.

förväntan på fungerande tjänster i samhället, och tillgänglighet till information från myndigheter, kommer inledningsvis vara på samma nivå som under fred.

### 1.2.3 Krig

Krig kan ta många olika former. När vi i rapporten resonerar om vad som kan hända i en krigssituation är utgångspunkten att det finns (åtminstone) en tydligt definierad antagonistisk statlig aktör som angriper Sverige i syfte att uppnå vissa bestämda mål. Angreppen kan genomföras både öppet och dolt med många medel, på hela skalan från vapenverkan och cyberattacker till desinformation och hot. I likhet med gråzonen kan alltså även kriget präglas av olika former av osäkerhet, men en avgörande skillnad ligger i att det råder enighet om att Sverige befinner sig i krig med en annan stat (eller flera stater) och att de påfrestningar som uppstår har sin grund i denna stats antagonism.

Det är regeringen som fattar ett formellt beslut om höjd beredskap när den anser att det råder krig eller krigsfara.[5] Då träder en speciell lagstiftning i kraft, som gör att de så kallade fullmaktslagarna kan tillämpas, vilket i sin tur gör det möjligt att snabba upp beslutsfattandet och understödja omställningen av samhället från fredstida behov till försvar av landet.[6] Regeringen kan också besluta om krigstjänstgöring för de totalförsvarspliktiga som är krigsplacerade inom det militära respektive det civila försvaret.[7]

Svenska myndigheter har inom ramen för det civila försvaret i uppgift att bland annat skydda landets civilbefolkning, se till att vital samhällsviktig verksamhet fungerar och ge stöd till Försvarsmakten.[8] Allmänheten förväntas förstå att situationen är mycket ansträngd och att myndigheternas stöd är begränsat, samt att befolkningen har ett eget ansvar för att ta hand om sig själva.

## 1.3 Avgränsningar

Studien som redovisas i denna rapport baseras på innehållet i tidigare FOI-rapporter. Flera av dessa presenterar fallstudier av enskilda verksamheter i specifika sektorer. Att en omständighet betraktas som ett problem i en enskild verksamhet behöver dock inte betyda att den är ett problem i alla verksamheter eller alla sektorer, något som ofta påpekas i rapporterna. Istället kan resultaten tolkas som att de pekar på presumtiva problem för en sektor, något som förhoppningsvis kan undersökas ytterligare i fördjupade studier. Några sådana fördjupningar har dock inte gjorts inom ramen för denna studie.

[5] SFS 1992:1403.
[6] Försvarshögskolan. 2023. s. 135-136.
[7] Försvarshögskolan. 2023. s. 135.
[8] Proposition 2020/21:30.

Studien har enbart beaktat problem som har med digitaliseringen att göra. Samhällsviktig verksamhet[9], offentlig såväl som privat, är i fokus. Hur militär verksamhet påverkas av digitaliseringen har inte beaktats. Fokus har också primärt legat på tillgänglighet för IT-system och data, snarare än på konfidentialitet och riktighet. Tidsperspektivet är nutid, såväl för de problem som har identifierats i litteraturen och för de hypotetiska följderna som kan uppstå i gråzon och krig. Litteratur publicerad under åren 2015–2023 bedömdes utgöra nutid.

## 1.4 Målgrupp

Den första målgruppen för rapporten är beredskapsplanerare inom samhällsviktig verksamhet där digitaliseringen redan har gjort intåg, eller är i antågande. Med beredskapsplanerare åsyftar vi dem som ansvarar för att analysera vilken verksamhet som ska bedrivas under höjd beredskap och krig, samt identifiera åtgärder som behövs för att klara av att bedriva verksamheten. I det arbetet är det värdefullt att förstå vilka sårbarheter och problem som digitaliseringen kan föra med sig, som ett underlag i den egna analysen.

Den andra målgruppen är digitaliseringsansvariga inom samhällsviktiga verksamheter. I arbetet med att effektivisera verksamheten och att göra kostnadsbesparingar är det viktigt att kunna relatera till den konflikt som kan uppstå i förhållande till beredskapsarbetet. Förhoppningen är att rapporten ska underlätta för beredskapsplanerare och digitaliseringsansvariga att föra en dialog med varandra i syfte att hitta gemensamma lösningar som främjar både digitaliseringen och beredskapen.

[9] För en mer utförlig diskussion kring vad samhällsviktig verksamhet är, se https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/samhallsviktig-verksamhet.

# 2 Metod

För att kunna besvara frågeställningarna som presenterades i avsnitt 1.1 genomfördes studien i fem sekventiella steg:

1. Identifiering av litteratur om digitalisering.
2. Identifiering av problem som kan hänföras till digitalisering.
3. Gruppering av identifierade problem i problemområden.
4. Analys av hur problemen i respektive problemområde yttrar sig i fred, gråzon och krig.
5. Identifiering av digitaliseringens fallgropar, vilka påverkar möjligheterna att genomföra verksamhet i gråzon och krig.

I det första steget identifierades källor i form av rapporter från tidigare studier som handlar om digitaliseringens påverkan på det svenska samhället och den svenska civila beredskapen. Urvalet av rapporter gjordes initialt utifrån rapporternas titel och sammanfattning. Tanken var från början att ta med rapporter från andra myndigheter och svenska lärosäten, men materialet blev då för stort för att kunna bearbetas inom ramen för studien. Samtidigt konstaterades att FOI har skrivit 35 rapporter inom området, varav många sammanställde kunskap från annan litteratur och offentliga utredningar. Källmaterialet begränsades därför till FOI-rapporterna, vilka ansågs ge en tillräckligt bra bild av helheten.

I det andra steget gjordes en mer grundlig genomläsning av rapporterna, varvid problem identifierades som kunde hänföras till digital teknik, till digitaliseringen i sig eller till datalagring. Av de 35 ursprungliga rapporterna gick det att identifiera problem med digitaliseringen i 16 av dem. De rapporter som sållades bort beskrev antingen problem på detaljerad teknisk nivå, problem i samband med militära tillämpningar eller så hade de fokus på scenarier, det vill säga hypotetiska händelser. Som problem räknades alla förhållanden som utpekades som exempelvis utmaningar, svårigheter, problem, sårbarheter, brister eller svagheter. Dessa kan sammantaget utgöra förhållanden som kan förstås som problematiska i ordets allmänna mening.

I det tredje steget grupperades problemen i problemområden där problemen inom ett problemområde antogs ha samma grundorsak, exempelvis bristande styrning eller externa beroenden. Grupperingen gjordes av författarna och stämdes av mot motsvarande indelningar i andra rapporter. Resultatet analyserades, reviderades och kompletterades därefter av FOI-forskare med kompetens inom digitaliseringsfrågor.

I det fjärde steget analyserades problemen i respektive problemområde för att först ge en samlad problembild utifrån en fredstida situation, i vilken problemen

primärt var beskrivna i litteraturen. Därefter gjordes en bedömning av hur problemen skulle ändra karaktär i en situation av gråzon eller krig. Bedömningarna baserades till största del på författarnas egen analys.

I det femte steget analyserades problemområdena och de underliggande problemen utifrån hur de förväntades påverka myndigheters och andra aktörers möjligheter att genomföra sin verksamhet när fred övergår i gråzon eller krig. Fokus för analysen var att hitta svårigheter som uppstår till följd av digitaliseringen, som skapar problem i gråzon eller i krig och där det finns målkonflikter mellan den fredstida nyttan och de säkerhetsrelaterade behoven för att kunna verka i ett höjt säkerhetsläge.

# 3 Problemområden

Identifieringen av rapporter som har skrivits kring digitalisering inleddes med en genomgång av publicerade FOI-rapporter. Dessa redovisas i bilaga 1. Rapporterna beskriver studier som bland annat har genomförts inom anslagsprojektet *Samhällets beredskap i kris och krig* (Sabek) samt *Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet* (NCS3) som finansierats av Myndigheten för samhällssäkerhet och beredskap, MSB. Dessa studier har ofta ett fredstida perspektiv som utgångspunkt men studieresultaten kan i vissa fall även ge en insikt om problem som är aktuella i gråzon eller krig.

Genomläsningen av rapporterna resulterade i drygt 100 identifierade problem. Identifieringen av problem utgick från en bred syn på vad som kan anses vara ett problematiskt förhållande. I tabell 1 nedan återges de benämningar som användes i de genomlästa rapporterna för att beskriva det som i denna rapport refereras till som *problem*. Flera av problemen överlappade, eller var snarlika. Dessa sammanfogades då, varför antalet problem som presenteras nedan är färre än 100.

Tabell 1: Benämningar på problem.

| Benämning |
|---|
| Asymmetri |
| Beroende |
| Brist |
| Dilemma |
| Exponering |
| Fallgrop |
| Fara |
| Farhåga |
| Flaskhals |
| Gap |
| Glapp |
| Hot |
| Obalans |
| Ointresse |
| Oklarhet |
| Problem |
| Risk |
| Sårbarhet |
| Utmaning |
| Övertro |

Den stora mängden problem som identifierades från rapporterna behövde grupperas då det fanns problem som var av såväl samma som likartad karaktär. Den slutliga grupperingen tog inspiration från den indelning i problemområden som användes i rapporten Vilse i lasagnen[10]. Resultatet blev följande åtta problemområden:

1. Otydlig styrning och bristande samordning
2. Snabb teknikutveckling
3. För högt ställda förväntningar
4. Bristfällig infrastruktur
5. Externa beroenden
6. Bristfällig plan B
7. Exponering av komponenter och information
8. Kompetensbrist

Problemområdena är inte fristående. Det finns såväl överlapp som beroenden mellan dem. De tre första områdena, *Otydlig styrning och bristande samordning, Snabb teknikutveckling* och *För högt ställda förväntningar,* är mer övergripande och strategiska än de övriga. De påverkar de områden som kommer därnäst: *Bristfällig infrastruktur* och *Externa beroenden*. Dessa påverkar i sin tur problemområdena *Bristfällig plan B* och *Exponering av komponenter och information*. *Kompetensbrist* är ett problemområde som genomgående överlappar alla andra problemområden.

För alla problemområden gick det att härleda problemens ursprung till brister i den fredstida planeringen. Att planeringsarbete tar sin utgångspunkt i en fredstida situation är rimligt då majoriteten av de identifierade problemen beskrivs utifrån att fred råder. Däremot kan det för de olika problemområdena variera om konsekvenserna blir som allvarligast i fred, gråzon eller krig.

I avsnitten som följer beskrivs respektive identifierat problemområde. Utöver att beskrivningarna ger en övergripande förklaring till vad problemområdet innebär, så presenteras även de underliggande problem som har identifierats. Det finns med nödvändighet ett visst överlapp mellan problemområdena, och likaså ett visst överlapp mellan de problem som inkluderas i dem.

Beskrivningarna av problemen och problemområdena bygger enbart på de FOI-studier (se bilaga 1) som har legat till grund för litteraturstudien.[11] Dessa studier är till sin karaktär olika. En del innehåller omfattande genomgångar av rapporter, artiklar och offentliga utredningar. Andra baseras på intervjustudier, där ett begränsat antal intervjupersoner har fått ge sin bild av hur digitaliseringen

[10] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020.
[11] I de fall vi refererar till andra källor än FOI-rapporter beror det på att FOI-rapporten har refererat till denna utan att göra någon egen analys. Vi har då valt att referera till ursprungskällan.

fungerar inom deras områden. De flesta studierna innehåller en blandning av litteratur- och intervjustudier, men fokus och metodupplägg varierar.

Resultaten från en intervjustudie som baseras på ett fåtal intervjuer redovisar enbart de problem som intervjupersonerna har upplevt. Resultatet går inte att generalisera till alla sektorer, eller ens till alla verksamheter inom den sektor som undersökts. Vi har inte alltid hittat information i källmaterialet om hur ofta förekommande, eller hur allvarliga, problemen är. Allvarligheten kan dessutom variera mellan olika verksamheter, varför det kanske inte ens är meningsfullt att försöka gradera hur svåra konsekvenser som kan uppstå till följd av ett specifikt problem. Sammanställningen av problem som redovisas i denna rapport bör dock kunna utgöra ett underlag för verksamhetsrepresentanter så att de själva avgöra i vilken utsträckning problemen kan få konsekvenser i den egna verksamheten.

Utifrån ovanstående resonemang betraktar vi de problem som har identifierats i FOI-rapporterna som presumtiva problem. Presentationen av problemområdena ska därmed ses som en palett av tänkbara problem som digitaliseringen kan föra med sig och inte som en heltäckande beskrivning av alla möjliga problem som kan uppstå. Paletten fungerar som ett underlag för att kunna göra en bedömning av hur de olika problemområdena skulle kunna yttra sig i gråzon eller krig. Dessa bedömningar baseras till största del på författarnas egna analyser.

## 3.1 Otydlig styrning och bristande samordning

Hos många offentliga aktörer pågår ett arbete med digitalisering av verksamheter och processer. Detta sker på statliga myndigheter inklusive länsstyrelser, regioner, kommuner, lärosäten, domstolar och statliga bolag. Till det kan adderas en stor mängd privata företag som driver och förvaltar samhällets infrastruktur. I och med att Sverige har en avreglerad marknad finns dessutom flera skikt av infrastrukturproducenter, operatörer och tjänsteutvecklare.[12] Den svenska digitala infrastrukturen förutsätter att privata aktörer ansvarar för vitala delar av infrastrukturen, och att statliga myndigheter och kommuner investerar i den och utövar tillsyn.[13] Behovet av styrning och samordning är därför stort för att kunna säkerställa att nya och befintliga delar av den digitala infrastrukturen blir robust med en tillräcklig kapacitet.

### 3.1.1 Problem i fredstid

Det stora antalet aktörer som ansvarar för samhällsviktig verksamhet gör såväl samordningen som styrningen komplex, och den snabba digitaliseringstakten gör

[12] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 80.
[13] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 80.

det svårt för lagstiftningen att hänga med. Flera rapporter och utredningar, som gjorts av bland annat Kungliga Ingenjörsvetenskapsakademin (IVA), Vetenskapsrådet och Ekonomistyrningsverket, har påpekat att samordningen och styrningen inom digitaliseringen i Sverige är för svag, och behöver stärkas.[14]

#### 3.1.1.1 Bristande helhetssyn

Det finns brister i helhetssyn och samordning av digitalisering på såväl statlig som kommunal nivå.[15] IVA påpekar också att styrningen och samordningen av digitaliseringsfrågor inom Regeringskansliet är svag och otillräcklig.[16] Övergripande lyfts i våra källor att utbyggnaden av digital infrastruktur och samordningen av informationssäkerhetsarbetet har hamnat på efterkälken. I och med att digitaliseringen går så fort saknas regler och planer för drift och utbyggnad av den digitala infrastrukturen, motsvarande den som finns för andra typer av infrastrukturer, såsom elnät och vatten- och avloppsnät.[17] Det finns inte heller någon samlad planering och kontroll av kvaliteten och driftsäkerheten för den digitala infrastrukturen.[18] Ansvaret är istället spritt på flera aktörer, och ansvarsförhållanden är ofta oklara. Detta är något som försvårar införandet av gemensamma informationssäkerhetskrav.[19]

#### 3.1.1.2 Lagstiftning och regelverk

Digitaliseringen, inom både den offentliga och den privata sektorn, karaktäriseras av snabb teknikutveckling. Lagstiftningen och regelverken hinner inte utvecklas i samma takt, utan är ofta anpassade till problem förknippade med äldre teknik snarare än till aktuella problem.[20] Ofta saknas det också gemensamma standarder.[21] Dessutom finns det en osäkerhet i hur lagar ska tolkas i förhållande till den nya tekniken.[22] När flera aktörer utfärdar regler inom området utan att samordna sig sinsemellan kan det uppstå en fragmentering av kravställningarna. Denna variation i kravställning kan leda till att samma typ av information får olika skydd beroende på var i förvaltningssystemet den hanteras.[23]

[14] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 80.
[15] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 80.
[16] IVA (2019), Digitalisering för ökad konkurrenskraft, s. 50.
[17] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 80.
[18] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 78.
[19] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 81.
[20] Johansson & Jonsson, 2018, s. 26.
[21] Mickelsson & Bengtsson, 2021, s. 37.
[22] Mickelsson & Bengtsson, 2021, s. 37.
[23] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 81.

#### 3.1.1.3 Datadelning

Bristen på styrning och samordning skapar inte bara problem inom utbyggnaden av den digitala infrastrukturen och för informationssäkerheten, utan innebär även ett problem ur ett datadelningsperspektiv.[24] Ekonomistyrningsverket har önskat att det skapas fler förvaltningsgemensamma tjänster och strukturer i Sverige och en ökad interoperabilitet genom att införa en modern lagstiftning som tillåter en effektivare informationsförsörjning.[25] Ett av flera hinder för det är den bristande tillgången på gemensamma grunddata för offentliga aktörer. Idag hämtar runt hälften av de offentliga aktörerna data direkt från företag och privatpersoner, trots att uppgifterna redan finns hos en annan offentlig aktör.[26]

#### 3.1.1.4 Otillräckliga krav på leverantörer

Majoriteten av regionerna saknar avtalsbestämmelser som säkerställer att (privata) leverantörer tillhandahåller olika tjänster i flertalet kris- och krigssituationer.[27] Sådana krav ställs i högre grad på den verksamhet som bedrivs i regionernas egen regi än när de upphandlas av privata leverantörer.[28] Problemet har särskilt lyfts inom vårdsektorn, men finns gissningsvis inom fler sektorer.

### 3.1.2 Problem i gråzon och krig

En bristande helhetssyn och otydlig styrning kan göra att olika aktörer tolkar lagar och regelverk på olika sätt, och därmed kommer fram till olika slutsatser om hur information ska klassificeras som skyddsvärd, och om hur information och IT-system ska skyddas.

I fredstid kan det vara en pragmatisk lösning att överlåta på aktörerna själva att välja hur de ska hantera sin information och sina IT-system utifrån rådande lagstiftning. Då förloras ingen tid och digitaliseringen kan rulla på, förhoppningsvis med effektiviseringsvinster som följd. Men om data finns lagrade på flera ställen så kan det räcka att *en* aktör avstår från att klassa en viss typ av information som skyddsvärd för att en angripare ska kunna få tillgång till informationen. Att andra aktörer har lagt ner arbete på informationssäkerhet kan då minska i betydelse.

Den bristande helhetssynen och samordningen kan alltså leda till att sårbarheter omedvetet byggs in i våra IT-system, och exponerar information och systemkomponenter på ett sådant sätt som gör det möjligt för en angripare att komma åt dem.

I en gråzon är det problematiskt för svenska offentliga aktörer att de måste följa den fredstida lagstiftningen. Det innebär att de i en mycket pressad situation även

[24] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 81.
[25] ESV. 2018. s. 46 och 54.
[26] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 81.
[27] Budryk, Dahl, Lackenbauer, Refors Legge & Lusua, 2023, s. 26-27.
[28] Budryk, Dahl, Lackenbauer, Refors Legge & Lusua, 2023, s. 26-27.

ska förhålla sig till haltande regelverk, oklara ansvarsförhållanden och problem med datadelning som den bristande styrningen och samordningen har gett upphov till. Krav som gissningsvis tonas ner i en krigssituation då en annan lagstiftning gäller.

Ett annat problem som också blir tydligare i gråzon och krig än i fred, är att många offentliga aktörer inte har tydliga avtal med sina leverantörer om vilka digitala tjänster som ska levereras under en kris eller i krig. Det är inte heller säkert att det räcker att skriva avtal. I en krissituation kan leverantören välja att bryta avtalet, och ta konsekvenserna av det, för att ge stöd till andra kunder där straffavgifterna är högre om man inte kan fullfölja avtalet. En ytterligare aspekt är att många IT-system och systemkomponenter kommer från utländska leverantörer eller tillverkas utomlands.[29] Utländska leverantörer kan förhindras att fullfölja avtalet på grund av att de är från, eller styrs av, ett land som Sverige är i konflikt med.

## 3.2 Snabb teknikutveckling

Den snabba teknikutvecklingen innebär att det idag finns möjligheter att skapa lösningar som inte ens var tänkbara för bara några år sedan. Den nya tekniken ger möjligheter att effektivisera verksamheter, exempelvis genom att automatisera arbetsmoment som tidigare har genomförts manuellt. Utöver en snabb utveckling av vad tekniken klarar av så har även kostnaderna för tekniken gått ner, vilket tillgängliggjort teknik till allt större delar av samhället. Ett exempel är strömsnåla trådlösa sensorer som monteras i dagvattenbrunnar för att mäta vattennivåer. Då sensorerna regelbundet skickar mätvärden kan ökande vattennivåer snabbt identifieras och åtgärdas. Sensorerna ersätter det tidigare förfarandet att personal åkte runt till alla dagvattenbrunnar och manuellt mätte den aktuella vattennivån. Den nya tekniken innebär en ökad precision och bättre möjlighet att förhindra översvämningar.

### 3.2.1 Problem i fredstid

Den snabba teknikutvecklingen för inte bara med sig förbättringar, det finns även baksidor.

#### 3.2.1.1 Kort supporttid

Den snabba utvecklingstakten har lett till att tillverkare ger allt kortare supporttid för de komponenter som säljs. Behovet av att ersätta komponenter drivs därför primärt inte av att komponenterna går sönder, utan av att tillverkaren inte längre tillhandahåller reservdelar eller uppdateringar av mjukvaror.[30] Att välja att

[29] Eidenskog, Eckersand & Mittermaier, 2023, s. 42.
[30] Hedtjärn Swaling, Malmberg Andersson & Clausen Mork, s. 28.

fortsätta använda komponenter som inte längre säljs, som det inte längre säljs reservdelar till och som inte längre får mjukvaruuppdateringar (exempelvis säkerhetsuppdateringar) kan innebära en svårighet när verksamhetens genomförande ska säkras.[31]

#### 3.2.1.2 Förändrade ändamål

Komponenter eller hela IT-system kan användas på andra sätt eller för andra ändamål än vad som var tänkt från början.[32] Denna typ av förändring brukar refereras till som syftesglidning (eng. purpose creep) eller funktionsglidning (eng. function creep). Att komponenter används för andra ändamål än de är tänkta för är något som över tid kan skapa svåröverskådliga beroenden.[33] Dessutom kan det med tiden bli svårt att ersätta dessa typer av speciallösningar. Utöver komponenter gäller detta problem även insamlade data som med tiden används för andra ändamål än det ursprungliga syftet.[34]

#### 3.2.1.3 Lagen om offentlig upphandling

När upphandling ska ske hos offentliga aktörer i enligt med lagen om offentlig upphandling (LOU)[35], för att säkerställa att skattebetalarnas pengar används så effektivt som möjligt, blir det svårt att hålla sig till en enda leverantör eller systemlösning.[36] Istället kan flera olika leverantörer vardera implementera olika lösningar för en tjänst, vilket kan resultera i ett lapptäcke av lösningar som gör det svårt att få ett enhetligt underhåll och support av verksamheten. Det blir dessutom svårare att skydda IT-systemet mot IT-attacker.[37]

#### 3.2.1.4 Säkerhetsarbetet hinns inte med

Säkerhetsarbetet hinns inte alltid med eller genomförs inte alltid i tillräcklig omfattning under digitaliseringsarbetet. Den kalendertid, arbetstid och kunskap som krävs för att bygga säkra IT-system underskattas ofta.[38] En orsak till problemet är att ny och omogen teknik används innan ordentlig testning har genomförts. Den nya tekniken har i många fall barnsjukdomar som innebär introduktion av sårbarheter eller att användningen av tekniken inte ger förväntad

[31] Hedtjärn Swaling, Malmberg Andersson & Clausen Mork, s. 35.
[32] Mickelsson & Bengtsson, 2021, s. 36.
[33] Hedtjärn Swaling. 2015. s. 2.
[34] Mickelsson & Bengtsson, 2021, s. 36.
[35] SFS 2016:1145
[36] Hedtjärn Swaling, Malmberg Andersson & Clausen Mork, 2016, s. 47.
[37] Hedtjärn Swaling, Malmberg Andersson & Clausen Mork, 2016, s. 47.
[38] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 75-76.

effekt.[39,40,41] Dessa barnsjukdomar kan även vara av sådan art att de uppdagas först när tekniken används i stor skala.[42] En annan orsak till problemet är att säkerhetsarbetet genomförs efter hand som digitaliseringsarbetet fortskrider. Eftersom digitaliseringsarbetet går snabbt och det är svårt att lägga till säkerhet i efterhand uppnås inte alltid adekvat säkerhet.[43]

#### 3.2.1.5 Gamla lösningar avvecklas

Vid digitalisering avvecklas gamla lösningar så fort de nya tas i bruk.[44] Den snabba avvecklingen av gamla lösningar innebär att det snabbt blir en situation där det inte finns någon alternativ lösning att återgå till om det skulle visa sig att den nya inte håller måttet eller om det inträffar en störning. Bakgrunden till snabb avveckling är troligtvis ekonomiska drivkrafter då det kostar att ha dubbla lösningar driftsatta och digitaliseringsarbetets syfte ofta är just effektivisering och kostnadsbesparing.[45] Ett exempel på den snabba förändringen är omställningen till elektroniska betalningar där kontanter visserligen fortfarande finns kvar som en lösning, men där få personer har kontanter och få verksamheter accepterar kontantbetalningar. Vid ett strömavbrott eller vid störningar i anslutningen till Internet är möjligheterna att betala praktiskt taget obefintliga.[46]

### 3.2.2 Problem i gråzon och krig

Vid övergång från fred till gråzon eller krig är bedömningen att problemen relaterade till snabb teknikutveckling kommer att vara som störst i gråzon för att därefter avta om situationen övergår till krig. Anledningen till att problemen bedöms vara större i gråzon än i krig är att det i gråzon fortfarande finns fredstida förväntningar på teknikutveckling och digitaliseringsarbete. Om situationen övergår till krig bedöms förväntningarna på både teknikutveckling och digitaliseringsarbete minska.

Problemet med tillverkarnas kortare supporthorisont kommer i gråzon och krig troligtvis att märkas mest i form av den sämre komponentkvaliteten. Problemet bedöms vara som störst vid en krigssituation. Komponenterna byggs med utgångspunkten att de ska bytas ut snarare än repareras när de fallerar, vilket kan påverka möjligheten att vid behov kunna reparera dem. I gråzon och krig, med troliga störningar i leveranskedjor, kan dessutom tillgången till reservdelar och

[39] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 82.
[40] Johansson & Jonsson. 2018. s. 26.
[41] Jonsson. 2018. s. 58.
[42] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 82.
[43] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 83.
[44] Mickelsson & Bengtsson, 2021, s. 40-41.
[45] Mickelsson & Bengtsson, 2021, s. 35.
[46] Mickelsson & Bengtsson, 2021, s. 40-41.

support vara begränsad, vilket ytterligare försvårar möjligheterna att både reparera och ersätta trasiga komponenter.[47]

Problemet med lapptäcken av komponenter, programvaror och systemlösningar från olika leverantörer som skapats av att nya upphandlingar behöver göras för att efterleva LOU kan i gråzon och krig ses på olika sätt. Å ena sidan kan lapptäcket göra det svårare att skydda hela IT-miljön då det är många olika komponenter och programvaror med olika sårbarheter som behöver hållas uppdaterade och skyddade. Å andra sidan kan lapptäcket göra det svårare för en angripare att slå ut hela IT-miljön då de olika komponenterna och programvarorna kommer från olika leverantörer och därmed kanske inte har samma sårbarheter som kan utnyttjas.

I gråzon och krig är det troligt att den snabba digitaliseringens bristande fokus på säkerhet kommer att synliggöras. Nya IT-system som i bästa fall har byggts för att klara fredstida påfrestningar kommer att utsättas för en ny hotbild som i högre grad inkluderar antagonistiska statsaktörer. Angrepp kommer troligtvis ske mot de IT-system som är sårbara, oavsett om de anses som viktiga. Att slå brett mot flera IT-system, oavsett viktighet, är något som kan skapa oreda och otrygghet i samhället. Dessutom kan det flytta fokus från andra händelser. Om de gamla IT-systemen dessutom redan har avvecklats, för att digitaliseringen ska ge kostnadsbesparingar, så finns det inte heller någon alternativ lösning att falla tillbaka på. Möjligheterna att under gråzon eller krig utveckla nya systemlösningar kan vara begränsade.

## 3.3 För högt ställda förväntningar

I Sverige har vi en stark tilltro till tekniska lösningar, en tilltro som förmodligen grundas i att vi historiskt sett har haft många framgångsrika uppfinnare.[48] Förväntningarna är därför stora på digitaliseringens möjligheter, såväl från staten och offentliga aktörer som från allmänheten. En av förväntningarna handlar om att digitaliseringen ska medföra effektiviseringar och ett minskat behov av administrativ personal, och därmed sänka kostnaderna för olika verksamheter. Digitala beslutsstödsystem förväntas också hjälpa olika yrkeskategorier att göra bedömningar, exempelvis vid sjukdomsdiagnostisering. En annan förväntan är att digitaliseringen ska underlätta kontakten mellan myndigheterna och medborgarna. Det förväntas bli enklare att i större utsträckning sköta myndighetsärenden via datorn, och inte behöva sitta i telefonkö eller passa öppettiderna på ett kontor.

[47] Eidenskog, Eckersand & Mittermaier, 2023, s. 42.
[48] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 87-88.

### 3.3.1 Problem i fredstid

Tilltro och förväntningar är i grunden något positivt eftersom det bidrar till att driva utvecklingen framåt. Men om tilltron till IT-systemen överstiger IT-systemens faktiska förmåga, eller om förväntningarna är för högt ställda, så riskerar de istället att bidra till att stjälpa utvecklingsprojekten. Det finns många exempel där en verksamhets arbete har försvårats istället för underlättats, och där kostnaderna har sprungit i väg. Denna typ av misslyckade utvecklingsprojekt kan i sin tur minska medborgarnas tilltro till samhällets förmåga att hantera samhällsviktig verksamhet.

#### 3.3.1.1 Höga förväntningar

Som redan nämnts finns det en förväntan att digitaliseringen ska kunna effektivisera många verksamheter och även öka säkerheten i dem. Detta gäller också mindre verksamheter som inte har möjlighet att ha anställd personal med rätt kompetens, eller ha tillräckligt många anställda. I den andan automatiseras många processer och de äldre manuella rutinerna rensas bort, något som kan leda till att det inte finns tillräcklig redundans om de automatiska systemen fallerar.[49] Ett illustrerande exempel är att många inte längre har en telefonbok där telefonnummer till familj och vänner finns uppskrivna, utan litar på att de finns tillgängliga i mobiltelefonen.

Ett annat problem uppstår när höga förväntningar kombineras med en, oftast omedveten, bristande beställarkompetens (vilket diskuteras vidare i avsnitt 3.8.2). Om de som ansvarar för verksamheten inte förstår vilka typer av tjänster eller IT-system som har beställts, och vilken service IT-systemen kan ge, finns en risk att tilltron till IT-systemen överstiger den faktiska funktionen som tekniken och infrastrukturen kan leverera. Sådana IT-system kan bli ineffektiva, opålitliga och dyra. Dessutom sänker de tilltron hos allmänheten inför nästa digitaliseringsprojekt.[50]

#### 3.3.1.2 Effektiviseringen uteblir

Det är ofta svårt att överblicka vilka följder ett nytt IT-system för med sig. Det som på pappret ser ut som en förenkling av arbetsuppgifter kan i praktiken medföra att det skapas nya administrativa och säkerhetsmässiga uppgifter. Dessa läggs på personal som inte har IT som sin huvudsakliga arbetsuppgift, vilket många inom exempelvis vården vittnar om.[51] En ny digital arbetsmiljö kan dessutom vara dålig ur fysisk, psykosocial eller kognitiv aspekt. I värsta fall kan den digitala arbetsmiljön ge omfattande problem såsom ökad belastning, stress

[49] Wedebrand & Veibäck, 2018, s. 10.
[50] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 87-88.
[51] Eidenskog, Eckersand & Mittermaier, 2023, s. 48-49.

och ohälsa hos personalen, samtidigt som verksamhetens effektivitet istället minskar.[52] Ytterligare en fara finns i användandet av digitala beslutsstödsystem, exempelvis stödsystem som hjälper läkare att ställa diagnoser. De kan i vissa fall ge mer tillförlitliga och enhetliga bedömningar än läkarna själva, vilket i sig är positivt. Men en övertro på sådana IT-system kan leda till en minskad tilltro till den egna förmågan att göra bedömningar.[53]

#### 3.3.1.3 Kostnadsbesparingar uteblir

Det är sällan lätt att på förhand bedöma ett digitaliseringsprojekts faktiska vinster, kostnader och risker. Därtill kommer att digitalisering sällan är kostnadsbesparande på kort sikt. Om befintliga rutiner replikeras till en digital miljö, utan att verksamheten förändras och effektiviseras i sig, så uppnås i regel inga kostnadsbesparingar.[54] En ogenomtänkt digitalisering kan dessutom ge dubbelarbete som leder till en sänkt effektivitet. Svåranvända eller opraktiska IT-system kan kosta mycket arbetstid för personalen, tid som tas från kärnverksamhet. Och tid är pengar. Det är också en fara att man vid anskaffningen av ett IT-system enbart tittar på investeringskostnaderna och det tillhörande förändringsarbetet, och inte tänker på att det tillkommer långsiktiga drift- och förvaltningskostnader.[55] Det är inte heller säkert att risken för ett eventuellt IT-angrepp vägs in. Konsekvenserna av ett sådant, exempelvis att känsliga uppgifter sprids till obehöriga, kan medföra stora kostnader.[56] Risken finns att kostnaderna, inte minst de säkerhetsrelaterade, underskattas när visionära projekt ska sjösättas under tidspress.

#### 3.3.1.4 IT-incidenter

Det finns en förväntan från medborgarna att grundläggande samhällsfunktioner ska fungera, oavsett om de är digitaliserade eller ej. Som nämnts tidigare är allmänhetens tilltro till digital teknik stor. Men tilltron har börjat naggas i kanten efter incidenter där IT-system har slutat fungera eller fungerat felaktigt, eller då känslig data läckt ut. Ett exempel på det senare är den så kallade 1177-skandalen där det 2019 uppdagades att 2,7 miljoner inspelade samtal till Vårdguiden legat öppna och oskyddade på en webb-server i flera år.[57] Skulle fler sådana händelser inträffa, eller om det skulle ske ett större sammanbrott inom en samhällsviktig verksamhet, exempelvis vården eller elförsörjningen, så kan det bli svårt att återupprätta förtroendet för sådana tjänster. Ett sänkt förtroende för vissa

[52] Eidenskog, Eckersand & Mittermaier, 2023, s. 32.
[53] Eidenskog, Eckersand & Mittermaier, 2023, s. 25.
[54] Eidenskog, Eckersand & Mittermaier, 2023, s. 37.
[55] Eidenskog, Eckersand & Mittermaier, 2023, s. 39.
[56] Eidenskog, Eckersand & Mittermaier, 2023, s. 48.
[57] ComputerSweden. 2019.

verksamheter skulle även kunna påverka hela digitaliseringsambitionen negativt.[58]

#### 3.3.1.5 Digitalt utanförskap

Digitala system, exempelvis för tidsbokningar och videomöten, kan effektivisera offentliga verksamheter, och även minska behovet av administrativ personal. Men digitalisering av offentliga tjänster riskerar också att lägga till ytterligare en klyfta mellan dem som har tillgång till datorer och Internet-uppkoppling, samt kunskap om hur de används, och dem som inte har det. Tidigare har myndighetskontakter skett genom personliga möten och telefonsamtal. Nu förväntas medborgarna till del själva kunna handlägga sina ärenden, och veta vilka myndigheter de ska kontakta och vilka digitala tjänster de ska använda.[59] Möjligheterna minskar därmed för den grupp av människor som inte har kunskap om den digitala tekniken och kompetens att navigera i den offentliga förvaltningen.[60] De grupper i samhället som inte har möjlighet att följa med i digitaliseringsutvecklingen riskerar att hamna i ett utanförskap som kan resultera i negativa konsekvenser både för individen och för samhället.[61]

### 3.3.2 Problem i gråzon och krig

Det är en paradox att vi ibland digitaliserar processer i offentliga verksamheter i effektiviseringssyfte, men att digitaliseringen istället resulterar i att verksamheten blir mer ineffektiv, och bedrivs till en högre kostnad. Sådana problem är frustrerande i fredstid, men rimligen blir konsekvenserna av dem ännu allvarligare i ett gråzonsläge. I gråzon ska vi utöver de fredstida friktionerna även hantera konsekvenserna av antagonistiska angrepp, och det med hjälp av fredstida lagar och fredstida byråkrati. I en krigssituation gäller andra lagar och regler, samtidigt som förväntningarna på vad samhället kan bistå med troligtvis är låga. Problemen med en ineffektiv digitaliseringsprocess blir därmed större i gråzon och krig.

För höga förväntningar i fredstid, i kombination med en ofullständig beställarkompetens, kan resultera i säkerhetsluckor och sårbarheter i IT-system som kan utnyttjas av en angripare i gråzon och i krig. För att undvika den typen av problem räcker det inte att komma till rätta med ogrundad tillit och obefogade förväntningar. Beställarkompetens, redundans, etcetera måste också finnas på plats.

Användandet av olika typer av digitala expertsystem, exempelvis för att ställa diagnoser inom vården eller för att felsöka fordon, kan göra att experternas

[58] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 86-87.
[59] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 84.
[60] Eidenskog, Eckersand & Mittermaier, 2023, s. 27.
[61] Mickelsson & Bengtsson, 2021, s. 40.

kompetens att göra egna bedömningar minskar. Detta behöver inte vara en nackdel i fredstid, så länge IT-systemen fungerar, men om systemen går ner i gråzon eller i krig behövs en alternativ lösning, en plan B, som då kanske inte är ordentligt övad.

Ytterligare en risk med en för hög tilltro till de digitala systemen är att antagonistiska statsaktörer i gråzon eller krig kan angripa IT-system i syfte att manipulera dem till att förmedla desinformation. Den höga tilltron till digitaliseringen och myndigheter kan göra att medborgarna inte är tillräckligt kritiska till den information som sprids.

## 3.4 Bristfällig infrastruktur

För att IT-system ska fungera förutsätts att viss infrastruktur finns tillgänglig. Under en lång tid var de flesta IT-system autonoma, och infrastrukturen bestod då primärt av den el-infrastruktur som gav systemen tillgång till el. Numera krävs ofta även infrastruktur som möjliggör kommunikation, eftersom IT-system till stor del inte längre används som fristående entiteter. IT-systemen använder istället primärt Internet för att kommunicera med andra IT-system som kan vara utspridda runtom i världen. Exempelvis kan det i en matbutik krävas att kassasystemet kan kommunicera med lagersystem, betalningssystem och bokföringssystem för att det ska vara möjligt att ta betalt av kunderna i en kassa.

Den infrastruktur som är i fokus för detta problemområde är den kommunikationsinfrastruktur i Sverige som möjliggör datakommunikation inom landet och med omvärlden. De viktigaste delarna av denna kommunikations-infrastruktur är det fibernät som utgör grundstommen för kommunikation över hela landet, samt den infrastruktur som därefter tar vid och möjliggör kommunikation ända fram till kunderna som i slutändan ansluter via exempelvis stadsnät, kabel-tv-nät eller mobilt bredband. Fibernäten i Sverige når ut till närmare 84 procent av hushållen.[62]

### 3.4.1 Problem i fredstid

I takt med att allt fler verksamheter digitaliseras ökar både krav och förväntningar på den kommunikationsinfrastruktur som för de flesta IT-system är en förutsättning. I de rapporter som utgör underlaget för denna studie lyfts två problem med den svenska kommunikationsinfrastrukturen i fredstid.

[62] Post- och telestyrelsen. 2023. s. 23.

#### 3.4.1.1 Otillräcklig kapacitet

Den befintliga kommunikationsinfrastrukturen har inte tillräcklig kapacitet överallt för att klara av framtida kommunikationsbehov.[63] Detta baseras på att användandet av Internet har gått från att primärt förmedla text, bilder och i vissa fall ljud till att även förmedla video.[64] Just video lyfts fram som en av anledningarna till att datamängderna som kommuniceras ökar snabbt. Strömmad video kan användas i verksamheter för att exempelvis övervaka vårdtagare inom hälso- och sjukvården eller för att övervaka trafikflöden i en stad. Det saknas kunskap om denna kapacitetsbrist både hos beslutsfattare och i samhället i stort.[65]

Förutsättningarna för kommunikation är generellt sett goda i Sverige med bredbandstillgång för över 99,99 procent av svenska hushåll.[66] Dock kan tillgången lokalt variera beroende på var i landet IT-systemet eller användarna befinner sig, speciellt för användare utanför tätorter och småorter och vars anslutning sker via trådlös accessteknik såsom LTE (4G).[67] Att tillgång till bredband finns för hushållen innebär dock inte att alla har valt att ansluta sig.

#### 3.4.1.2 Otillräcklig redundans

Det är otillräcklig redundans i kommunikationsinfrastrukturen, vilket innebär att det vid störningar på ett ställe, exempelvis på grund av att en fiberkabel har grävts av, inte alltid går att dirigera om trafiken i kommunikationsnäten.[68] En av anledningarna som lyfts fram är bristande koordinering mellan de aktörer som bygger ut infrastrukturen samtidigt som utbyggnaden av fibernät sker på affärsmässiga grunder.[69] Att bygga redundans i fibernäten innebär att skapa alternativa kommunikationsvägar, vilket i praktiken innebär att fiber behöver dras mellan områden som redan är anslutna. Att dra fiber mellan områden som redan är anslutna blir svårmotiverat om utbyggnaden ska ske på rent affärsmässiga grunder. Det läggs allt för lite tankekraft på att säkerställa att kommunikationen är tillförlitlig.[70]

### 3.4.2 Problem i gråzon och krig

Vid övergång från fred till gråzon eller krig kommer konsekvenserna av de fredstida problemen troligtvis att öka. Det är rimligt att anta att angrepp mot kommunikationsinfrastrukturen kommer att ske vid både gråzon och krig. I gråzon sker angreppen troligtvis i form av sabotage utfört av en aktör som vill

[63] Ingemarsdotter, Eidenskog & Hedtjärn Swaling. 2020. s. 78.
[64] Ekholm, Jebari & Markovic. 2018. s. 19.
[65] Kungliga Ingenjörsvetenskapsakademien (IVA). 2019. s. 7.
[66] Post- och telestyrelsen. 2023. s. 22-23.
[67] Post- och telestyrelsen. 2023. s. 21-22.
[68] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 78.
[69] Vetenskapsrådet. 2018. s. 2.
[70] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 88.

undgå att bli upptäckt, och därmed väljer sina mål med omsorg utifrån vilka tillfällen som ges. I krig finns inte samma behov för aktören att undvika upptäckt.

Båda de fredstida problem som har identifierats kommer troligtvis att förvärras i gråzon och krig. Redan i fredstid varierar kommunikationsinfrastrukturens täckning på lokal nivå utanför tätorter och småorter samtidigt som alla inte väljer att ansluta sig, vilket innebär att hela befolkningen inte nås. Samtidigt är redundansen i infrastrukturen bristfällig, vilket innebär att det kan saknas alternativa kommunikationsvägar vid angrepp mot vissa delar av infrastrukturen. Den bristande redundansen skulle då leda till att kommunikationsinfrastrukturens täckning blir ännu lägre. Bristande redundans i kombination med att det finns kapacitetsbrist redan i fredstid kan ytterligare förvärra situationen. Båda problemen sammantaget förvärrar möjligheten till kommunikation under gråzon och krig.

Utöver de två fredstida problemen, nämns det i en rapport[71] att det inte finns samma beredskap för avbrott i den digitala kommunikationen som det finns exempelvis för elförsörjningen. För att hantera avbrott i elförsörjning finns ofta lokal redundans för de viktigaste systemen genom användning av elverk och avbrottsfri kraft (eng. uninterruptible power supply, UPS). Den avbrottsfria elen utgörs av batterier som syftar till att hantera korta avbrott samt möjliggöra för systemet att stänga ner sig på ett kontrollerat sätt. För hantering av längre avbrott används elverk. För den digitala kommunikationen används istället ofta standardiserade kommunikationstjänster från operatörer som har byggt tjänsten för att erbjuda hög tillgänglighet i fredstid, inte i onormala situationer såsom gråzon eller krig.

Något som också kan påverka tillgången till kommunikationsinfrastruktur är att ägandet av kritisk infrastruktur i allt större grad flyttats ut till privata aktörer, och då även utländska aktörer. Kontrollen över kritisk infrastruktur är något som kan utnyttjas av annat land för att påverka Sverige i gråzon såväl som krig.[72] Möjligheten för utländsk aktör att, med kontroll över infrastrukturen, bedriva underrättelseverksamhet i Sverige diskuterades exempelvis vid utbyggnaden av Sveriges 5G-nät.[73]

## 3.5 Externa beroenden

IT-system är inte längre något som mestadels har lokala beroenden som verksamheten själv rår över. Dagens IT-system byggs till stor del med standardiserade komponenter och programvaror som kombineras och anpassas

[71] Eidenskog, Eckersand & Mittermaier, 2023, s. 49.
[72] Johansson & Jonsson, 2018, s. 35.
[73] Mickelsson & Bengtsson, 2021, s. 37.

utifrån verksamhetens behov. Denna kompott av standardiserade komponenter och programvaror som till stor del utgör ett IT-system i en verksamhet kan komma från ett stort antal tillverkare baserade runtom i världen. Komponenterna och programvarorna som används kan i sin tur ha ytterligare beroenden, vilket innebär att digitalisering av en verksamhet kan ge upphov till ett stort antal externa beroenden som ofta är komplexa och svåröverskådliga.

### 3.5.1 Problem i fredstid

I de rapporter som utgör underlaget för denna studie lyfts fyra problem som relaterar till externa beroenden.

#### 3.5.1.1 Svårt att överblicka och förstå

Det är svårt att ha en överblick och förståelse för vilka externa beroenden som digitaliseringen medför.[74] Bristande förståelse om externa beroenden kan göra det svårt att skydda de egna systemen mot angrepp. Med beroenden till olika underleverantörer kan intrång i underleverantörers IT-system även påverka den egna verksamhetens IT-system.[75] Detta var exempelvis något som drabbade flera svenska butikskedjor, exempelvis Coop, under 2021 då en underleverantör drabbades av en cyberattack.[76]

#### 3.5.1.2 Beroendet av elektricitet

Beroendet av elektricitet är inte svåröverskådligt, men är däremot ett beroende som har ökat i takt med ökad digitalisering.[77] Alla IT-system är beroende av elektricitet, och när allt fler verksamheter digitaliseras blir beroendet av elektricitet alltmer påtagligt. Genom att vara ett beroende som finns i alla digitaliserade verksamheter är det ett beroende där störningar kan resultera i konsekvenser för många samhällsviktiga verksamheter samtidigt.[78,79]

#### 3.5.1.3 Ett fåtal marknadsdominerande underleverantörer

Det finns ett beroende till vissa tjänster som tillhandahålls av ett fåtal helt marknadsdominerande underleverantörer.[80] Att en underleverantör är marknadsdominerande behöver inte innebära att denne är dominerande på världsmarknaden, utan dominansen kan vara i Sverige eller för en viss typ av

[74] Veibäck, Stenérus Dover & McWilliams. 2021. s. 39.
[75] Veibäck, Stenérus Dover & McWilliams. 2021. s. 39.
[76] Sveriges television. 2021.
[77] Mickelsson & Bengtsson. 2021. s. 35.
[78] Mickelsson & Bengtsson. 2021. s. 35.
[79] Wedebrand & Veibäck. 2018. s. 19.
[80] Ingemarsdotter, Eidenskog & Hedtjärn Swaling. 2020. s. 84.

verksamheter i Sverige. Ett exempel på tjänst med väldigt hög användandegrad i Sverige är Bank-id som används för att bekräfta användarnas identitet. Bank-id används av de flesta svenska bank- och myndighetstjänster som tillhandahålls via Internet. Problemet är inte tjänsten i sig, utan att det är så många verksamheter som har ett beroende till en och samma underleverantör. Om det inträffar störningar i tjänsten som Bank-id tillhandahåller får det en påverkan på majoriteten av användarna av bank- och myndighetstjänster i Sverige.[81] Motsvarande problematik finns även i relationen till andra marknadsledande leverantörer såsom Alphabet (Google), Amazon, Meta (Facebook), Apple och Microsoft.[82]

Utöver att marknadsdominerande leverantörer skapar gemensamma beroenden för många verksamheter så riskerar bristen på alternativa leverantörer även att skapa en inlåsningseffekt. Inlåsningseffekten innebär att verksamheten har ett så starkt beroende till leverantörens tjänster att det blir svårt att byta leverantör, även om leverantören väsentligt skulle ändra sina villkor eller priser.[83]

#### 3.5.1.4 Just-in-time

I syfte att minimera kostnader använder sig verksamheter av just-in-time-principen.[84] Med just-in-time avses att verksamheten enbart håller små lager och att bemanningen sätts utifrån vad som behövs vid normalbelastning på verksamheten. Dagens möjligheter till snabba och välfungerande transporter gör det möjligt för verksamheter att minska storleken på sina egna lager och istället beställa nya produkter, exempelvis reservdelar, löpande i takt med att lagerförda produkter används. Minskad lagerhållning binder inte upp lika mycket kapital för verksamheten, samtidigt som verksamheten undviker risken att få stora lager av föråldrade produkter då produktutvecklingen går snabbt framåt. Samma sak gäller för bemanningen av personal där bemanningen sker utifrån normalläget, och sedan hyrs konsulter eller bemanningspersonal in för att hantera arbetstoppar.[85]

Problemet med just-in-time uppstår när störning inträffar som resulterar i att flera verksamheter samtidigt förflyttas från ett normalläge till en situation med ökat beroende av den icke-lagerhållna produkten eller extra bemanningen.[86] Leverantörerna av produkter och tjänster har nämligen också lagerhållning och bemanning enligt just-in-time anpassat utifrån kundernas normalläge, vilket resulterar i att efterfrågan överstiger utbudet. Något som ytterligare kan förvärra

[81] Kungliga Ingenjörsvetenskapsakademien (IVA). 2019. s. 28
[82] Ingemarsdotter, Eidenskog & Hedtjärn Swaling. 2020, s. 84.
[83] Budryk, Dahl, Lackenbauer, Refors Legge & Lusua. 2023. s. 38.
[84] Eckersand & Stenérus Dover. 2020. s. 12-13.
[85] Eckersand & Stenérus Dover. 2020. s. 12-13.
[86] Eckersand & Stenérus Dover. 2020. s. 12-13.

situationen är att det, för exempelvis reservdelar, ofta enbart finns ett fåtal leverantörer att välja på.[87] Denna typ av problematik blev tydlig under corona-pandemin då störningar i leverantörskedjor resulterade i att verksamheter med lagerhållning enligt just-in-time drabbades av komponentbrist.

### 3.5.2 Problem i gråzon och krig

En övergång från fred till gråzon eller krig kommer troligtvis att innebära att angripare i form av statsaktörer kommer att försöka identifiera och utnyttja de svagaste punkterna i samhället. Attacker mot marknadsdominerande under-leverantörer kan vara prioriterade då ett lyckat angrepp hos en underleverantör kan ge upphov till konsekvenser i många, såväl svenska som internationella, verksamheter samtidigt. Med tanke på att externa beroenden för IT-system är komplexa och svåra att få en överblick över kan det även vara så att ett angrepp från ett land gentemot en marknadsdominerande aktör i ett annat land kan leda till stora påfrestningar i Sverige även om Sverige inte varit den tänkta måltavlan för attacken.

Det stora beroendet av tillgång till el kommer märkas av mer. Störningar i el-produktionen, el-transmissionen eller el-distributionen kommer att få stor påverkan på hela samhället. Den vanligaste beredskapen för el-bortfall är användning av avbrottsfri kraft (UPS) samt elverk. Elverket drivs med bensin eller diesel och syftar till att hantera längre avbrott än UPS. Dock är elverken beroende av drivmedel för att kunna användas under längre perioder, vilket skapar ett beroende till regelbundna drivmedelsleveranser. Eftersom elverk är en vanlig lösning kommer det vara många verksamheter som samtidigt har behov av regelbundna drivmedelsleveranser för att fortsatt ha tillgång till el.[88]

Problemen med att både lagerhållning och bemanning sker enligt just-in-time-principen kommer att resultera i ökade konsekvenser i gråzon och krig. Erfaren-heter från coronapandemin kan ge en fingervisning om hur problemet kan tänkas utveckla sig i gråzon eller krig som inte bara drabbar Sverige utan även när-liggande länder. Störningar i leveranskedjor leder snabbt till minskade lager och brist. När det gäller avtal med utländska företag kan det dessutom vara så att andra länders nationella behov prioriteras avseende tillgång till bemanning och tillverkade produkter, vilket begränsar leverantörernas möjligheter att fullfölja avtal med svenska verksamheter.

## 3.6 Bristfällig plan B

Att ha en plan B syftar till att vara förberedd på hur en verksamhet ska kunna fortgå under olika typer av störningar som påverkar dess genomförande. En

[87] Wedebrand & Veibäck. 2018. s. 10-11.
[88] Ekholm, Jebari & Markovic. 2018. s. 9.

förutsättning för att kunna utforma en plan B är att veta vilken verksamhet som faktiskt genomförs. Därtill behövs en förståelse för vad som utgör kärnverksamhet som måste fungera, exempelvis för en myndighet i syfte att uppfylla dess instruktion, regleringsbrev och regeringsuppdrag. Därefter kan utformningen av en plan B påbörjas utifrån vilka störningar som bedöms kunna inträffa och ha en påverkan på kärnverksamheten. Plan B ska beskriva reservrutiner eller andra typer av förändringar som behöver träda i kraft för att hantera de identifierade störningarna i verksamheten. En reservrutin kan innebära att verksamheten begränsas till att genomföra vissa delverksamheter, och att alternativa IT-system eller att helt manuella arbetssätt används för att uppnå den nödvändiga förmågan.

För att säkerställa den dagliga driften i fredstid kan plan B utgöras av kontinuitetsplanering. För situationer av gråzon eller krig kan det exempelvis vara beredskapsplanen som träder i kraft som en plan B. Målbilden med en plan B är således att kunna säkerställa viss förmåga vid olika typer av störningar.

### 3.6.1 Problem i fredstid

Den problembild som målas upp i rapporterna kring plan B kan sammanfattas i fyra problem.

#### 3.6.1.1 Plan B är kostnadsdrivande

En väl fungerande plan B är kostnadsdrivande. Att ha alternativa arbetssätt som verksamheten kan övergå till vid störning innebär ytterligare rutiner, IT-system och kompetens som ska underhållas. Då ett vanligt syfte med digitalisering är just att effektivisera och minska kostnader blir plan B något som motverkar digitaliseringens effektiviseringar och besparingar.[89]

#### 3.6.1.2 Det finns ingen plan B

Alla verksamheter har inte någon plan B. Anledningen till att en plan B saknas kan bero på att det i den egna verksamheten saknas kunskap om den nya teknik som används.[90] När kunskap om tekniken saknas vet den egna organisationen inte hur problem kan eller får åtgärdas.[91] Det blir då svårt för den egna organisationen att utforma en plan B.

Något som också påverkar möjligheterna att utforma en plan B är att dagens ordinarie lösningar numera sällan är ett resultat av att en manuell arbetsprocess har digitaliserats. Att ha en plan B som baseras på återgång till en manuell

[89] Eidenskog, Eckersand & Mittermaier, 2023, s. 42.
[90] Mickelsson & Bengtsson, 2021, s. 38.
[91] Mickelsson & Bengtsson, 2021, s. 38.

arbetsprocess är således inte en självklarhet. Att det ofta saknas en tidigare manuell process innebär att beroendet till de befintliga IT-systemen är totalt. Det är inte heller säkert att det i verksamheten finns kunskap om innehållet i de bakomliggande processerna som IT-systemen implementerar.[92]

#### 3.6.1.3 Plan A och B har samma beroenden

I de fall verksamheter har en plan B så kan detta alternativa arbetssätt ha samma beroenden som ordinarie arbetssätt. Om exempelvis plan B innebär att ett alternativt IT-system ska användas så har detta, genom att också vara ett IT-system, troligtvis flera liknande beroenden som det ordinarie.[93] Exempel på sådana beroenden kan vara grundförutsättningar såsom tillgång till el och fungerande anslutning till Internet, eller mer specifika beroenden såsom fungerande anslutning till en viss bank eller tillgång till autentisering via Bank-id. Om plan B istället skulle vara att återgå till ett manuellt förfarande som tidigare har använts så har detta arbetssätt förmodligen helt andra beroenden än det ordinarie arbetssättet.[94] Beroenden för ett manuellt förfarande kan vara av typen tillgång till papper och penna, eller att ha tillgång till viss mängd personal. Det är därmed bättre förutsättningar att en plan B med andra beroenden än ordinarie plan A skulle fungera vid en störning.[95]

#### 3.6.1.4 Bemanning för manuell drift saknas

Verksamheter som i teorin kan genomföras manuellt utan tillgång till IT-system kan sakna nödvändig bemanning för att genomförandet ska fungera i praktiken.[96] Digitalisering sker ofta med målbilden att effektivisera, exempelvis genom att automatisera uppgifter som tidigare har genomförts manuellt.[97] Effektiviseringen har då lett till att verksamheten har kunnat minska bemanningen, vilket innebär en brist på personal vid återgång till manuell drift.[98] Eventuella toppar i arbetsbördan hanteras i dagsläget genom att hyra in tillfällig personal i form av konsulter eller bemanningspersonal, men under en kris kan det vara många som är beroende av konsulter och bemanningspersonal och då är det inte säkert att verksamheten kan få den hjälp som krävs.[99,100]

I dagsläget finns fortfarande personal som har varit med då olika verksamheter genomfördes manuellt, exempelvis dricksvattenproduktion. Den yngre

[92] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 88-90.
[93] Karlzén. 2022. s. 23.
[94] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 88-90.
[95] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 88-90.
[96] Eckersand & Stenérus Dover. 2020. s. 29.
[97] Veibäck, Stenérus Dover & McWilliams. 2021. s. 37.
[98] Eckersand & Stenérus Dover. 2020. s. 29.
[99] Eckersand & Stenérus Dover. 2020. s. 12-13.
[100] Veibäck, Stenérus Dover & McWilliams. 2021. s. 37.

generationen har dock inte den erfarenheten, vilket kommer att öka svårigheten att övergå till manuell drift framöver.[101]

### 3.6.2 Problem i gråzon och krig

I gråzon och krig kommer konsekvenserna av de fredstida problemen troligtvis att öka. En anledning är att orsaken till störningar inte längre enbart beror på icke-antagonistiska händelser såsom olyckor, misstag och väderfenomen. I gråzon och krig behöver det även tas höjd för antagonister som med uppsåt försöker orsaka störningar. En annan anledning är att normalläget i Sverige är fred och att det då är fredstida störningar orsakade av typiska fredstida orsaker som den praktiska erfarenheten till stor del baseras på.

För de verksamheter som inte har någon plan B är det rimligt att anta att de kommer att fortgå tills en störning inträffar, varefter verksamheterna reduceras eller avstannar fram till dess att normalläget återställs eller att en plan B har utformats utifrån då rådande förutsättningar. Förutsättningarna att utforma en plan B är då troligtvis mindre fördelaktiga än om planering och förberedelse hade skett redan i fredstid.

Verksamheter som har en plan B, men där planen har motsvarande beroenden som ordinarie arbetssätt, kommer troligtvis att vara i ett bättre läge än de verksamheter som inte hade någon plan B alls. Däremot kan det vara så att påverkan på något av arbetssättens gemensamma beroenden omöjliggör båda. Att bygga IT-system som är robusta och har hög tillgänglighet är kostnadsdrivande, vilket resulterar i att IT-system i regel inte är dimensionerade utifrån hotbilden i gråzon eller krig. Att förlita sig på att IT-system fungerar i gråzon eller krig kan således innebära ett risktagande.[102]

För verksamheter som har en plan B som innebär återgång till manuellt förfarande nämndes redan för fredstid att otillräcklig bemanning är ett problem, men att det är något som hanteras genom inhyrd personal efter behov. Det är en lösning som är rationell i fredstid, men som kan vara problematisk i gråzon eller krig då även konsultbolagen och bemanningsföretagen har dimensionerat bemanningen utifrån ett normalläge för deras uppdragsgivare i fred. I gråzon eller krig kommer det troligtvis inte enbart vara en verksamhet som påverkas, utan snarare flera delar av samhället samtidigt – och möjligtvis även flera länder samtidigt. Tillgången till personal att hyra in kan vid en sådan situation vara begränsad, vilket påverkar möjligheten att bemanna verksamhet i en plan B om inte den egna ordinarie personalstyrkan är tillräcklig.

[101] Olsén, Valassi & Stenérus Dover. 2023. s. 32.
[102] Eidenskog, Eckersand & Mittermaier, 2023, s. 42.

Oavsett hur bra plan B en verksamhet har är det troligtvis nödvändigt att detta alternativa arbetssätt övas så att personalen är medvetna om och insatta i det alternativa arbetssättet.

## 3.7 Exponering av komponenter och information

Den snabba utvecklingen inom digitaliseringen har gjort det möjligt att effektivisera många offentliga verksamheter. Det har också i många fall införts nya funktioner som ger mervärden. Exempel på sådana mervärden är att mäta luftkvaliteten på vissa platser i en stad och dirigera om fordonstrafiken när mätvärdena är för höga.[103] Många tekniska enheter och IT-system kan numera kopplas upp via Internet och därmed avläsas, fjärrstyras, uppgraderas och felsökas på distans. Vissa funktioner kan dessutom automatiseras, vilket minskar behovet av personal och sänker kostnaderna. Teknikutvecklingen gör att IT-system blir mer och mer komplexa till sin natur, samtidigt som det blir enklare och billigare att köpa färdiga lösningar. Sammantaget öppnar teknikutvecklingen upp möjlighet till ny funktionalitet och systemlösningar.

### 3.7.1 Problem i fredstid

Utvecklingen som beskrivs ovan kan ses som både positiv och oundviklig. Regionerna är numera inte beroende av att en läkare befinner sig på samma fysiska plats som sina patienter för att kunna utföra en läkarundersökning. Elproducenter kan optimera elproduktionen utifrån analyser av data över hur de enskilda konsumenterna förbrukar el över tid, och mycket av kommunikationen mellan myndigheter och medborgare kan nu göras digitalt. Sammantaget har digitaliseringen fört med sig många fördelar. Men det finns även uppenbara sårbarheter inbyggda i utvecklingen. En av dem är den ökade exponeringen av delkomponenter i IT-system. En annan den ökade exponeringen av data som lagras i IT-systemen. Exponering baseras i huvudsak på att många IT-system är sammankopplade med varandra, via lokala nätverk eller över Internet. Eventuella säkerhetsluckor i ett IT-system kan då göra att alla IT-system blir exponerade för angripare som kan göra intrång, manipulera data eller sprida desinformation.

#### 3.7.1.1 Anslutning till Internet

Många tekniska system som tidigare har varit autonoma kopplas nu upp mot Internet i större utsträckning. Ett exempel är cyberfysiska system, det vill säga datorbaserade system som kan hämta data från sin omgivning med hjälp av sensorer och interagera med maskiner, fordon och annan utrustning.[104] Sådana

[103] Mickelsson & Bengtsson, 2021, s. 28.
[104] Myndigheten för samhällsskydd och beredskap. 2019. s. 3.

informations- och styrsystem kopplas i allt högre utsträckning upp mot andra IT-system, men där finns inte alltid samma tradition av säkerhetstänkande som inom IT-sektorn, varför det kan uppstå sårbarheter när tekniken exponeras mot exempelvis Internet.[105] Att IT-system och hårdvara kopplas ihop i allt större utsträckning, och dessutom är uppkopplade mot Internet, ökar sannolikheten för att en angripare ska kunna ta sig in i systemen. Det kan räcka med att en av komponenterna innehåller en sårbarhet för att en angripare även ska kunna komma åt de andra systemen.[106] Även verksamheter som i sig inte är känsliga kan bli utsatta för intrång om en angripare kan gå via dem för att komma åt andra verksamheter som hanterar skyddsvärd information.[107] Fysiska enheter kan utsättas för angrepp som gör dem obrukbara, eller får dem att fungera felaktigt. I värsta fall kan angreppet också orsaka fysisk skada.[108] Sårbarheten kan också utnyttjas för cyberterrorism eller ransomware,[109] det senare i syfte att kryptera information i systemet eller låsa ute användarna och sedan kräva pengar för att göra informationen åtkomlig igen.

#### 3.7.1.2 Avsaknad av säkerhetskultur

Ett problem som nämns i avsnitt 3.2.1.2 är att komponenter eller hela IT-system används på ett sätt som de inte har designats för. Många industriella informations- och styrsystem är designade för att köras i fristående nätverk, där operatören är tvungen att vara på plats för att kunna koppla in sig i nätverket och läsa av och styra systemen. Nu kopplas många system istället upp mot Internet för att operatören ska kunna sitta på distans var som helst i världen. Många aktörer är omedvetna om riskerna det innebär och inför därför inte åtgärder för att skydda sig mot IT-intrång. Avsaknaden av säkerhetskultur kan bero på att de som arbetar med systemen kommer från sektorer som inte tidigare har drabbats av incidenter.[110] Att lägga till säkerhet i efterhand är dessutom mycket svårare än att bygga in den från början.[111]

#### 3.7.1.3 Färdiglösningar

Marknaden för smarta hem har växt explosionsartat. Det finns gott om billiga elektronikkomponenter som riktar sig till vanliga konsumenter, och som går att köpa på närmaste elektronikvaruhus. Det kan vara lockande att köpa dem, även när man arbetar med samhällsviktig verksamhet, eftersom man kan få mycket funktion till en låg kostnad. Färdiglösningar innebär dock ofta att användarna har

[105] Hedtjärn Swaling, Malmberg Andersson & Clausen Mork, 2016, s. 43.
[106] Mickelsson & Bengtsson, 2021, s. 35.
[107] Budryk, Dahl, Lackenbauer, Refors Legge & Lusua, 2023, s. 38.
[108] Vidar Hedtjärn Swaling, 2018, s. 32.
[109] Mickelsson & Bengtsson, 2021, s. 35.
[110] Mossberg Sonnek & Lindgren, 2015, s. 25.
[111] Mossberg Sonnek & Lindgren, 2015, s. 36.

mindre kunskap om hur IT-systemen fungerar, än när de utvecklat IT-systemen själva.[112] Utrustningen är inte alltid ordentligt testad, och nya tekniker har ofta olika typer av barnsjukdomar.[113] En respondent i en av studierna påpekar att det kan finnas sårbarheter i tekniken som är kända och kan fungera som en ingång för en hacker.[114] Ibland är aktörerna inte ens är medvetna om att en enhet har möjlighet att kopplas upp mot Internet, och den kan då användas i en säkerhetskritisk tillämpning i tron att den inte är uppkopplingsbar.[115]

En fördel med att det blir enklare och billigare att köpa färdiga lösningar, är att många användare tillsammans kan finansiera förbättringar av IT-systemen kontinuerligt. En nackdel är dock att eventuella sårbarheter som identifieras i lösningen då återfinns hos alla aktörer som använder lösningen. Eventuella IT-attacker som nyttjar sårbarheten kan slå brett mot flera aktörer, exempelvis samhällsviktiga verksamheter, samtidigt.[116]

#### 3.7.1.4 Stora mängder data

Att ha sina IT-system uppkopplade mot Internet gör det möjligt att samla in stora mängder sensordata. Förmågan att analysera och hantera data har förbättrats och blivit billigare, vilket exempelvis kan utnyttjas i den smarta staden för att följa upp och styra trafiken.[117] Insamlade data kan också associeras till individer för att kunna göra mer omfattande dataanalyser på individnivå. Sådana data kan också aggregeras. Exempelvis kan ett elkraftföretag samla in beteendemönster på individnivå, som kan användas för att planera kommande produktion.[118] Vid ett IT-intrång finns det då risk för att en obehörig aktör kan få tillgång till data som berör enskilda elkonsumenter, eller än värre, känslig information som patientjournaler inom vården.[119]

Det finns effektiviseringsvinster med att samla och analysera data. Men användandet av stora datamängder kan även vara intressant för en angripare, och IT-system där data lagras kan därför bli föremål för dataintrång. Känslig information, om såväl individer som verksamheter, kan vara av intresse. I det så kallade Vastaamo-fallet blev ett psykoterapicenter i Finland utsatt för dataintrång och utpressning, efter att patientjournaler och personuppgifter blivit stulna.[120] Utöver att samla in data kan en angripare också vara intresserad av att

[112] Hedtjärn Swaling, Malmberg Andersson & Clausen Mork, s. 47.
[113] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 82.
[114] Mossberg Sonnek & Lindgren, 2015, s. 33.
[115] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 82-83.
[116] Jonsson, 2018, s. 57.
[117] Mickelsson & Bengtsson, 2021, s. 37.
[118] Wedebrand & Veibäck, 2018, s. 17.
[119] Budryk, Dahl, Lackenbauer, Refors Legge & Lusua, 2023, s. 42.
[120] Yle. 2022.

manipulera data, i syfte att exempelvis skapa falska lägesbilder eller att sprida desinformation.[121]

#### 3.7.1.5 Inbyggnad i viss typ av teknik

Det finns en fara med att bygga in sig i en viss typ av teknik. Många IT-system som är uppkopplade mot nätet har utformats för tidigare standarder för mobil kommunikation. När standarderna uppgraderas, succesivt till 3G, 4G och 5G, finns det en risk att den nya standarden används med så kallade molntjänster. Det innebär att data som inte har varit tänkta att vara publika riskerar att exponeras i molnet, och det är inte ens säkert att användarna är medvetna om det. Och även om medvetenheten finns, så är det inte säkert att det är möjligt att hitta en annan lösning som kan ersätta den man har byggt in sig i.[122]

Ett annat exempel på tekniklösning som kan vara svår att ersätta är beroendet av globala positioneringssystem såsom GPS och Galileo. GPS-satelliter har atomur ombord, vilket ger tillgång till en synkroniserad, exakt tid, något som är en förutsättning för utbyggnaden av exempelvis smarta elnät. Tillgången till noggrann tid är en fördel i en ostörd miljö, men om GPS är den enda källan till synkroniserad tid, kan det få stora konsekvenser om GPS störs ut.[123]

#### 3.7.1.6 Ägande av utländska företag

En annan omständighet, som innebär både för- och nackdelar, är att många samhällsviktiga verksamheter numera ägs av större utländska företag. Fördelarna är att de utländska företagen ofta är större än de svenska företagen och ingår i gränsöverskridande koncerner. Dessa har ofta många kunder vilket gör att utvecklingskostnaderna fördelas på flera, samt stora nätverk. Deras verksamhet prioriteras då ofta av underleverantörerna, vilket ökar leveranstillförlitligheten.[124]

Men en utländsk ägare är också en presumtiv ingång för antagonistiska statliga aktörer. Företag från vissa länder lyder dessutom under lagar som innebär att de nationella myndigheterna har rätt att begära ut data från företagen. Denna typ av lagar finns exempelvis i USA, Kina och Indien och omfattar även utlämnande av data som berör svenska invånare.[125] Säpo har flaggat för att statliga aktörer kan skaffa sig inflytande i Sverige, och information om svensk säkerhetskänslig

[121] Mickelsson & Bengtsson, 2021, s. 37.
[122] Mickelsson & Bengtsson, 2021, s. 35.
[123] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 83.
[124] Budryk, Dahl, Lackenbauer, Refors Legge & Lusua, 2023, s. 10.
[125] Mickelsson & Bengtsson, 2021, s. 42.

verksamhet, genom att delta i och vinna upphandlingar hos svenska myndigheter.[126] I det sammanhanget kan nämnas att exempelvis kinesiska aktörer förvärvar och etablerar företag i Sverige.[127]

### 3.7.2 Problem i gråzon och krig

Uppkopplingen mot Internet gör det möjligt för IT-system över hela världen att kommunicera med varandra. IT-systemen kan samla in och skicka data till en analysfunktion som finns på en annan geografisk plats. IT-systemen kan dessutom underhållas och uppgraderas på distans. I en fredstida situation är möjligheterna näst intill obegränsade. Problemen uppstår när freden övergår i gråzon eller krig.

Exponeringen av IT-system och data gör att även sårbarheter, för användaren kända såväl som okända, exponeras. Men för att det ska bli allvarliga konsekvenser till följd av exponeringen krävs att exempelvis en hacker, en kriminell organisation eller en statlig aktör utnyttjar sårbarheterna. Det krävs alltså att någon med både kompetens och uppsåt utnyttjar hålen i IT-systemen för att orsaka skada. Förmodligen finns kompetensen hos olika aktörer redan under fredstid i syfte att användas framför allt i gråzon och krig. IT-intrång under ett gråzonsskede kan orsaka skada utan att det går att upptäcka vem som står bakom angreppen. IT-attackerna kan också maskeras som olyckshändelser eller incidenter.

I en krigssituation behöver en angripare inte dölja sina attacker i samma utsträckning, och eventuella IT-angrepp kan ske både öppet och dolt. En angripare har då även konventionella inslag som vapenverkan i sin verktygslåda. En skillnad mot gråzonen är att ägarna av IT-systemen troligtvis förväntar sig angreppen och vet vem som kan förväntas ligga bakom dem. Medborgarna lär också ha en större acceptans för att samhällets tjänster inte fungerar som i fredstid och att stora störningar kan förekomma.

Även om det kan finnas ekonomiska fördelar i att en verksamhet i Sverige köps av utländska ägare, kan utländskt ägande i gråzon och krig öppna upp ingångar för statliga antagonister till svensk samhällsviktig verksamhet.

Exponerade system eller systemdelar som i fredstid är ointressanta, kan vara intressanta i gråzon och krig då det finns ett ökat intresse för att störa på bred front och skapa oreda eller oro. Exponering av information eller av en komponent kanske därför inte uppfattas som problematisk förrän i ett mer eskalerat läge. Att sårbarheter och brister byggs in, men kanske inte exploateras i fredstid skapar alltså en falsk trygghet.

[126] Säkerhetspolisen. s. 5-6.
[127] Almén. 2023. s. 18.

## 3.8 Kompetensbrist

Den snabba digitalisering som samhället genomgår ställer höga krav på kompetens inom många olika områden. Det behövs teknisk kompetens för att kunna utveckla nya och underhålla gamla IT-system. Teknisk kompetens behöver även de som upphandlar IT-system ha, för att förstå vilka möjligheter tekniken ger, vilka tekniska krav som är möjliga att ställa på IT-systemen, samt vilka begränsningar och beroenden som finns.[128] De som upphandlar IT-system behöver dessutom ha kompetens inom juridik, och speciellt kring vilka regler som gäller vid offentlig upphandling i de fall upphandlingen görs inom en offentlig verksamhet.[129] Utöver det behövs kompetens inom humaniora (exempelvis etik) och samhällsvetenskap, speciellt vid utveckling av artificiell intelligens och AI-applikationer, eftersom de nya tillämpningarna berör politiska, sociala, juridiska och ekonomiska delar av samhället.[130]

### 3.8.1 Problem i fredstid

De höga krav som digitaliseringen ställer på kompetens är inte lätta att leva upp till. Utvecklingen går fort, och det tar tid att utbilda ingenjörer, jurister och andra yrkeskategorier. Efterfrågan på specialister inom informations- och kommunikationsteknik är idag större än utbudet, även om Sverige i en internationell jämförelse har en hög andel specialister inom området.[131] Ingenjörsbristen bedöms dessutom öka de närmsta åren.[132] Likaså saknas till stor del specialistkompetens för att bedöma och hantera risker i samband med att nya IT-system installeras.[133]

Ett annat problem är att specifika nyckelkompetenser inom olika områden, som en viss process eller leverantörsprodukt, ofta bara återfinns hos enstaka specialister.[134] I effektiviseringens fotspår skalas redundansen bort, och därmed blir verksamheter känsliga för att personer med spetskompetens slutar. När det gäller offentlig verksamhet, som oftast inte utvecklar sina IT-system själv, så är det för det mesta beställar- och upphandlingskompetens som lyfts som en brist i de studerade rapporterna.

[128] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 77.
[129] Malmberg Andersson & Stenérus Dover, 2016, s. 16.
[130] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 76.
[131] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 77.
[132] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 77.
[133] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 77.
[134] Eckersand & Stenérus Dover, 2020, s. 29.

#### 3.8.1.1 Bristande beställarkompetens

När digitaliserade system upphandlas för att stödja en verksamhet är det ofta den organisatoriska enhet som ansvarar för verksamhetsutvecklingen som står för upphandlingen. IT-ansvariga, som sitter i en annan del av organisationen, kopplas inte alltid in i alla delar av processen.[135] De ansvariga för en upphandling kan därför ha begränsade IT-kunskaper, och även begränsad kännedom om vilka lagar och regler som gäller i Sverige i dessa frågor. Exempelvis kan det vara rektorn i en skola som är ansvarig för att handla upp ett övervakningssystem, även om upphandling inte ligger inom rektorns huvudsakliga kompetensområde.[136] Konsekvensen kan bli att de säkerhetskrav som ställs på IT-systemet inte är anpassade för hur produkten ska användas. Och i de fall som rätt säkerhetskrav ställs, är det inte säkert att kraven verifieras vid leverans.[137]

Att upphandla ett IT-system kan vara så pass komplext att det kan vara svårt att inse vilken kompetens som behövs i alla avseenden. Om upphandlaren är medveten om sina begränsningar kan det hända att risk- och sårbarhetsperspektivet överlåts till ett konsultföretag. Även det kan innebära en risk eftersom konsultföretaget inte alltid har tillräcklig kunskap om den upphandlande organisationens verksamhet för att kunna göra en sådan analys.[138]

#### 3.8.1.2 Fragmenterad kompetens

IT-system och automationsutrustning utvecklas snabbt, nya IT-system avlöser varandra och äldre IT-system uppfattas snabbt som omoderna. Ofta är det leverantörernas supporthorisont som avgör hur länge ett IT-system kan hållas vid liv.[139] Detta blir problematiskt när kompetensen inom både gamla och nya IT-system ska upprätthållas. Inte alla nya civilingenjörer är intresserade av att lära sig hur gamla styrsystem fungerar. Samtidigt kan äldre ingenjörer å sin sida ha mindre intresse av att lära sig de nya IT-systemen.[140] Det innebär att kompetensen fragmenteras, och att olika personer har kompetens om olika IT-system men ingen har kunskap om helheten. Det finns också en risk att de gamla IT-systemen läggs i händerna på konsulter, och att kunskapen om dem då inte finns i den egna organisationen. I värsta fall känner ingen i organisationen till hur IT-systemen fungerar och de blir då som ”svarta lådor”.[141]

[135] Mickelsson & Bengtsson, 2021, s. 38.
[136] Mickelsson & Bengtsson, 2021, s. 39.
[137] Mickelsson & Bengtsson, 2021, s. 39.
[138] Mickelsson & Bengtsson, 2021, s. 37.
[139] Hedtjärn Swaling, Malmberg Andersson & Clausen Mork, 2016, s. 47.
[140] Hedtjärn Swaling, Malmberg Andersson & Clausen Mork, 2016, s. 44.
[141] Hedtjärn Swaling, Malmberg Andersson & Clausen Mork, 2016, s. 44.

#### 3.8.1.3 Balansering av säkerhetskrav

Om den som upphandlar ett IT-system inte kan kravställa vilka säkerhetsnivåer IT-systemet ska klara av, och inte heller hur dessa ska kontrolleras när IT-systemet levereras, så riskerar säkerheten att bli lidande.[142] Men kravställningar kan också vara orimligt höga, vilket gör att ingen leverantör kan eller vill leverera.[143] Ett exempel är de trygghetslarm som används inom hemtjänsten. Trygghetslarm bygger på att brukarna ska känna sig trygga med att alltid få hjälp när de behöver det. Därför ställs höga krav på tillgänglighet och redundans när larmen köps in. Ibland för höga krav, som operatörerna för de nät till vilka larmen kopplas inte klarar av att uppfylla.[144] Detta illustrerar vikten av att det finns en förståelse på beställarsidan både avseende nödvändiga säkerhetskrav och avseende vad tekniken och leverantörerna rimligen kan leverera, och hitta en balans däremellan.

#### 3.8.1.4 Utkontraktering

Säkerheten måste upprätthållas i hela kedjan av leverantörer och underleverantörer.[145] I syfte att effektivisera verksamheter strävar många organisationer efter specialisering.[146] I den strävan kan det vara mer ekonomiskt fördelaktigt att anlita konsulter och underleverantörer än att ha egen kompetens inom vissa områden, även för kommuner och regioner.[147]

Delar av verksamheter, exempelvis inom vården och elförsörjning, kan även utkontrakteras.[148,149] Vid utkontraktering är det svårt för verksamhetsutövaren att upprätta en fullständig kravställning av skyddsåtgärder gentemot leverantören, bland annat för att det kan vara svårt att identifiera alla skyddsvärden inom verksamheten.[150] Då finns en risk att vissa värden inte skyddas i den utsträckning de borde. En annan nackdel med att lägga ut verksamheter externt är att den egna organisationen får minskad insyn i den, samtidigt som myndigheters tillsyn av verksamheten, i de fall det är aktuellt, försvåras.[151] Om det finns utländska underleverantörer, som beställaren kanske inte ens är medveten om, så kan problemen förstärkas ytterligare.[152]

[142] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 77.
[143] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 88-89.
[144] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 88-89.
[145] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 77.
[146] Johansson & Jonsson, 2018, s. 27.
[147] Budryk, Dahl, Lackenbauer, Refors Legge & Lusua, 2023, s. 27.
[148] Budryk, Dahl, Lackenbauer, Refors Legge & Lusua, 2023, s. 37
[149] Ingemarsdotter, Eidenskog & Hedtjärn Swaling, 2020, s. 58.
[150] Budryk, Dahl, Lackenbauer, Refors Legge & Lusua, 2023, s. 38.
[151] Johansson & Jonsson, 2018, s. 27.
[152] Johansson & Jonsson, 2018, s. 27.

#### 3.8.1.5 Bristande säkerhetskultur

Utredningar som har gjorts av inträffade IT-incidenter visar att de ofta orsakats av att de ansvariga organisationerna slarvat med ”grundläggande IT-hygien”.[153] Med IT-hygien avses de mest grundläggande IT-säkerhetshöjande aktiviteterna såsom säkerhetskopiering, segmentering, säkerhetskritiska uppdateringar och riskanalyser. En förklaring till slarvet kan vara att kulturen i organisationen inte tar säkerhetsproblemen på allvar.[154] En annan förklaring kan vara okunskap eller ointresse.[155]

Ytterligare en förklaring kan vara att den som gjort kravställningen av ett nytt IT-system inte har haft förmåga att föreställa sig vilka hot som Sverige, och enskilda verksamheter, kan ställas inför.[156] Föreställningsförmågan har gissningsvis ökat sedan Rysslands angreppskrig mot Ukraina inleddes, och fler har fått upp ögonen för nödvändigheten av att kunna skydda samhällsviktig verksamhet även mot antagonistiska angrepp från statliga aktörer. Men många IT-system designades innan Ryssland angrep Ukraina. Då fanns det en mer utbredd mentalitet att det inte skulle inträffa någon större kris eller ofred i närtid.[157]

Slutligen kan den bristande säkerheten bero på att man har designat IT-systemen först, och försökt addera säkerheten i efterhand. Detta är något som har visat sig vara svårt att göra.[158]

### 3.8.2 Problem i gråzon och krig

Om den person som i fredstid ansvarar för upphandlingen av ett IT-system inte har tillräcklig kompetens, och inte heller tar hjälp av andra med rätt kompetens, är risken stor att kravställningen blir felaktig och inte lever upp till de lagar, regler, krav och behov som finns. Om det beställda IT-systemet inte motsvarar behoven i fredstid, så har det förmodligen inte heller förutsättningar att kunna fungera tillfredsställande under gråzon och krig. En bristande kravställning kan dessutom, likväl som en bristande säkerhetskultur, göra att det byggs in sårbarheter i IT-systemen som inte upptäcks under fredstid, men som kan utnyttjas av en angripare i gråzon eller krig, vilket diskuterades i avsnitt 3.7.2.

Det finns risker med att den tekniska utvecklingen går snabbt. Det kommer hela tiden ny teknik, och generationsväxlingen för IT-systemen går snabbt. Samtidigt kan nyutexaminerade känna ett motstånd till att lära sig hur de äldre IT-systemen fungerar, speciellt om de inte längre används. I gråzon eller krig, när de nyare IT-systemen angrips och slås ut, är det en styrka att kunna gå tillbaka de gamla IT-

[153] Karlzén, 2022, s. 22.
[154] Karlzén, 2022, s. 22.
[155] Eidenskog, Eckersand & Mittermaier, 2023, s. 47-48.
[156] Eckersand & Stenérus Dover, 2020, s. 28.
[157] Eckersand & Stenérus Dover, 2020, s. 28.
[158] Karlzén, 2022, s. 22.

systemen om de finns kvar. Om det saknas personal med kompetens att hantera dem, är det inte möjligt.

Utkontraktering uppfattas ofta som en ekonomisk åtgärd för att hålla kostnaderna nere i fredstid. Verksamheterna behöver då inte ha egen kompetens inom alla områden utan kan samsas om den med andra verksamheter. Vid ett höjt säkerhetsläge med parallella angrepp mot olika verksamheter, kan de personer som innehar rätt kompetens bli gränssättande för vilka verksamheter som kan fungera. Utomstående bolag som tillhandahåller konsulter, bemanningspersonal eller tjänster kan behöva välja vilka uppdragsgivare de ska prioritera. Det är inte säkert att det blir den svenska samhällsviktiga verksamheten. Om bolagen har många avtal kan de välja att prioritera att genomföra arbete hos den kund där kontrakten medför högre straffavgifter när de bryts. Om bolagen dessutom är utländska eller att deras personal är utländska medborgare kan även det påverka vilken kund som prioriteras, beroende på omvärldsläget.

Staten har rätt att krigsplacera personer. Under höjd beredskap, när krigslagarna initierats, kan de vara till hjälp för att säkerställa att personer med rätt kompetens prioriteras till rätt uppgifter. Problemet med bristande kompetens kan därför vara enklare att hantera i samhällsviktig verksamhet under krig än i gråzon.

# 4 Fallgropar i gråzon och krig

I kapitel 3 beskrivs åtta problemområden som identifierats utifrån problem i tidigare genomförda studier relaterade till digitalisering. Där förs även resonemang kring hur problemen i dessa problemområden kan tänkas utvecklas i gråzon eller ytterst krig. I beskrivningen av problemområdena framgår att vissa tillvägagångssätt är problematiska, men att de i fredstid ändå i många fall kan anses vara funktionella eftersom det då inte inträffar störningar så ofta. Vid en övergång till gråzon eller krig förändras dock hotbilden och sannolikheten ökar att antagonistiska aktörer med uppsåt försöker orsaka störningar. De fredstida tillvägagångssätten blir då inte alltid längre ändamålsenliga. Ett sådant exempel är lagerhållning enligt principen just-in-time som i fredstid kan ses som rationell då det är kostsamt att hålla större lager än vad som normalt behövs. Vid kriser, i gråzon eller krig kan dessa begränsade lager skapa problem, något som exempelvis uppdagades under coronapandemins komponentbrist.

En vanlig målbild med digitaliseringsarbete är att uppnå ökad service, kostnadsbesparingar och effektivisering. Målbilden är ändamålsenlig i fredstid för att på bästa sätt hushålla med tillgängliga medel, och resulterar i att gamla IT-system och andra alternativa lösningar avvecklas då de utgör onödiga kostnader. Dessutom kan personalstyrkan som arbetade med de gamla IT-systemen komma att reduceras som ett resultat av effektiviseringen. Vid en övergång till gråzon och krig är det dock av vikt att verksamheterna är robusta och kan klara störningar i form av uppsåtliga angrepp. De fredstida effektiviseringarna och kostnadsbesparingarna kan resultera i att det i gråzon och krig inte längre finns några alternativa lösningar att återgå till vid behov. Väl genomförd digitalisering i fredstid kan således riskera att motverka beredskapsarbetet, vilket kanske inte är uppenbart vid en första anblick. Under genomförandet av studien som presenteras i denna rapport har författarna identifierat 15 möjliga fallgropar med digitaliseringen som samhällsviktiga verksamheter kan riskera att hamna i.

De fallgropar som beskrivs är identifierade utifrån de problemområden med underliggande problem som beskrivs i kapitel 3. Fallgroparna representerar oftast inte ett enstaka problem eller problemområde, utan karakteriseras av att de återkommer i flera problemområden. De har valts utifrån att de uppfyller något av nedanstående kriterier:

- En följd av digitaliseringen som bedöms kunna skapa problem om omvärldsläget förändras från fred till gråzon eller krig.
- Ett tillvägagångssätt som bedöms rationellt i fredstid men inte i gråzon eller krig.
- Det bedöms finnas en konflikt mellan fredstida målsättningar med digitaliseringen och säkerhetsrelaterade behov i gråzon eller krig.

Författarna gör inget anspråk på att listan är komplett eller att fallgroparna återspeglar aktuell status för alla, eller ens majoriteten av, samhällsviktiga verksamheter i Sverige. Däremot utgör fallgroparna möjliga situationer som samhällsviktiga verksamheter kan riskera att hamna i om beredskapen för gråzon eller krig inte har beaktats under digitaliseringsarbetet. Fallgroparna kan användas som en utgångspunkt för att analysera förutsättningarna för att en verksamhet ska kunna fortgå i gråzon eller krig.

1. **Otydliga lagar och regelverk**
   Otydliga lagar och regelverk med stort tolkningsutrymme kring vad som är skyddsvärt och hur det ska skyddas kan resultera i en variation i hur exempelvis information hanteras i fredstid av olika aktörer. Otydligheten kan exempelvis bero på att lagar och regelverk inte hänger med teknikutvecklingen och därmed blir svårapplicerade på nya tekniska lösningar. Denna diskrepans i informationshantering kan innebära sårbarheter som antagonistiska statsaktörer kan utnyttja i gråzon eller krig.
2. **Snabb digitalisering utan återvändo**
   Digitaliseringsarbetet går snabbt medan säkerhetsarbete och testning inte alltid hinns med i tillräcklig utsträckning. Men för att hänga med i teknikutvecklingen introduceras de nya IT-systemen ändå. För att inte missa målsättningen att digitaliseringsarbetet ska leda till effektivisering och kostnadsbesparing avvecklas troligtvis de gamla lösningarna efter introduktionen av den nya. I gråzon och krig finns det inte längre några gamla lösningar att falla tillbaka på om de nya fallerar.
3. **Kort supporttid**
   Den snabba utvecklingstakten har lett till att tillverkare ger allt kortare supporttid för de komponenter som säljs. Kortare supporttid innebär att tillverkaren garanterar tillgång till exempelvis säkerhetsuppdateringar och reservdelar under en allt kortare tidsperiod. Snabb teknikutveckling och kort supporttid resulterar i att kunderna ofta byter ut komponenter snarare än reparerar dem när de går sönder. Det är enklare att köpa nya. Då kvalitet kostar har tillverkarna inga incitament att tillverka produkter av högre kvalitet än nödvändigt. Även möjligheten att kunna byta ut delar på komponenten eller ens köpa reservdelar från tillverkaren kan begränsas om en sådan möjlighet ändå inte är något som kunden nyttjar. Denna anpassning av kvalitet och reparationsmöjligheter kan vara rationell under fredstid, men i gråzon eller krig med störningar i leveranskedjorna kan komponentkvaliteten vara begränsande.
4. **Överskattad förmåga att arbeta manuellt**
   Digitalisering innebär ofta att arbetsuppgifter som tidigare genomförts manuellt automatiseras. Allteftersom den automatiserade lösningen används minskar kunskapen om och erfarenheten av att genomföra arbetsuppgiften manuellt. Att vid en störning övergå till ett manuellt förfarande var tidigare görbart, men blir med tiden mindre realistiskt.

Det är därmed troligt att förmågan att kunna genomföra arbetsuppgifter manuellt i gråzon eller krig överskattas.

5. **Överskattad robusthet från redundans**
   I fredstid uppnås robusthet ofta genom redundans, exempelvis genom att ha fiberanslutning från flera olika leverantörer. Att det är likadana lösningar innebär exempelvis samma behov av reservdelar och kompetens, vilket i fredstid är rationellt. Den redundanta lösningen har dock samma beroenden som den ordinarie, vilket kan bli problematiskt i gråzon och krig när hotbilden inkluderar antagonistiska statsaktörer. Ett angrepp mot ett beroende kan slå ut både den ordinarie och den redundanta lösningen. Robustheten som redundanta lösningar ger kan därmed överskattas i gråzon eller krig.
6. **Underskattat kommunikationsberoende**
   Digitaliseringens IT-system behöver kunna kommunicera via interna nätverk och ofta även externt via Internet. Hur beroendet till kommunikationsinfrastrukturen ser ut samt hur specifika verksamheter, såsom kärnverksamheten, påverkas av avbrott kan dock i många fall vara svåröverskådligt och komplext, vilket gör det svårt att förebygga. I gråzon eller krig har den fredstida hotbilden förändrats och det är rimligt att anta att antagonistiska statsaktörer kommer att ge sig på kommunikationsinfrastrukturen. Verksamheters förmåga att kunna fortgå under längre perioder med begränsad eller obefintlig kommunikationsinfrastruktur riskerar därmed att överskattas.
7. **Reservkraft dimensionerad utifrån fredstid**
   Tillgång till reservkraft kan vara dimensionerad utifrån fredstida scenarier där avbrott primärt beror på el-ledningar som av misstag grävs av eller påverkas av nedblåsta träd. I dessa scenarier används reservkraft i form av avbrottsfri kraft (UPS) och elkraftverk för att hantera kortare avbrott (minuter, timmar, dagar) snarare än längre avbrott (veckor eller månader). Vid längre avbrott, som kan vara rimligt att anta i gråzon eller krig, blir tillgången till bränsle till elkraftverken och distributionen av detta bränsle en flaskhals när flera verksamheter nyttjar reservkraft samtidigt.
8. **Just-in-time-lager blir en flaskhals**
   Lärdomarna från coronapandemin om vikten av lagerhållning kan snabbt falla i glömska. I takt med att pandemin ligger allt längre bak i tiden blir den extra kostnaden för lagerhållning allt svårare att motivera. Även om en verksamhet inte använder sig av just-in-time-lager är dagens beroenden så svåra att överskåda att det någonstans i beroendekedjorna kan finnas ett just-in-time-lager som innebär att komponentbrist kan uppstå. Vid övergång till gråzon och krig kommer allt fler verksamheter att ha ett samtidigt behov av produkter, exempelvis reservdelar från centrallager som är dimensionerade utifrån just-in-time-principen. Efterfrågan på produkter i form av reservdelar och insatsvaror kan

komma att överstiga befintliga lager. Bunkring skulle dessutom förvärra problemet.

9. **Underskattat behov av att öva plan B**
   En plan B ska vara ett alternativt arbetssätt att övergå till om det ordinarie arbetssättet av någon anledning inte kan utföras. Att ha en plan B kan vara betryggande, men om personalen inte övas på detta alternativa arbetssätt är det inte rimligt att tro att det kommer att fungera vid en skarp situation. Det är även vid användande av det alternativa arbetssättet som det kan bekräftas att det fungerar samt vilken påverkan ändringen av arbetssätt har på verksamhetens genomförande. Likt en utrymningsövning är det nödvändigt att öva så att personalen vet vad de förväntas göra när en skarp situation uppstår. Verksamheter som har en plan B kan underskatta vikten av att detta alternativa arbetssätt övas.
10. **Olika verksamheters plan B har inte koordinerats**
    Verksamheter utformar en plan B för hur verksamheten ska kunna fortgå när ordinarie arbetssätt inte kan utföras, men planens realiserbarhet och funktion beror inte enbart på den egna verksamheten. I gråzon eller krig är det mer troligt att det är flera verksamheter som samtidigt arbetar enligt sin plan B, vilket kan göra det nödvändigt att ha koordinerade planer. Om två myndigheter är beroende av att kommunicera med varandra så behöver deras respektive plan B vara koordinerade så att exempelvis inte ena parten har övergått till kommunikation via radiolänk medan den andra kommunicerar via brev.
11. **Den fredstida bekvämlighetens sårbarheter**
    Under fredstid är det smidigt att ha IT-system uppkopplade mot Internet för att på så sätt möjliggöra allt från sammankoppling av geografiskt skilda IT-system till fjärradministration. Vid övergång till gråzon och krig förändras hotbilden till att i större grad inkludera antagonistiska statsaktörer. Den fredstida smidigheten kan då innebära en möjlighet för angripare att på distans utnyttja eventuella sårbarheter i de exponerade IT-systemen. Smidigheten övergår till att möjliggöra för angripare att förhindra, störa eller manipulera aktuell verksamhet.
12. **Omedveten okunskap om hotbild**
    Det är svårt att ge IT-systemen adekvat säkerhet utan god förståelse om hotbilden i olika skeenden. För digitaliseringsprojekt är ökad service, kostnadsbesparingar och effektivisering troligtvis i fokus snarare än säkerhet. Säkerhet hanteras efter hand, efteråt eller inte alls, något som kan bero på en omedveten okunskap om hotbilden. Att bedöma hotbilden i fredstid kan vara nog så svårt, men under framför allt gråzon blir det svårare. En omedveten okunskap om hotbilden kan resultera i upphandling av sårbara IT-system utan adekvat säkerhet dimensionerad för att även fungera i gråzon och krig.

13. **Beroendekedjan är lång**
    Att vara medveten om vilka beroenden verksamheten har är nödvändigt för att kunna förbereda sig på olika typer av störningar. En svårighet, som bland annat är ett resultat av digitaliseringen, är att kunna utröna hela beroendekedjan. Ett IT-system består idag av ett så stort antal komponenter och programvaror från olika tillverkare, som i sin tur har andra beroenden, att det är svårt att få en överblick över och kunna kontrollera hela beroendekedjan. Dessa beroenden kan vara spridda geografiskt över hela jorden. Samtidigt blir det allt viktigare att ha kontroll över beroendekedjorna i gråzon och krig. Verksamhetens exponering utifrån beroendekedjorna riskerar att underskattas.
14. **Obetydliga IT-system blir betydliga**
    Exponerade IT-system som i fredstid bedöms vara ointressanta, kan under gråzon eller krig bli intressanta för en motståndare. Intresset kan exempelvis bestå i att hitta information eller att vara en del i att störa eller skapa oro i samhället. Att angripa ett sådant IT-system kan upplevas som oproblematiskt, men vid flera samtidiga angrepp kan en minskad tilltro uppstå kring företags, myndigheters eller hela Sveriges förmåga att försvara sig. De under fredstid ointressanta IT-systemen kan helt enkelt uppfattas som säkra enbart på grund av att ingen aktivt letar och nyttjar sårbarheter i dem under fredstid.
15. **Överbokad inhyrd kompetens**
    Att vid behov hyra in den kompetens och bemanning som den egna verksamheten saknar kan i fredstid vara en rationell åtgärd för att minska kostnader. I gråzon eller krig, med parallella angrepp mot olika verksamheter, är det dock inte säkert att konsulter och bemannings-personal räcker till för att stödja alla uppdragsgivare samtidigt. Detta beror på att konsultbolagen och bemanningsföretagen dimensionerar sin personal utifrån att kunna hantera uppdragsgivarnas normalläge. Tillgången till inhyrd kompetens i gråzon och krig kan således överskattas.

# 5 Diskussion

Drivkrafterna bakom digitaliseringen är ofta ökad service, effektivisering och kostnadsbesparingar. I realiteten är det de drivkrafterna som styr hur IT-system och kommunikationsinfrastruktur utformas, snarare än en helhetssyn över hur det digitaliserade samhället ska kunna stå emot angrepp i ett höjt säkerhetsläge. Offentliga utredningar och rapporter har pekat på problem som digitaliseringen för med sig. Problemen kan ändra karaktär i ett gråzonsskede eller i krig, något som kan vara svårt att förutsäga i fredstid. I många fall finns också en konflikt mellan åtgärder som betraktas som rationella i fredstid och säkerhetsrelaterade problem i gråzon och krig.

I avsnitten som följer diskuteras rapportens tre frågeställningar:

1. Vilka fredstida problem har digitaliseringen i Sverige fört med sig?
2. Hur kan digitaliseringens fredstida problem uppträda i gråzon och krig?
3. Finns det några fallgropar med digitaliseringen som påverkar möjligheterna att genomföra verksamheter i gråzon och krig?

## 5.1 Problem i fredstid

Den första frågeställningen, som handlar om vilka fredstida problem digitaliseringen i Sverige har fört med sig, besvaras i kapitel 3. Problemen är kategoriserade i åtta problemområden, mellan vilka det finns både beroenden och i viss mån överlapp:

1. Otydlig styrning och bristande samordning
2. Snabb teknikutveckling
3. För högt ställda förväntningar
4. Bristfällig infrastruktur
5. Externa beroenden
6. Bristfällig plan B
7. Exponering av komponenter och information
8. Kompetensbrist

Den fredstida problembild som målas upp visar på en komplexitet av beroenden och samband. Komplexiteten byggs upp av det stora antalet sammankopplade datorer, infrastrukturen som ska möjliggöra kommunikationen mellan dem, olika typer av teknik och mjukvara, och sist men inte minst, användarna av IT-system som har olika behov och olika kompetens. IT-systemen har dessutom ett stort antal externa beroenden som ofta är svåröverskådliga. Utöver elektricitet och kommunikationsinfrastruktur, exempelvis Internet, så finns det även beroenden till underleverantörer av tjänster och till leverans av exempelvis reservdelar.

Sammantaget ser vi att många av de problem som redovisas med digitaliseringen indirekt är orsakade av den snabba teknikutvecklingen. Teknikutveckling har

gjort det möjligt att automatisera processer, övervaka IT-system och samla in data, möjligheter som i grunden är positiva. Men i och med att utvecklingen går så snabbt hänger inte lagstiftning och säkerhetsarbete med. Att lagstiftningen är anpassad för den gamla, snarare än den nya, tekniken ger upphov till ett tolkningsutrymme för den enskilda aktören om vad som är skyddsvärt. Den höga hastigheten, med vilken tekniken byts ut, gör det också svårt att hinna identifiera sårbarheter och barnsjukdomar i tekniken, samt att utbilda tillräckligt många personer inom de kunskapsområden som krävs för att beställa och hantera IT-systemen. Dessutom avvecklas ofta de gamla IT-systemen, varpå kompetensen om de tidigare rutinerna försvinner, vilket gör det svårt att ha en realistisk plan B för att hantera en nedgång i IT-systemen.

De höga förväntningarna som finns i samhället på digitaliseringen, tillsammans med tilliten till tekniken, gör att många verksamheter hakar på teknik-utvecklingen utan att ha tillräcklig kompetens om säkerhetsfrågor och hur de ska inkluderas i upphandlingen. Risken finns då att de IT-system som köps in har kända eller okända säkerhetsluckor, är beroende av underleverantörer som inte kan leverera tjänster eller produkter i en krissituation, kräver högre kapacitet än vad infrastrukturen klarar av eller saknar tillräcklig redundans vid störningar.

## 5.2 Problem i gråzon och krig

Den andra frågeställningen, som handlar om hur digitaliseringens fredstida problem kan uppträda i gråzon och krig, diskuteras också i kapitel 3. Diskussionen baseras på beskrivningarna av de enskilda problemen i fredstid, och redovisas separat för varje problemområde. På samma sätt som det finns beroenden och överlapp mellan de fredstida problemen, finns det också beroenden och överlapp mellan problemen när de uppträder i gråzon och krig.

Gråzon präglas av oro, otrygghet och en osäkerhet kring vad som är sant. Den mest påtagliga förändringen vid övergången är den förändrade hotbilden, som då även inkluderar antagonistiska statsaktörer. Detta är aktörer som, även under fredstid, har nödvändig kapacitet och resurser för att kunna genomföra angrepp mot svenska IT-system. I gråzonen är dock intentionen högre än i fredstid. Syftet med angreppen i gråzon kan vara att i det fördolda ha en påverkan som skapar oro i samhället, exempelvis genom att sprida desinformation. Även om det i gråzon blir ett ökat antal angrepp så försöker statsaktörer undvika att bli upptäckta.

IT-system som under fredstid vanligen inte utsätts för angreppsförsök kan i ett gråzonsläge bli måltavlor om angreppen slår brett mot många, förhållandevis oviktiga, IT-system. På så vis kan angriparen uppnå målet att skapa oro och otrygghet samt att misskreditera svenska myndigheter och företag. Samtidigt som

hotbilden under gråzon förändras jämfört med fredstid, så har den samhällsviktiga verksamheten fortfarande fredstida lagar och regelverk att förhålla sig till. Handlingsutrymmet att motverka gråzonens hotbild är således begränsat.

Om kriget bryter ut förändras förutsättningarna. Det blir delvis tydligare vem motståndaren är, även om andra aktörer som inte är direkt inblandade i kriget också kan passa på att utnyttja situationen. Samtidigt sker en förändring av handlingsutrymmet i och med att regeringen deklarerar höjd beredskap och när krigslagstiftningen träder i kraft. Med dessa lagar finns det större möjligheter att genomföra åtgärder för att motstå och hantera angreppen. Å andra sidan ökar förmodligen motståndarens intention att genomföra ytterligare angrepp eftersom behovet av att undvika upptäckt till viss del försvinner. Att som angripare kunna visa på lyckade angrepp kan vara något positivt ur propagandasyfte. Men det kan också vara så att en angripare förbereder en större koordinerad operation för att skapa oreda eller sprida desinformation, och därmed vill vara dold.

I gråzon eller krig förväntas de digitaliserade systemen utsättas för angrepp och stora påfrestningar. Hur pass väl angreppen mot IT-system eller infrastruktur kan hanteras i gråzon och krig beror till stor del på vilket förberedande arbete som har gjorts i fredstid. I stort påverkar det förberedande arbetet två aspekter. Den första aspekten är hur stor del av IT-systemen, infrastrukturen och informationen som är exponerade för en angripare. Det vill säga, i vilken utsträckning det är möjligt för en angripare att komma in i systemen för att förstöra dem, manipulera data eller sprida desinformation. Anledningen till att system och data är exponerade kan vara flera, exempelvis att oskyddade system kopplas upp mot Internet, att data inte är klassade och hanterade som skyddsvärda på grund av otydliga regelverk, eller att IT-systemet är ihopkopplade med andra IT-system till vilka en angripare kan ha tillgång via en underleverantör.

Den andra aspekten som påverkas av det förberedande arbetet är hur pass bra en aktör kan upprätthålla delar av sin verksamhet trots icke-fungerande IT-system, en utslagen kommunikationsinfrastruktur eller oåtkomliga digitala data. Det är en stor fördel om det redan på förhand finns en utarbetad och inövad plan B, samt en inbyggd redundans av system och kommunikationsvägar. Det är också viktigt att känna till vilka externa beroenden som finns, och om möjligt bygga redundans även för dessa. Om attackerade IT-system ska kunna repareras behövs både kompetens och reservdelar, något som behöver planeras för redan i fredstid. Likaså behöver det planeras för, och kravställas, att underleverantörer kan leverera sina tjänster även när samhället utsätts för stora påfrestningar.

## 5.3 Fallgropar i gråzon och krig

Den tredje frågeställningen, ”Finns det några fallgropar med digitaliseringen som påverkar möjligheterna att genomföra verksamheter i gråzon och krig?”, besvaras i kapitel 4. Där förs ett resonemang kring vad som kan gå snett i en verksamhet

som använder digitala system, och där verksamheten ska kunna upprätthållas oavsett om vi befinner oss i fred, i gråzon eller i krig. Tillvägagångssätt och lösningar som är adekvata i fredstid är inte nödvändigtvis det i gråzon eller krig, en målkonflikt som kan utgöra en fallgrop. I kapitel 4 presenteras 15 fallgropar som vi bedömer vara relevanta för samhällsviktiga verksamheter att beakta.

Fallgroparna som har presenterats pekar ut vissa systemegenskaper som byggts in i IT-system eller i omkringliggande verksamheter och som kan bli problematiska i gråzon och krig. Fallgroparna motsvarar inte enskilda problem som enkelt kan identifieras och åtgärdas, utan är en del av det fredstida samhället som har byggts upp. Systemegenskaperna kan innehålla sårbarheter som på ett mer oförutsägbart sätt nyttjas i gråzon eller krig.

En sådan sårbarhet kan vara att den snabba teknikutvecklingen gör att det inte nödvändigtvis lönar sig att reparera komponenter som går sönder, eftersom tillverkarnas korta supporttider gör att komponenten troligtvis ändå behöver bytas ut mot en annan inom kort. Och att tillverkaren av komponenterna då inte heller har incitament att tillverka komponenter som är möjliga att reparera. Detta är en sårbarhet som kanske inte märks i fredstid, men som kan skapa stora problem i en krigssituation när leveranskedjorna är störda samtidigt som IT-system och infrastruktur dessutom kan vara utsatta för fysisk åverkan.

En fallgrop kan också innebära att en sårbarhet blir synlig först när det inte längre är möjligt att backa och återgå till den tidigare lösningen om den nya inte fungerar. Så är fallet när ett nytt IT-system introduceras i syfte att minska kostnaderna, och ekonomin inte tillåter att det gamla IT-systemet behålls, eller att IT-systemen körs parallellt under en tid. Det kan då bli dyrt att återupprätta det gamla IT-systemet om man hittar sårbarheter i det nya, och det kan även bli dyrt att addera säkerhet i efterhand till det nya systemet om man inte tänkt igenom säkerheten ordentligt vid införandet av det.

Många problem kan samverka på ett svåröverskådligt sätt, och om man inte har en helhetssyn är det svårt att undvika konsekvenserna. Ett otydligt regelverk kan exempelvis tolkas olika av olika aktörer, och då finns det risk att någon aktör bedömer att skyddsnivån på ett system är låg, och kopplar upp det mot Internet. I och med det introduceras nya sårbarheter. En annan sak som kan vara svårt att se helheten av är alla de externa beroenden som ett IT-system kan ha, och vilka beroenden dessa externa beroenden i sin tur har.

En ytterligare kategori av fallgrop är när det finns en plan B för de fall IT-systemet fallerar, men att planen är framtagen för mindre krishändelser och inte för ett scenario där stora delar av samhällsviktig verksamhet i Sverige är utslagen. Risken är då att många verksamheter har en plan B som är beroende av samma externa resurser, i form av elkraftverk, personal med rätt kompetens eller mobil infrastruktur. Sådan redundans är en bra lösning i fredstid, men avsaknaden av diversitet blir en nackdel i gråzon och krig.

# 6 Avslutande ord

Alla samhällsviktiga verksamheter bör ha en beredskap för hur verksamheten ska kunna fortgå i gråzon och krig. Beredskapen kan stärkas exempelvis genom att göra risk- och sårbarhetsanalyser (RSA) och införa de åtgärder som analysen resulterar i, samt genom att ha en förberedd plan B. RSA ska enligt lagen genomföras kontinuerligt av statliga myndigheter, regioner och kommuner. Syftet med analyserna är att föreslå åtgärder som reducerar risker och minskar sårbarheter i syfte att öka förmågan att förebygga, motstå och hantera kriser och extraordinära händelser. En plan B skulle kunna vara en identifierad åtgärd för att hantera en kris som inte har kunnat förebyggas. Planen utgör ett alternativt arbetssätt som kan användas vid en störning som påverkar det ordinarie arbetssättet. En plan B kan exempelvis utgöras av att använda ett alternativt IT-system för att stödja verksamheten, eller att verksamheten använder sig av det arbetssätt som användes före digitaliseringen.

Det kostar att införa åtgärder för att reducera sårbarheter i digitala system. Åtgärder som exempelvis kan bestå av att utforma IT-system som autonoma system utan internetuppkoppling, att se över och minimera externa beroenden till underleverantörer, eller att dimensionera reservkraft utifrån ett krigsscenario, kan vara dyra att införa och motverka de kostnadsbesparingar som eftersträvas i fredstid. Men det kan också kosta att inte ha infört åtgärder den dag hotnivån höjs och samhällsviktig verksamhet blir svår att genomföra. I det senare fallet är det fördelaktigt att ha en fungerande plan B för hur verksamheten ska genomföras. Men även beredskap i form av en plan B kostar, både i utvecklandet av planen, säkerställandet av att det som behövs för att plan B ska fungera finns på plats, samt att personalen har övat på att arbeta enligt plan B.

Det kan också kosta att inte ha en plan B. Att inte vara förberedd med alternativa arbetssätt i gråzon och krig kommer troligtvis göra verksamheten handlingsförlamad, samtidigt som förutsättningarna att utveckla en plan B då är betydligt sämre. I denna rapport har det tydliggjorts att det finns ett stort antal beroenden mellan olika verksamheter och leverantörer, så för varje samhällsviktig verksamhet kommer det troligtvis även att finnas beroenden till andra samhällsviktiga verksamheter. Att inte ha en plan B kan således påverka fler samhällsviktiga verksamheters möjlighet att fortgå i gråzon och krig än enbart den egna.

Vid första anblicken ser kanske uppgiften att förbereda en verksamhet för att kunna fortgå i gråzon och krig överväldigande ut. Det kommer inte att, till en rimlig kostnad, vara möjligt att förutse alla risker, bygga bort alla sårbarheter och hantera alla möjliga problem som kan uppstå om IT-systemen inte längre fungerar. Det är därför nödvändigt att avgränsa uppgiften. Det är svårt för en extern person att göra en sådan analys då det krävs kunskap om verksamheten och insikt i hur den fungerar i praktiken. För att kunna göra en RSA och utforma en plan B behövs kunskap om vilken verksamhet som utgör kärnverksamheten.

Med kärnverksamhet avses den funktion eller nytta som måste tillhandahållas oavsett om det råder fred eller krig. För en myndighet kan det exempelvis vara det som uttrycks i form av regeringens instruktion, regleringsbrev och regeringsuppdrag.

När kärnverksamheten har identifierats är det möjligt att börja analysera vilka störningar som skulle kunna inträffa i gråzon eller krig, vilka sårbarheter som finns i verksamheten samt hur störningarna skulle kunna påverka verksamhetens genomförande. Analysen kan ligga till grund för att göra en RSA i vilken sårbarhetsreducerande åtgärder identifieras, eller för att utforma en plan B. Det är vid detta analysarbete som denna rapports beskrivningar av problemområden och fallgropar kan komma till användning. Problemområdena i kapitel 3 beskriver en palett av bristande förutsättningar, svårigheter och konsekvenser som finns på samhällsnivå eller i den enskilda organisationen. Fallgroparna som beskrivs i kapitel 4 kan användas som en checklista för att identifiera vilka problem som är allvarligast i den egna verksamheten. Ett ytterligare stöd som kompletterar problemområdena och fallgroparna är att använda sig av scenarier för hur gråzonshot kan tänkas gestalta sig[159]. De problem och fallgropar som beskrivs i denna rapport kan då användas som i inspel i scenarioanalyser.

[159] Gråzonsscenarier beskrivs exempelvis i Jonsson, Eriksson, Ingemarsdotter, Rossbach & Wedebrand. 2023.

# Referenser

Almén, O. *Kinesiska investeringar i Sverige: en kartläggning*. 2023. FOI-R--5474--SE.

Bengtsson, J., Eriksson, C., Olsson, M. (2022). *IT-system med externa anslutningar - Metod för analys av verksamheters beroenden*. FOI-R--5306--SE.

Budryk, M., Dahl, A., Lackenbauer, H., Refors Legge, M., Lusua, J. (2023). *Utländska investeringar och ägande i svensk hälso- och sjukvård - En studie om risker*. FOI-R--5448--SE.

ComputerSweden. 2019. *2,7 miljoner inspelade samtal till 1177 Vårdguiden helt oskyddade på internet.* https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-vardguiden-oskyddade-internet. Hämtad 2023-12-04.

Eckersand, U., Stenérus Dover, A-S. (2020). *NCS3 – Industriella informations- och styrsystem i kris och krig*. FOI-R--4935--SE.

Eckersand, U.,Mittermaier, E., Stenérus Dover, A-S., Wahrenberg, J. (2022). *Patient- och cybersäkerhet rörande medicinteknisk utrustning. En NCS3-studie om avvikelsehantering och CE-märkning*. FOI-R--5226--SE.

Eidenskog, D., Bildsten, C., Endres, B. (2019). *Säkra leveranskedjor för IT-system*. FOI-R--4851--SE.

Eidenskog, D., Eckersand, U., Mittermaier, E. (2023). *Digitaliseringens risker i hälso- och sjukvård*. FOI-R--5367--SE.

Ekholm, A., Jebari, K., Markovic, D. (2018). *Förbjuden framtid? Den digitala kommunen*.

ESV. 2018. *Digitalisering av det offentliga Sverige – En uppföljning, Ekonomistyrningsverket.* ESV 2018:31.

Försvarsberedningen. (2017). *Motståndskraft: Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021-2025*. Ds 2017:66, Försvarsdepartementet, Regeringskansliet.

Försvarshögskolan. 2023. *Förutsättningar för krisberedskap och totalförsvar i Sverige*. 930/2011.

Hedtjärn Swaling, V. (2018). *NCS3 Studie - IoT-relaterade risker och strategier*. FOI-R--4591--SE.

Hedtjärn Swaling, V. (2015). *Beroende av korrekt tid i elsystem*. FOI MEMO 5069.

Hedtjärn Swaling, V., Malmberg Andersson, F., Clausen Mork, J. (2016). *Gammalt är inte äldst*. FOI-R--4292--SE.

Hedtjärn Swaling, V., Mossberg Sonnek, K. (2016). *NCS3 Förstudie - Beroenden till industriella informations- och styrsystem*. FOI-R--4280--SE.

Ingemarsdotter, J., Eidenskog, D., Hedtjärn Swaling, V. (2020). *Vilse i lasagnen - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur*. FOI-R--4814--SE.

Johansson, B., Jonsson, D.K.(2018). *Beredskap i framtida energisystem. En analys med utgångspunkt i Energimyndighetens ”Fyra framtider”*. FOI-R--4589--SE.

Jonsson, D.K, Eriksson, C., Ingemarsdotter, J., Rossbach, N.H., Wedebrand, C. (2023). *Gråzonslägen i krig och fred*. FOI-R--5447--SE.

Jonsson, D.K. (2018). *Gråzonsproblematik och hybridkrigföring - påverkan på energiförsörjning*. FOI-R--4590--SE.

Jonsson, D.K., Ingemarsdotter, J., Johansson, B., Rossbach, N.H., Wedebrand, C., Eriksson, C. (2019). *Civilt försvar i gråzon*. FOI-R--4769--SE.

Karlzén, H. (2022). *IT när de externa anslutningarna går ner - Konsekvenser och reservalternativ i offentliga verksamheter*. FOI-R--5260--SE.

Kungliga Ingenjörsvetenskapsakademien (IVA). (2019). *Digitalisering för ökad konkurrenskraft*. IVA-M 499.

Malmberg Andersson, F., Stenérus Dover, A-S. (2016). *NCS3 - Översikt över arbetet med cyberfysiska system på kommunal nivå*. FOI-R--4370--SE.

Mickelsson, L., Bengtsson, J. (2021). *Svenska smarta städer - En explorativ studie om förväntad nytta och potentiella sårbarheter*. FOI-R--5117--SE.

Mossberg Sonnek, K., Holm, H., Lindgren, J., Lindgren, F., Westring, E. (2015). *NCS3 - informations- och styrsystem inom spårbunden trafik. En kartläggning*. FOI-R--4029--SE.

Mossberg Sonnek, K., Lindgren, F. (2015). *Industriella informations- och styrsystem inom fastighetsautomation – en förstudie*. FOI-R--4206--SE.

Myndigheten för samhällsskydd och beredskap (MSB). (2019). *Cyberfysiska system – vad är det?*. MSB1449.

Nevhage, B., Roffey, R., Johansson, J., Mittermaier, E. (2017). *Värna civilbefolkningen - En litteraturstudie med fokus på hot, sårbarheter, förmågor, resiliens, konsekvenser och åtgärder*. FOI-R--4437--SE.

Odell, A., Stenérus Dover, A-S. (2019). *NCS3 - Industriella styrsystem i svensk processindustri*. FOI Memo 6765.

Olsén, M., Valassi, C., Stenérus Dover, A-S. (2023). *NCS3-Ett skepp kommer lastat - En kartläggning av informationsflöden, cyberfysiska system och aktörer inom svenska hamnar*. FOI-R--5405--SE.

Post- och telestyrelsen. (2023). *PTS mobiltäcknings- och bredbandskartläggning 2022 – En geografisk översikt av tillgången till bredband och mobiltelefoni i Sverige*. PTS-ER-2023:13.

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

Reichel, B., Ingemarsdotter, J. (2023). *Samhällets beroende av rymdinfrastruktur*. FOI-R--5368--SE.

SFS 1992:1403. *Lag om totalförsvar och höjd beredskap.* Försvarsdepartementet.

Severin, M. (2018). *Tidig förvarning och icke-militära angreppssätt - Utmaningar för underrättelsetjänsten*. FOI-R--4577--SE.

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

Stenérus Dover, A-S., Ingemarsdotter, J. (2021). *Nationell försörjningsberedskap - FOI:s analys av försörjningsberedskapen som svar på regeringsuppdrag Ju2020/02565/SSK, Ju2018/05358/SSK*. FOI-R--5174--SE.

Sveriges television. (2021). *Leverantören: Coop är hårdast drabbat*. https://www.svt.se/nyheter/inrikes/leverantoren-coop-ar-hardast-drabbad. Hämtad 2023-11-28.

Säkerhetspolisen. 2019. *Hotbild mot säkerhetskänslig verksamhet*. Stockholm: Säkerhetspolisen.

Valassi, C., Karresand, M. (2020). *Cyberfysiska sårbarheter i tunga fordon - Med inriktning mot tunga fordon av vikt för civilförsvaret*". FOI-R--5067--SE.

Valassi, C., Karresand, M. (2019). *NCS3 - Komponenter på avstånd. Säkerhetsbeaktanden för direkt adresserbara trådlöst nätverks-anslutna komponenter i industriella informations- och styrsystem*. FOI-R--4757--SE.

Valassi, C., Westerdahl, L., Gudmundson Hunstad, A. (2019). *NCS3 - Förstudie Fjärrvärme*. FOI-R--4738--SE.

Veibäck, E., Stenérus Dover, A-S., McWilliams, A. (2021). *Gråzonsproblematik och hybrida hot i transportsystemet*. FOI-R--5118--SE.

Vetenskapsrådet. (2018). *Att motverka överbelastning av samhällsviktiga webbplatser – Slutrapport 2018 från projekt Särimner*.

Waleij, A., Simonsson, L., Liljedahl, B. (2019). *Konsekvenser av energibortfall på samhällets funktionalitet och civilbefolkningens hälsa*. FOI-R--4755--SE.

Wedebrand, C. (2020). *Planering under osäkerhet: Om att planera för det okända inom krisberedskapen, totalförsvaret och andra områden*. FOI-R--4972--SE.

Wedebrand, C., Lindgren, J., Granholm, N., Jonsson, K.D., Öhlund, E., Östensson, M., Odell, A. (2020). *Coronapandemins påverkan på försörjningen av kritiska varor och tjänster i Sverige: Tänkbara konsekvenser och åtgärder*. FOI Memo 7056.

Wedebrand, C., Reichel, B., Stenérus Dover A-S. (2021). *Omställningar under coronapandemin – Erfarenheter och lärdomar inför framtida kriser*. FOI-R--5247--SE.

Wedebrand, C., Veibäck, E. (2018). *Litteraturstudie om framtidens elförsörjning och elberedskap*. FOI-R--4565--SE.

Yle. 2022. *Dataintrånget mot Vastaamo: Det här har hänt och det här vet vi nu*. https://svenska.yle.fi/a/7-1496439. Hämtad 2023-11-23.

Öhlund, E., Wedebrand, C., Ryghammar, C. (2022). *Flexibel beredskap - En inledande analys av ett koncept för att ställa om industriproduktionen i Sverige under kriser och krig*. FOI-R--5351--SE.

# Bilaga 1. Studerade FOI-rapporter

Nedan redovisas de 35 FOI-rapporter som utgjorde underlag för studien som redovisas i denna rapport. I 16 av rapporterna identifierades problem knutna till digitaliseringen. För dessa rapporter redovisas vilken typ av studie som rapporten presenterade och inom vilken sektor studien gjordes.

| Författare/år | Titel | Typ av studie | Sektor |
|---|---|---|---|
| Bengtsson, J., Eriksson, C., Olsson, M. (2022). | *IT-system med externa anslutningar - Metod för analys av verksamheters beroenden.* | | |
| Budryk, M., Dahl, A., Lackenbauer, H., Refors Legge, M., Lusua, J. (2023). | *Utländska investeringar och ägande i svensk hälso- och sjukvård - En studie om risker.* | Intervjuer med tre regioner och fem företag. Rättsdogmatisk metod (för att undersöka rättsligt källmaterial) | Hälso- och sjukvård. |
| Eckersand, U., Stenérus Dover, A-S. (2020). | *NCS3 – Industriella informations- och styrsystem i kris och krig.* | Litteraturstudie, av lagar, förordningar och föreskrifter, vägledningar från statliga myndigheter. Fem intervjuer med två privata företag, MSB, Post- och Telestyrelsen (PTS) samt Livsmedelsverket. | ICS-tung verksamhet, övergripande. |
| Eckersand, U.,Mittermaier, E., Stenérus Dover, A-S., Wahrenberg, J. (2022). | *Patient- och cybersäkerhet rörande medicinteknisk utrustning. En NCS3-studie om avvikelsehantering och CE-märkning.* | | |

| Författare/år | Titel | Typ av studie | Sektor |
|---|---|---|---|
| Eidenskog, D., Eckersand, U., Mittermaier, E. (2023). | *Digitaliseringens risker i hälso- och sjukvård.* | Explorativ tematisk litteraturstudie, akademisk litteratur samt rapporter från myndigheter och organisationer. | Hälso- och sjukvård. |
| Hedtjärn Swaling, V. (2018). | *NCS3 Studie - IoT-relaterade risker och strategier.* | Litteraturstudie. | Övergripande. |
| Hedtjärn Swaling, V. (2015). | *Beroende av korrekt tid i elsystem.* | Litteraturstudie, främst forskningsartiklar och utredningar från olika branschaktörer. | Elförsörjning. |
| Hedtjärn Swaling, V., Malmberg Andersson, F., Clausen Mork, J. (2016). | *Gammalt är inte äldst.* | Litteraturskanning, Intervjuer med åtta aktörer inom VA, transport, energi (fjärrvärme och gasdistribution) och process-industri. | Övergripande. |
| Hedtjärn Swaling, V., Mossberg Sonnek, K. (2016). | *NCS3 Förstudie - Beroenden till industriella informations- och styrsystem.* | | |
| Ingemarsdotter, J., Eidenskog, D., Hedtjärn Swaling, V. (2020). | *Vilse i lasagnen - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur.* | Litteraturstudier (akademisk forskning, myndighets-dokument och rapporter), ett mindre antal intervjuer med MSB, Internet-stiftelsen och Netnord. | Brett samhälls-perspektiv. |

| Författare/år | Titel | Typ av studie | Sektor |
|---|---|---|---|
| Johansson, B., Jonsson, D.K. (2018). | *Beredskap i framtida energisystem. En analys med utgångspunkt i Energimyndighetens ”Fyra framtider”.* | Litteraturstudie, författarnas mångåriga erfarenheter inom området. | Energiförsörjning. |
| Jonsson, D.K, Eriksson, C., Ingemarsdotter, J., Rossbach, N.H., Wedebrand, C. (2023). | *Gråzonslägen i krig och fred.* | | |
| Jonsson, D.K. (2018). | *Gråzonsproblematik och hybridkrigföring - påverkan på energiförsörjning.* | Litteraturstudie. | Energiförsörjning. |
| Jonsson, D.K., Ingemarsdotter, J., Johansson, B., Rossbach, N.H., Wedebrand, C., Eriksson, C. (2019). | *Civilt försvar i gråzon.* | | |
| Karlzén, H. (2022). | *IT när de externa anslutningarna går ner - Konsekvenser och reservalternativ i offentliga verksamheter.* | Litteraturstudier, akademiska artiklar, myndighets-dokument. | Övergripande. |
| Malmberg Andersson, F., Stenérus Dover, A-S. (2016). | *NCS3 - Översikt över arbetet med cyberfysiska system på kommunal nivå.* | Sex intervjuer med representanter för sju kommuner. | Kommunal verksamhet. |
| Mickelsson, L., Bengtsson, J. (2021). | *Svenska smarta städer - En explorativ studie om förväntad nytta och potentiella sårbarheter.* | Litteraturstudie, intervjuer med representanter från tre kommuner (en-två respondenter per kommun). | Kommunal verksamhet. |

| Författare/år | Titel | Typ av studie | Sektor |
|---|---|---|---|
| Mossberg Sonnek, K., Holm, H., Lindgren, J., Lindgren, F., Westring, E. (2015). | *NCS3 - informations- och styrsystem inom spårbunden trafik. En kartläggning.* | | |
| Mossberg Sonnek, K., Lindgren, F. (2015). | *Industriella informations- och styrsystem inom fastighetsautomation – en förstudie.* | Litteraturstudie (inledande), Intervjuer med åtta personer på MSB och tre fastighetsägare/ förvaltare/ leverantörer. | Samhällsviktig verksamhet beroende av fastighets-automation. |
| Nevhage, B., Roffey, R., Johansson, J., Mittermaier, E. (2017). | *Värna civilbefolkningen - En litteraturstudie med fokus på hot, sårbarheter, förmågor, resiliens, konsekvenser och åtgärder.* | | |
| Odell, A., Stenérus Dover, A-S. (2019). | *NCS3 - Industriella styrsystem i svensk processindustri.* | | |
| Olsén, M., Valassi, C., Stenérus Dover, A-S. (2023). | *NCS3-Ett skepp kommer lastat - En kartläggning av informationsflöden, cyberfysiska system och aktörer inom svenska hamnar*. | Intervjuer (tio stycken), Studiebesök (fyra hamnar). | Transporter/sjö fart/hamnar. |
| Reichel, B., Ingemarsdotter, J. (2023). | *Samhällets beroende av rymdinfrastruktur*. | | |
| Severin, M. (2018). | *Tidig förvarning och icke-militära angreppssätt - Utmaningar för underrättelse-tjänsten.* | | |

| Författare/år | Titel | Typ av studie | Sektor |
|---|---|---|---|
| Stenérus Dover, A-S. (2019). | *NCS3 Studie: ICS och gråzonsproblematik.* | | |
| Stenérus Dover, A-S., Ingemarsdotter, J. (2021). | *Nationell försörjningsberedskap - FOI:s analys av försörjnings-beredskapen som svar på regeringsuppdrag Ju2020/02565/SSK, Ju2018/05358/SSK.* | | |
| Valassi, C., Karresand, M. (2020). | *Cyberfysiska sårbarheter i tunga fordon - Med inriktning mot tunga fordon av vikt för civilförsvaret*". | | |
| Valassi, C., Karresand, M. (2019). | *NCS3 - Komponenter på avstånd. Säkerhets-beaktanden för direkt adresserbara trådlöst nätverks-anslutna komponenter i industriella informations- och styrsystem.* | | |
| Valassi, C., Westerdahl, L., Gudmundson Hunstad, A. (2019). | *NCS3 - Förstudie Fjärrvärme.* | | |

| Författare/år | Titel | Typ av studie | Sektor |
|---|---|---|---|
| Veibäck, E., Stenérus Dover, A-S., McWilliams, A. (2021). | *Gråzonsproblematik och hybrida hot i transportsystemet*. | Litteraturstudie, workshoppar med aktörer inom transportområdet, diskussioner med Sjöfartsverket, Transport-styrelsen, Luftfartsverket och Trafikverket, dels med representanter från tre länsstyrelser. | Transporter. |
| Wedebrand, C. (2020). | *Planering under osäkerhet: Om att planera för det okända inom krisberedskapen, totalförsvaret och andra områden.* | | |
| Wedebrand, C., Lindgren, J., Granholm, N., Jonsson, K.D., Öhlund, E., Östensson, M., Odell, A. (2020). | *Coronapandemins påverkan på försörjningen av kritiska varor och tjänster i Sverige: Tänkbara konsekvenser och åtgärder*. | | |
| Wedebrand, C., Reichel, B., Stenérus Dover A-S. (2021). | *Omställningar under coronapandemin – Erfarenheter och lärdomar inför framtida kriser*. | | |

| Författare/år | Titel | Typ av studie | Sektor |
|---|---|---|---|
| Wedebrand, C., Veibäck, E. (2018). | *Litteraturstudie om framtidens elförsörjning och elberedskap*. | Litteraturgenomgång, 80-tal publikationer, vetenskapliga artiklar, offentliga utredningar, rapporter från myndigheter och energibranschen, säkerhetspolitiska analyser. | Elförsörjning. |
| Öhlund, E., Wedebrand, C., Ryghammar, C. (2022). | *Flexibel beredskap - En inledande analys av ett koncept för att ställa om industriproduktionen i Sverige under kriser och krig*. | | |

FOI

ISSN 1650-1942

www.foi.se