kahn pedersen

Beredskap och robust digital transformation i offentlig förvaltning

Advokatfirman Kahn Pedersens skriftserie 2023:1

På Advokatfirman Kahn Pedersen ser vi det som en naturlig del i vår roll som specialistbyrå att delta i den juridiska debatten för att bidra till att föra fram och utveckla särskilt svåra rättsfrågor inom våra specialistområden. Ett led i detta arbete är att regelbundet ge ut denna skriftserie. Tanken med skriftserien är att lite mer djupgående utreda aktuella och mer komplicerade rättsfrågor, som vi märker är av intresse för våra klienter och samhället i stort.

Målsättningen är att vårt arbete med skriftserien ska komma inte bara våra klienter och samarbetspartners till del, utan även ska kunna bidra till utvecklingen av de rättsområden som är våra specialistområden. Därför tillhandahålls alla nummer av skriftserie kostnadsfritt på vår webbplats under en Creative Commons Erkännande-Inga Bearbetningar 4.0 Internationell Licens, vilket möjliggör mångfaldigande och spridning av materialet förutsatt att inga ändringar görs och att källan anges.

Ämnet för denna rapport, som har nummer 2023:1, är beredskap och robust digital transformation i offentlig förvaltning.

ISBN 978-91-986495-3-6

Innehållsförteckning

Definitionslista

DIGG	Myndigheten för digital förvaltning
FEH	Förordningen (2006:637) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
LEH	Lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap
LOU	Lagen (2016:1145) om offentlig upphandling
LUF	Lagen (2016:1146) om upphandling inom försörjningssektorerna
LUFS	Lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet
MSB	Myndigheten för samhällsskydd och beredskap
NIS-lagen	Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
URL	Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk
Verksahets-utövare	Utövare av säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585)

1. Inledning och avgränsningar

1.1 Varför en rapport om robust digital transformation av offentlig förvaltning?

Sveriges minister för civilt försvar, Carl-Oskar Bohlin, erbjöd ett tänkbart svar på denna fråga i ett uttalande med anledning av ettårsdagen för Rysslands invasion av Ukraina:

> *Det säkerhetspolitiska läget i vår omvärld har försämrats i en snabbare takt än vad förmågan i det svenska totalförsvaret har tillvuxit under de senaste åren. I klartext, nu är inte tiden att vänta på andra, på den perfekta lösningen, den perfekta lagstiftningen, eller ta saknad finansiering till intäkt för att inte göra någonting. Det saknas inte åtgärder att vidta här och nu. Regeringen arbetar i en lång rad spår för att omhänderta frågor på strukturell nivå, men låt oss vara ärliga med att säga det uppenbara: Det svenska utredningsväsendet är inte anpassat för de snäva tidshorisonter vi måste förhålla oss till här och nu. Låt inte upplevda otydligheter kring mandat bli en ursäkt för passivitet. Gör hellre anspråk på ett otydligt mandat än att peka på någon annan. Arbeta med vad ni har, håll näsan i spåret och fråga er vad som ger mest förmåga per satsad krona och tidsintervall.*
>
> *Världen före den 24/2 2022 kommer inte tillbaka i någon närtid. Vi måste alla förhålla oss till världen av idag.*

Många av våra klienter, inte minst de som är upphandlande organisationer, brottas idag med att förstå de nya utmaningar och krav som den pågående upprustningen av Sveriges civila försvar innebär, och kommer att innebära, för just deras verksamheter.

Beredskapsfrågorna är både omfattande och komplexa och det finns många gånger endast begränsad vägledning att få. Inte minst gäller detta det juridiska och förvaltningsmässiga ramverk som myndigheter har att förhålla sig till under sitt beredskapsarbete, dvs. den administrativa beredskapen. Sveriges system för civil beredskap är i allra högsta grad under uppbyggnad men kraven på myndigheter att bidra till upprustningen av det civila försvaret finns här och nu.

Alla delar av det civila försvaret förväntas agera för att öka sin robusthet. Det är också vad som följer av den ansvarsprincip som utgör grunden för hur det civila försvaret ska fungera. Varje aktör ska, inom ramen för sin fredstida verksamhet, göra vad den kan för att bidra till en ökad motståndskraft vid höjd beredskap.

Det föll sig därför naturligt för oss att ägna denna rapport åt de risker som de senaste årtiondenas digitala transformation av den offentliga förvaltningen har fört med sig och vad som kan och måste göras för att minska dessa risker. Ytterst handlar det om att grundläggande funktioner i samhället, även sådana som förlitar sig på en digital infrastruktur, måste vara tillräckligt robusta för att även kunna hantera en krigssituation eller en annan situation då regeringen fattat beslut om höjd beredskap.

1.2 Avgränsning

Inom ramen för denna rapports begränsade format gör vi naturligtvis inte anspråk på att ge en fullständig redogörelse för den problematik som den digitala transformationen för med sig för totalförsvaret. Med det sagt, är vår förhoppning att kunna ge en översiktlig orientering i vissa av de frågor som myndigheter måste orientera sig i för att fullgöra sina skyldigheter för totalförsvaret.

På grund av ämnets komplexitet måste vidare följande avgränsningar göras.

Totalförsvaret består av en militär del och en civil del. Den militära delen leds av Försvarsmakten som ytterst ansvarar för att försvara Sverige mot väpnat angrepp och hävda Sveriges territoriella integritet.[1] Denna rapport behandlar inte den militära delen av totalförsvaret.

Den civila delen av totalförsvaret kan å sin sida sägas ha två huvudsakliga skyldigheter. Den ena är att under kriser och krig stödja försvarsmakten. Den andra skyldigheten är att värna civilbefolkningen mot verkningar av krigshandlingar och under kriser och i krig trygga en livsnödvändig försörjning.[2] Vi kommer i denna rapport i första hand att fokusera på det civila försvarets förmåga att upprätthålla grundläggande samhällsfunktioner för att värna civilbefolkningen och säkerställa en nödvändig försörjning i samhället. Det civila försvarets bidrag till det militära försvarets förmåga vid höjd beredskap är således inte denna rapports huvudsakliga fokus. Däremot hänvisar vi ofta till begreppet höjd beredskap som är ett samlingsbegrepp för när Sverige antingen är i krig, krigsfara eller om det råder utomordentliga förhållanden på grund av krig utanför Sverige eller av att Sverige varit i krig eller krigsfara.[3]

---

1 Målen för den militära delen av totalförsvaret fastställs i vid var tid gällande försvarsbeslut och har varierat över åren. Enligt nuvarande försvarsbeslut ska den militära delen av totalförsvaret förutom att försvara Sverige mot väpnat angrepp och hävda Sveriges territoriella integritet även värna suveräna rättigheter och nationella intressen i Sverige och utanför svenskt territorium i enlighet med internationell rätt, främja svensk säkerhet samt förebygga och hantera konflikter och krig genom att i fredstid genomföra operationer på svenskt territorium och i närområdet samt delta i internationella fredsfrämjande insatser, och skydda samhället och dess funktionalitet genom att med befintlig förmåga och resurser bistå övriga samhället såväl i fred som vid höjd beredskap. Se prop. 2020/21:30, s. 87-88.

2 Även målen för totalförsvarets civila del fastställs i vid var tid gällande försvarsbeslut. Den definition av det civila försvarets mål som vi använder här är tagen från 1992 års försvarsbeslut. Målsättningen i nu gällande mål för totalförsvarets civila del är mer omfattande men kan fortfarande sägas innehålla dessa två huvudsakliga mål.

3 Det är regeringen som beslutar om höjd beredskap enligt 3 § lagen (1992:1403) om totalförsvar och höjd beredskap.

En ytterligare avgränsning ligger i vem denna rapport vänder sig till. Ansvaret för det civila försvaret är, till skillnad från det militära försvaret, inte koncentrerat till någon eller några särskilda myndigheter, såsom Försvarsmakten. Istället består Sveriges civila försvar av all den civila verksamhet som myndigheter, kommuner och regioner samt enskilda, företag och det civila samhället m.fl. vidtar för att förbereda Sverige för krig.[4]

Denna rapport koncentrerar sig emellertid på myndigheters roll i det civila försvaret. Den skyldighet som åligger det privata näringslivet, frivilligorganisationer eller andra enskilda behandlas endast i den utsträckning detta har relevans för de offentliga myndigheternas skyldigheter inom ramen för det civila försvaret.

Inom ramen för det civila beredskapsarbetet brukar man även skilja mellan planering inför höjd beredskap och krig å ena sidan och beredskap inför fredstida kriser å den andra. De åtgärder som en myndighet vidtar för att öka sin grundläggande robusthet och sin förmåga att motstå fredstida kriser, såsom exempelvis naturkatastrofer eller pandemier, kan naturligtvis även bidra till att öka samhällets generella motståndskraft mot externa påtryckningar och därmed även bidra till att stärka det civila försvaret.[5]

Det motsatta är naturligtvis också sant i så måtto att de förberedelser en myndighet vidtar för att höja sin förmåga vid höjd beredskap eller krig många gånger även kommer att göra myndigheten bättre förberedd för allehanda fredstida kriser. Som vi kommer att se nedan finns det dock, trots dessa potentiella samordningsvinster, skäl att skilja en myndighets förmågehöjande arbete inför höjd beredskap och krig från myndighetens mer allmänna krisförberedande arbete.

Även denna rapport gör en sådan åtskillnad, genom att den endast behandlar myndigheters roll i det civila försvaret. Arbete och skyldigheter avseende fredstida kriser behandlas således inte.

En sista, men nog så viktig, avgränsning av denna rapports omfång är att den fokuserar på de särskilda problem och frågeställningar som en ökad digital transformation av den offentliga förvaltningen medför för myndigheters deltagande i det civila försvaret. Rapporten gör således inte några anspråk på att, ens på en mycket övergripande nivå, vara en fullständig redogörelse för myndigheters skyldigheter i beredskapshänseende inom ramen för det civila försvaret. Däremot berörs flera av dessa skyldigheter inom kontexten för en digital offentlig förvaltning.

4 Se prop. 2020/21:30, s. 89.

5 Se prop. 2014/15:109, s. 105.

Figur 1.1: Beskrivning av höjd beredskap inom ramen för totalförsvaret

1.3 Disposition

Syftet med denna rapport är att, i ljuset av det skärpta säkerhetsläget och uppbyggnaden av Sveriges civila försvar, redogöra för de risker som den digitala transformationen medfört och vad som kan göras för att minska dessa.

I avsnitt 2 beskriver vi därför hur den digitala transformationen av den svenska offentliga förvaltningen har gjort denna mindre robust och motståndskraftig inför höjd beredskap. Vi understryker också de huvudsakliga sårbarheter i beredskapshänseende som vi bedömer att den digitala transformationen fört med sig.

I avsnitt 3 beskriver vi avvecklingen och återuppbyggnaden av det svenska civila försvaret. Detta för att ge en bild av det säkerhetspolitiska läge vi befinner oss i och de ambitioner som riksdag och regering ställt upp för det civila försvaret.

I avsnitt 4 beskriver vi sedan fördelningen av ansvaret för Sveriges civila försvar med fokus på de skyldigheter som enligt lag åligger olika typer av upphandlande organisationer.

I avsnitt 5 föreslår vi, mot bakgrund av dessa skyldigheter och ett allmänt behov av en ökad robusthet i den digitala förvaltningen, ett antal åtgärder för att minska leverantörsberoenden vad avser samhällsviktig verksamhet.

Avslutningsvis redogör vi i avsnitt 6 för de många möjligheter och verktyg som upphandlingslagarna erbjuder upphandlande organisationer som önskar uppställa beredskapsvillkor på sina leverantörer.

AVSNITT 2 – ROBUSTHET I EN DIGITAL VÄRLD

Inledningsvis redogör vi för den digitala utvecklingen och hur denna har påverkat myndigheters robusthet

AVSNITT 3 – NYTT SÄKERHETSPOLITISKT LÄGE ÖKAR BEHOVET AV ROBUSTHET

Vidare beskriver vi hur det säkerhetspolitiska läget förändrats och på vilket sätt det påverkar behovet av robusthet

AVSNITT 4 – LAGSTIFTNING FÖR HANTERING AV HÖJD BEREDSKAP OCH ÖKADE KRAV PÅ ROBUSTHET

Därefter redogör vi för de krav som ställs på robusthet i gällande lagstiftning

AVSNITT 5 – ÅTGÄRDER FÖR ROBUST DIGITALISERING

I avsnittet redogör vi för de åtgärder som behöver vidtas för att öka robusthet

AVSNITT 5.4 – EN MODELL FÖR ATT MINSKA LEVERANTÖRSBEROENDE

Vidare presenterar vi en modell som kan användas oberoende av tjänst för att minska leverantörsberoenden

AVSNITT 6 – UPPHANDLAD BEREDSKAP

Avslutningsvis beskriver vi hur upphandlingsregelverket påverkar möjligheterna att vidta åtgärder för att öka robusthet

Figur 1.2: Rapportens disposition

2. Robusthet i en digital värld

2.1 Inledning

Vad som menas med att något är robust kan förklaras som dess förmåga att motstå störningar till följd av såväl inre som yttre påverkan.[6] Den påverkan som avses kan vara avsiktlig såväl som oavsiktlig och bestå av allt ifrån naturkatastrofer och fysiska angrepp till mindre incidenter och enskilda handhavandefel.[7]

Robusthet handlar med andra ord om att kunna fortsätta fungera och bedriva den aktuella verksamheten trots att något oförutsett händer. Inom ramen för myndigheters robusthet vid höjd beredskap kan detta beskrivas som att myndigheten har möjlighet att fortsätta bedriva sin verksamhet trots att en del eller delar av verksamheten utsatts för angrepp eller andra störningar till följd av krig.

Den teknologiska och digitala utvecklingen under de senaste 15–20 åren har förändrat samhället i grunden. Detta gäller inte minst offentliga myndigheter, vars uppdrag och samhällsfunktion numera i stor utsträckning bedrivs med ett stort antal egenutvecklade och införskaffade digitala verktyg, lösningar och tjänster.

En digitaliserad förvaltning är ofta en effektiv förvaltning. En grov uppskattning har exempelvis visat att det inom kommunal verksamhet bör kunna sparas cirka nio miljarder kronor per år bara i minskade lönekostnader för administratörer.[8] Vidare innebär en digitaliserad förvaltning ofta stora fördelar ur ett medborgarperspektiv såsom kortare handläggningstider, större möjligheter till insyn och tillgänglighet samt enklare administration.

Digital transformation kan ha både positiva och negativa effekter på en myndighets förmåga att motstå störningar. Digital transformation gör verksamheter mindre beroende av fysiska platser där arbetet kan bedrivas och tillgängligheten ökar när information och arbetsverktyg kan hanteras i flera olika redundanta miljöer. Automatisering kan i sin tur öka verksamhetens förmåga att hantera en anstormning av ärenden och förfrågningar i en krissituation.

De senaste årens utveckling av IT-branschen, och inte minst myndigheters roll som köpare på denna marknad, har dock blottlagt en rad negativa effekter vad avser myndigheters robusthet. I och med att myndigheter i allt större utsträckning gått över till att använda komplexa digitala

6 Se exempelvis prop. 2004/05:5, s. 210 och s. 216-219.

7 Post- och telestyrelsen, ”Goda råd till dig som jobbar med bredband på regional nivå – Robusthet”, s. 2.

8 DIGG, dnr: 2022–0466, ”Digitala Sverige 2021: En samlad analys av digitaliseringen i offentlig förvaltning och förslag på indikatorer för digitaliseringen i samhället”, s. 8-10. I denna rapport uppskattas även den ekonomiska potentialen i Sverige av automatisering och avancerad dataanalys samt teknik för uppkoppling, molntjänster och kommunikation till 850 – 1 400 miljarder kronor per år efter 2025.

tjänster har detta i stor utsträckning medfört att myndigheter, precis som alla andra IT-köpare, har ökat sitt beroende av privata mjukvaru- och tjänsteleverantörer. Detta beroende är i någon mån ofrånkomligt eftersom IT-system bygger på upphovs- och ensamrätt för den leverantör som utvecklat systemet (se vidare avsnitt 2.3 nedan).

Av olika skäl menar vi att beroendet, även med detta beaktat, har tilltagit under de senaste åren, inte minst genom ökad tjänstefiering och närmare leverantörssamarbeten (inklusive utkontraktering). Detta har skapat både ökad komplexitet och ett ständigt ökande behov av fler tjänster till myndigheten, i form av allt ifrån enklare konsulttjänster till verksamhetskritiska tjänster för IT-drift eller applikationsförvaltning.

Vi menar att myndigheters ökade beroende till mjukvaru- och tjänsteleverantörer måste beaktas även i frågor om robusthet och höjd beredskap.[9] I avsnittet nedan kommer vi kort att beskriva den digitala transformationens konsekvenser för myndigheters oberoende och robusthet.

2.2 Informationsteknikens olika lager

En verksamhet som använder informationsteknik är beroende av många olika *lager* av funktionalitet eller förmåga. Först och främst behövs en eller flera fysiska platser med tillgång till el, kyla/ventilation, nätverk och skalskydd. På dessa fysiska platser behöver datorer, nätverksutrustning och annan hårdvara driftsättas. Datorerna behöver i sin tur systemprogramvara som ska fungera och underhållas.

På denna grundläggande IT-infrastruktur kan sedan ytterligare lager av programvara, data och konfiguration läggas för att skapa funktionalitet i form av exempelvis slutanvändarprogramvara, utvecklingsplattformar/run-times/middleware, batchkörningar, automatisering och integration mellan andra system. För exempel på vad som kan ingå i sådana lager, se illustration i avsnitt 2.5.

I den bästa av världar är lager utbytbara, det vill säga en viss hårdvara är inte beroende av att ström eller nätverk kommer från någon viss leverantör. På motsvarande sätt kan en systemprogramvara köra på hårdvara från många olika tillverkare och en utvecklingsplattform köras ovanpå flera olika typer av systemprogramvara.

Ju mer utbytbara de olika lagren är desto robustare kan verksamheten göras i och med att tjänster eller komponenter, som av en eller annan anledning inte längre kan användas, lättare kan bytas ut.[10]

2.3 Leverantörsberoende

Under de tidiga faserna av myndigheternas digitala transformation, det vill säga den som skedde från 1970-talet och fram till en bit in på

9 Se även MSB, publ. MSB2179, ”När kriget kom nära – årsrapport it-incidentrapportering 2022”.

10 Se MSB, publ. MSB2179, ”När kriget kom nära – årsrapport it-incidentrapportering 2022”, s. 46 f.

2000-talet, var det helt nödvändigt för myndigheten att i förhållandevis stor utsträckning driva och kontrollera sin egen IT-förmåga.

Genom bland annat egen IT-organisation, lokalt installerad mjukvara (numera kallad ”on-prem”), egenutvecklade och skräddarsydda IT-system och egna data- eller serverhallar hade många myndigheter en hög grad av kontroll över samtliga eller de flesta lager i sin IT. Det fanns därmed en jämförelsevis stor möjlighet för myndigheten att själv förebygga störningar och yttre påverkan. Därmed fanns det även en större grad av digital robusthet, än vad som är fallet idag.

För många svenska myndigheter ser dock verkligheten väsentligt annorlunda ut nu jämfört med för bara 10–15 år sedan. En stor andel av de svenska myndigheterna har under denna period effektiviserat, avvecklat och utkontrakterat sin kompetens, förmåga och infrastruktur till privata leverantörer som därmed fått ta ansvar för allt fler lager i myndighetens IT-miljö.

Det som generellt kännetecknar leverantörsberoende gentemot just IT-leverantörer är följande:

- Leverantören har en ensamrätt (exempelvis patent eller upphovsrätt) till ett bakomliggande system eller teknologi såsom ett visst datorprogram.
- På grundval av detta datorprogram erbjuder leverantören en eller flera digitala tjänster som myndighetens verksamhet är beroende av.
- Därutöver har leverantören ofta ett kunskapsövertag gentemot myndigheten, exempelvis avseende systemfunktionalitet, säkerhetslösningar, teknikutveckling och i vissa fall även hur marknaden ser ut.

När det gäller ensamrätter i samband med IT-system och digitala tjänster är det främst upphovsrätt till ”datorprogram” som aktualiseras. Begreppet ”datorprogram” är definierat i URL och utgör en särskild typ av upphovsrättsligt verk.

Ett datorprogram består av programkod tillsammans med förberedande designmaterial, men omfattar inte bakomliggande idéer, logik eller algoritmer.[11] Programkod delas ofta in i oläsbar objektkod och läsbar källkod.

Den som utvecklat ett datorprogram för kommersiella ändamål tillhandahåller och upplåter typiskt sett licens endast till datorprogrammets objektkod, medan källkoden hålls inom en betydligt snävare krets av särskilda utvecklare och programmerare hos licensgivaren av datorprogrammet.

Tillgång till källkoden är helt nödvändigt för att effektivt kunna förvalta och förbättra datorprogrammet.[12] Detta innebär att datorprogram som

11 Se 1 kap 1 § URL samt direktiv 2009/24/EG av den 23 april 2009 om rättsligt skydd för datorprogram.

12 Det är teoretiskt möjligt, och i vissa fall en tvingande rättighet enligt 26 § h URL, för den som innehar objektkod att från objektkod återskapa (dekompilera) den läsbara källkoden. I regel är dock sådant förfarande otillåtet enligt licensgivarens licensvillkor, när förfarandet om det inte omfattas av tvingande lagregler. Dekompilering som åtgärd för mera robust digitalisering är därmed sällan effektivt.

utvecklats i kommersiella syften per definition medför ett särskilt starkt beroende till den aktör som licensierar, utvecklar och förvaltar datorprogrammet.

För att en myndighet själv och oberoende från leverantören (licensgivaren) ska kunna förvalta ett datorprogram krävs åtminstone:

1) Tillgång till källkod och källkodsdokumentation.

2) Djup och uppdaterad kompetens om datorprogrammets funktion, uppbyggnad och struktur.

3) Egna resurser med kompetens att förstå programmet och som löpande kan arbeta med systemet.

Det ska nämnas att det för en myndighet ofta är svårt att i praktiken skapa ett effektivt oberoende i relation till kommersiella mjukvaruleverantörer. Även om en myndighet vidtar det första steget ovan, det vill säga säkerställer tillgång till källkod i samband med en upphandling, är det svårt att skapa tillräcklig egen kompetens för att kunna förvalta mjukvaran oberoende av leverantören.

Ett bättre alternativ kan därför vara att i samband med upphandling och systemval försöka identifiera system och digitala tjänster som är byggda med så kallad ”öppen mjukvara”,[13] eftersom sådana system och tjänster skapar avsevärt bättre möjligheter för myndigheter att förvalta systemet självständigt. Normalt är källkoden för öppen mjukvara allmänt tillgänglig för att alla vidareutvecklingar och förbättringar som görs (oavsett vem som utför dem) ska komma hela användarkretsen tillgodo. Användning av öppen mjukvara kan därför gynna en robust digital transformation för myndigheter.

Ytterligare ett skäl till att myndigheter kan ha ett stort leverantörsberoende till sina IT-leverantörer är att myndigheter ofta har ingått oförmånliga avtalsvillkor eller köpt digitala tjänster på ett sätt som begränsar myndighetens möjligheter att agera effektivt och självständigt gentemot leverantören. Risken för detta är särskilt stor för IT-funktionalitet som helt eller till övergripande del erbjuds som tjänst snarare än i form av licensierad och installerad programvara i kundens IT-miljö.

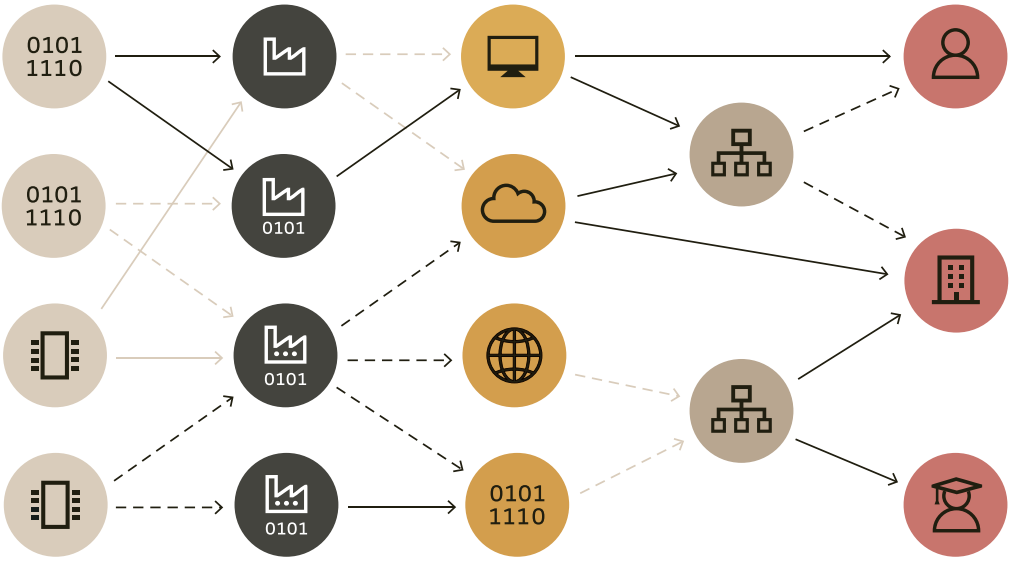
Myndigheter måste på olika sätt försöka minska detta leverantörsberoende. Detta gäller särskilt om den aktuella leverantören tillhandahåller tjänster eller teknologi som krävs för att myndigheten ska kunna upprätthålla sin mest grundläggande verksamhet och utföra sitt uppdrag även i händelse i av krig eller höjd beredskap.

13 För mera information om öppen mjukvara hänvisas till Open Source Initiative, en ideell stiftelse vars syfte är att förespråka öppen källkod. Se https://opensource.org.

2.4 De utökade digitala leveranskedjorna

Dagens IT-infrastruktur är ofta en del av en digital leveranskedja, där olika funktioner för tjänstens användning finns hos olika, separata leverantörer. Detta skapar i sin tur beroenden i flera led.

Förhållandet kan synliggöras enligt nedan[14]:



Figur 2.1: Den digitala leveranskedjan

Effekten av att en del av kedjan slås ut är oftast allvarligast då den tjänst som myndigheten får tillgång till utgör ett så kallat monoberoende.[15] En organisation har ett monoberoende av (exempelvis) en tjänst när den är beroende av tjänsten och det inte finns några alternativ att använda ifall den tjänst man redan använder upphör.[16]

2.5 Utkontraktering och tjänstefiering

Utkontraktering eller *outsourcing* innebär att ett företag eller en myndighet anlitar en extern part för att utföra en process eller en serie processer som företaget eller myndigheten tidigare har utfört eller skulle kunna utföra i egen regi.[17] Särskilt de lägre lagren i en organisations IT-drift

14 Bilden är hämtad ur MSB, Publ. MSB1855, ”Hoten mot de digitala leveranskedjorna – 50 rekommendationer för att stärka samhällssäkerheten”, s. 23.

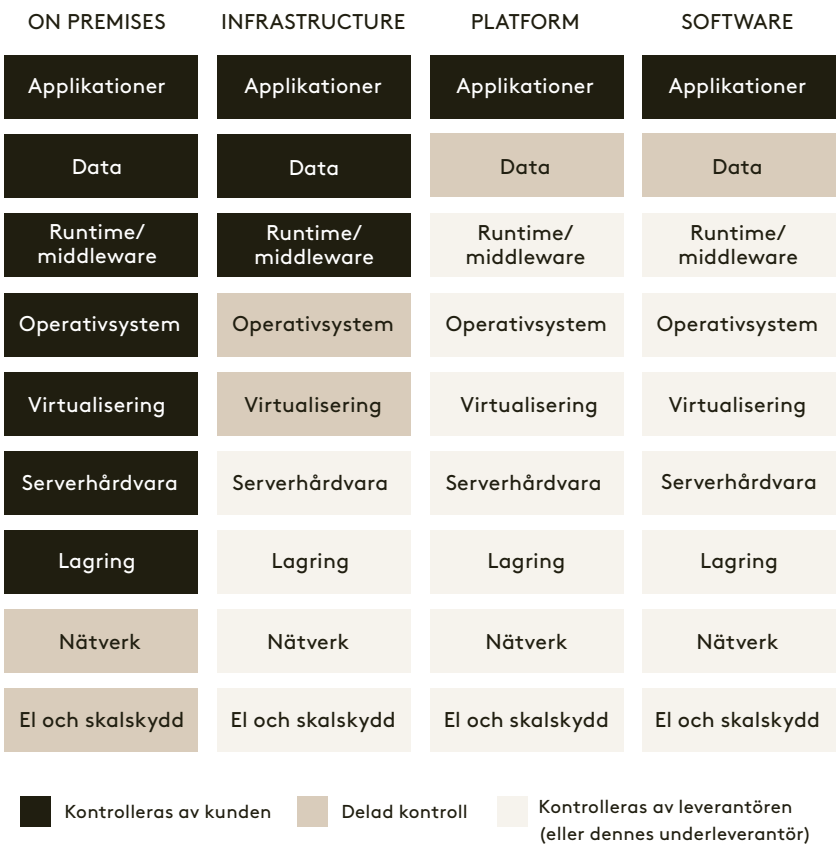
15 Se MSB, publ. MSB2179, ”När kriget kom nära – årsrapport it-incidentrapportering 2022”, s. 23, 51 och 55.

16 Se MSB, publ. MSB2179, ”När kriget kom nära – årsrapport it-incidentrapportering 2022”, s. 5.

17 Lindberg, A., Kahn, J. & Krouthén, B., ”IT-avtal – särskilt om outsourcing”, 1:a uppl. (2009), s. 15.

kan lämpa sig för outsourcing. Den mest grundläggande typen av sådana tjänster är datorhallstjänster där leverantören ansvarar för skalskydd, el, nätverk och i viss utsträckning grundläggande hårdvara, men där köparen av tjänsten i övrigt har full exklusiv kontroll över sin databehandling.

Högre upp i lagren har sedan etablerats olika leveransmodeller som kan sägas inkludera viss utkontraktering. Infrastructure as a Service (IaaS) innebär att de mest grundläggande datorresurserna i form av lagrings-, beräknings- och kommunikationskapacitet tillhandahålls som tjänst. Platform as a Service (PaaS) används för applikationsutveckling eller -drift ovanpå en standardiserad och underhållen mjukvaruplattform och Software as a Service (SaaS) för färdiga applikationer avsedda för slutanvändare.[18] Fördelningen av kontroll i de olika leveransmodellerna kan illustreras enligt nedan:[19]



Figur 2.2: Vem som i olika molntyper ansvarar för de olika lagren i den stack som behövs för att kunna leverera IT-tjänster

18 SOU 2021:1, s. 43.

19 Se vidare Publika molntjänster i näringslivet, Kahn Pedersens skriftserie 2020:3, s. 22.

Som beskrivs nedan har det blivit allt vanligare att myndigheter utkontrakterar sin IT-drift, antingen i form av renodlade och traditionella serverdrift- eller infrastrukturtjänster eller i form av molntjänster av IaaS, PaaS eller SaaS-karaktär.[20]

Det finns flera effektivitetsvinster med att utkontraktera en del av sin IT-verksamhet, till exempel i form av ökad skalbarhet och mer robusta mekanismer för katastrofberedskap. Det är sällan ekonomiskt försvarbart för en myndighet att investera i den teknik, de lokaler och personal som krävs för att sköta driften av ett stort IT-system i helt egen regi. Det finns inte heller en omedelbar nytta i att ta ansvar och kostnader för de nedre lagren om det är funktionaliteten i de övre lagren, exempelvis den funktionalitet som en viss SaaS-tjänst erbjuder, som man vill åt.

Även i de fall där myndigheten byggt upp en förmåga till grundläggande IT-drift med exempelvis egna datacenter så är det inte alltid lämpligt eller ens möjligt att tillgodose framväxande it-behov med drift helt i egen regi. En orsak är att mjukvaran i IT-lösningar i allt större utsträckning inte erbjuds licensierad för installation i egenkontrollerad IT-miljö, utan endast finns tillgänglig som molntjänst. Det tydligaste exemplet för myndigheter är kanske samarbets- och videokonferenssystemet Microsoft Teams som till skillnad från sina föregångare (exempelvis Sharepoint eller Skype for Business) endast levereras som tjänst. Även när den aktuella mjukvaran kan licensieras för lokal installation är det allt mer ovanligt att det går att köpa en evig licens för denna. Istället används prenumerationsupplägg där rätten att använda programvaran är knuten till en pågående prenumeration som kan komma att avslutas av leverantören.

Sammantaget har framförallt de övre lagren i den typiska IT-miljön tjänstefierats, det vill säga den funktionalitet som tillhandahålls erbjuds i första hand som en pågående tjänst snarare än genom ett engångsköp. Detta skapar ett ihållande leverantörsberoende.

Fördelarna med att inte behöva ansvara för lagren under den funktionalitet som eftersträvas behöver vägas mot det beroendeförhållande som en utkontraktering ger upphov till. En god beredskap förutsätter att myndigheten även vid höjd beredskap kan säkerställa kontinuerlig tillgång till den utkontrakterade processen. Den utkontrakterade verksamheten ska kunna gå att ”hämta hem” på ett snabbt och funktionellt sätt. En utkontraktering innebär alltid att myndigheten, i någon utsträckning, avsäger sig den direkta kontrollen över säkerhet och robusthet och istället blir hänvisad till att ställa relevanta krav inom ramen för en beställarroll.

2.6 De digitala systemens inneboende komplexitet

En faktor som påverkar möjligheten att skapa en digital robusthet är de digitala systemens komplexitet. Denna komplexitet leder i sin tur till flera utmaningar.

20 SOU 2021:1, s. 86. Enligt en enkät som IT-driftsutredningen gjorde under 2020 så använder 35% respektive 31% av de tillfrågade myndigheterna molntjänster av IaaS- eller PaaS-karaktär. För SaaS-tjänster var siffran istället 89%.

En av dessa är att det skapas ett systemberoende. En myndighet som köper in ett IT-system kan sällan använda en standardiserad lösning utan behöver ofta anpassa systemet efter den egna verksamhetens behov.

Att myndigheten gör anpassningar är inte ett problem i sig, men många gånger blir det inköpta IT-systemet en grund för flera andra viktiga funktioner och lösningar. Det skapar en inlåsningseffekt som gör det svårt för myndigheter att efter en tid byta ut det ursprungliga IT-systemet. Detta blir särskilt tydligt med föråldrade IT-system.

Riksrevisionen publicerade 2019 en rapport om utmaningarna med föråldrade IT-system. Där beskrivs att alla myndigheter som inte är nyetablerade sannolikt har en IT-miljö som utvecklats över tid och är byggda på ärvda system, det vill säga sådana som anskaffats för olika syften och under olika epoker.[21]

Problematiken med föråldrade IT-system beskrivs enligt följande:

> *Många äldre it-system är byggda utifrån tanken att systemet ska hantera alla steg i en process, exempelvis handläggning och utbetalning av en förmån. Det innebär att systemet utformas utifrån hur processen såg ut när systemet skapades. Under åren kanske processerna förändras och därmed görs även förändringar i själva systemet. Detta skapar på sikt ett mycket komplext system. Äldre system saknar även många gånger tillräcklig dokumentation för att kunna förstå hur systemet är uppbyggt. Många system är baserade på gammalt programspråk och bygger ofta på att man måste göra batchkörningar för att uppdatera de underliggande databaserna, vilket innebär att systemet inte är tillgängligt under den tiden körningen görs. Att systemen är byggda med gammalt programspråk innebär även att det är svårt att få tag på medarbetare som har tillräcklig kompetens, och kostnaderna blir höga. Hög komplexitet och bristfällig dokumentation innebär i sin tur att förändringar i systemet kräver en ökad mängd tester som i sin tur leder till högre kostnader. Sammantaget innebär dessa faktorer att kostnaderna för att förvalta föråldrade system ökar med tiden. Komplexiteten innebär även att det blir svårare och svårare att göra förändringar i systemet, vilket i sin tur innebär att det blir svårt att tillgodose förändrade behov i kärnverksamheten.*[22]

Sammanfattningsvis innebär ett föråldrat och över tid vidareutvecklat IT-system att myndigheten ofta behöver förlita sig på en och samma externa leverantör, vilket minskar den egna robustheten.[23]

Problemet med systemberoende kan förvärras när olika system ska samverka genom att utbyta data. Detta kräver att systemen integreras, det vill säga konfigureras för att kunna kommunicera med varandra och utbyta data i de olika processer som IT-verksamheten i sin helhet ska stödja.

---

21 Riksrevisionen, rir 2019:28, ”Föråldrade it-system – hinder för en effektiv digitalisering”, s. 10.

22 Riksrevisionen, rir 2019:28, ”Föråldrade it-system – hinder för en effektiv digitalisering”, s. 22.

23 MSB, publ. MSB2179, ”När kriget kom nära – årsrapport it-incidentrapportering 2022”, s. 47 f.

Komplexiteten i integrationen beror bland annat på hur anpassningsbara de enskilda systemen är och om organisationen har en mogen IT-arkitektur för system-till-systemkommunikation.

I värsta fall har olika IT-konsultföretag skapat ett stort antal integrationer mellan system som kommunicerar punkt-till-punkt och som utgår från den eller de datamodeller som de ingående systemen använder sig av.

Detta leder till en situation där det är svårt att byta ut ett enskilt system eftersom många andra system i verksamheten har integrerats på ett direkt sätt mot just det systemet, dess kommunikationsprotokoll och datamodeller. Kunskapen om hur själva integrationen har gjorts kanske inte heller finns bevarad i myndigheten utan endast hos den IT-konsult som gjort integrationen.[24]

2.7 Otillräcklig digital suveränitet

Med digital suveränitet avses förmågan att ha exklusiv kontroll över data, inklusive att kunna besluta vem som får tillgång till denna, samt att självständigt utveckla, förändra, kontrollera och komplettera informationstekniska system.[25] Har man digital suveränitet har man också goda förutsättningar för en robust digital transformation.[26]

På unionsnivå, och i ännu större utsträckning nationell nivå, saknas tillräcklig digital suveränitet vad gäller både hårdvara, mjukvara och molntjänster. Det är i hög grad utomeuropeiska bolag som bygger både IT-infrastruktur och digitala tjänster och som därmed bestämmer över stora delar av de grundläggande säkerhetsfrågorna avseende IT. Såväl EU som Sverige kan sägas ha relativt låg digital suveränitet och är beroende av andra staters beslut och lagstiftning.[27] Det innebär att en svensk myndighet ofta har begränsade möjligheter att kontrollera eller påverka hur ett IT-system hanterar och skyddar myndighetens information, särskilt när det gäller säkerhet i de lägre lagren av myndighetens IT-miljö.

Ett exempel på när detta påverkar svenska aktörers förmåga var under den så kallade halvledarkrisen under 2021 och 2022 då framförallt fordonsindustrin drabbades av brist på hårdvarukomponenter.[28] Ett annat är svenska myndigheters beroende av Microsoft Teams som digital samarbetsplattform, vars betydelse för robusthet har adresserats i samverkansarbetet Digital samarbetsplattform för offentlig sektor.[29]

---

24 MSB, publ. MSB2179, ”När kriget kom nära – årsrapport it-incidentrapportering 2022”, s. 55.

25 Jfr Försäkringskassan, dnr. 013428-2019, ”Vitbok – Molntjänster i samhällsbärande verksamhet”.

26 MSB, publ. MSB2179, ”När kriget kom nära – årsrapport it-incidentrapportering 2022”, s. 57.

27 Jfr MSB, publ. MSB2179, ”När kriget kom nära – årsrapport it-incidentrapportering 2022”, s. 57.

28 Se exv. Dagens Industri, 19 april 2021: ”Scaniatoppen spår fortsatt halvledarbrist hela 2022: ”Förödande”.

29 Se https://www.esamverka.se/vad-vi-gor/utvecklingsarbetet-inom-esam/digital-samarbetsplattform.html. Läst den 2023-03-22.

2.8 Bristande IT-kompetens

Många myndigheter har alltså varit tvungna att använda sig av digitala lösningar och tjänster som de inte själva förmått utveckla. Myndigheterna har därför behövt lägga ut delar av sin verksamhet på externa leverantörer, exempelvis i form av drift och underhåll av IT-system. Detta har i sin tur skapat ett beroende av externa leverantörer som inte funnits på samma sätt före den digitala utvecklingen. Det har också utarmat myndighetens egen IT-kompetens ytterligare i och med att man gått från att vara utvecklare till beställare.

IT-systemens komplexitet gör det även svårt för enskilda specialister på den kommersiella marknaden att ha tillräcklig kunskap om systemen i sin helhet. Istället har kunskapen fragmenterats och spridits ut på flera olika kompetenser, där var och en är nödvändig för att säkerställa systemens drift och eventuella vidareutveckling. För att uppnå tillräcklig kompetens för IT-systemen i sin helhet krävs därför flera olika resurser.[30]

Detta resursbehov hos både offentlig och privat sektor har hittills som regel inte kunnat mötas av marknaden och det finns idag en stor kompetensbrist.[31] I de fall resurser finns tillgängliga finns de ofta hos en centraliserad enhet hos respektive leverantör och inte sällan utanför Sveriges gränser. Den digitala transformationen av offentlig förvaltning har med andra ord gjort myndigheter både leverantörs- och handelsberoende.[32]

2.9 Växande datamängder

En följd av digital transformation är att den kräver och skapar stora mängder data. Denna data kan sedan struktureras upp och användas för en mängd olika ändamål, exempelvis för att vidareutveckla tjänster eller för att ta fram information och underlag.

Inom offentlig förvaltning har det över tid byggts upp omfattande register kring allt från patientdata, fastighetsdata, deklarationer och trafikflöden. Uppkopplade maskiner kommunicerar och levererar data till olika system. Data utvecklas på detta sätt till en slags infrastruktur, som binder samman sektorer och som är nödvändig för att leverera olika tjänster i det moderna samhället.[33]

Insamling och strukturering av data är en förutsättning för den digitala utvecklingen, men innebär även vissa samhällsrisker ur ett beredskapshänseende. Riskerna rör såväl uppgifternas konfidentialitet som tillgänglighet och riktighet. För att öka kontrollen över den egna verksamheten är det nödvändigt att säkra kritisk information. Det innebär att myndigheter måste säkerställa att information som är nödvändig för upprätthållande av det civila försvaret finns tillgänglig, är korrekt och

30 Se MSB, publ. MSB1855, ”Hoten mot de digitala leveranskedjorna – 50 rekommendationer för att stärka samhällssäkerheten”, s. 27.

31 Riksrevisionen, rir 2019:28, ”Föråldrade it-system – hinder för en effektiv digitalisering”, s. 22.

32 SOU 2021:1, avsnitt 4.3.

33 Digitaliseringsrådet, dnr. 19-3731, ”Data som strategisk resurs”, s. 8.

skyddad från obehöriga även under höjd beredskap. För att kunna säkerställa detta krävs hög informationssäkerhet inom myndigheten.

Om data inte hålls konfidentiell kan den komma att utnyttjas av en antagonistisk makt i en krigssituation. Det är inte nödvändigtvis så att sådana data enskilt är känsliga för Sveriges säkerhet, utan det är när de sammanställs som det kan vara möjligt att utvinna känslig information.

Denna problematik diskuteras i SOU 2021:1 i förhållande till säkerhetskänslig verksamhet:

> *En särskild fråga är hur man bör hantera den situationen att en utkontraktering av viss it-drift involverar en stor mängd uppgifter som sedda var för sig är klassificerade som begränsat hemliga, eller som inte är säkerhetsskyddsklassificerade alls, men som sammantagna kan vara betydligt känsligare i förhållande till Sveriges säkerhet. Det kan t.ex. handla om situationer där uppgifter som sammanställts har bearbetats eller kan bearbetas så att man av sammanställningen kan utvinna en annan och mer känslig information än av uppgifterna var för sig. En annan situation kan vara att den sammanställda informationen visar på exempelvis beroenden mellan olika verksamheter, förmåga, sårbarheter eller andra förhållanden som kan leda till en inte obetydlig skada för Sveriges säkerhet om den röjs.*[34]

I SOU 2021:25 framhålls vidare att grunddata, det vill säga grundläggande information om personer, företag, fastigheter och geografi, behöver kunna göras tillgänglig för olika aktörer som bedriver samhällsviktig verksamhet även i händelse av fredstida kriser eller vid krigsfara och ytterst krig. Den digitala suveräniteten för grunddata är också en förutsättning för att kunna återuppbygga ett samhälle efter en väpnad konflikt.[35]

2.10 Automatisering

Slutligen har den digitala transformationen även inneburit en ökad automatisering, vilken i sig medför vissa sårbarhetsproblem.

Ett exempel är den IT-attack som drabbade Kalix kommun i december 2021. Attacken påverkade samtliga IT-system, vilka låg nere i tre veckors tid. IT-attacken innebar bland annat att de schemaläggningsverktyg och övriga verktyg som hemtjänsten använde sig av för sina planerade insatser och besök inte var tillgängliga.[36]

Verksamheten fick därför snabbt övergå till att använda papper och penna för sin arbetsplanering. I detta fall var kommunens räddning att medarbetarna hade god kontinuitet och kunskap om de brukare som

34 SOU 2021:1, s. 177.

35 SOU 2021:25, s. 234.

36 Kalix kommun, ”Rapport IT-attacken socialförvaltningen Kalix kommun. En summering av arbetet före, under och efter it attacken som drabbade kommunen den 16 december 2021”, s. 6 f.

var i behov av hemtjänst och snabbt kunde sammanställa nödvändig information för att säkerställa arbetets fortsättning.[37] Kontinuitet och god kunskap hos medarbetarna var en förutsättning för att i kris kunna övergå till ett analogt och manuellt arbetssätt.

2.11 Sammanfattning

Sammanfattningsvis skapar den tekniska utvecklingen, utbredningen av digitala lösningar och ökade datavolymer inte bara stora möjligheter utan även risker och sårbarheter för myndigheter och för samhället i stort. Även den data som genereras medför i sig såväl sårbarheter som möjligheter.[38]

Det finns flera utmaningar med digital transformation och många av de system som är kritiska för att upprätthålla samhällets funktionalitet är redan i fredstid sårbara för störningar. Dessa sårbarheter blir naturligtvis ännu större vid höjd beredskap.

En myndighet som är beroende av resurser i andra länder kan inte räkna med att få tillgång till dessa resurser vid höjd beredskap, kriser eller krig. Detta gäller särskilt om resurserna är belägna hos en antagonistisk makt, men så kan även vara fallet när det land där resurserna befinner sig av annat skäl måste prioritera sin egen försörjning.[39]

Som kommer att beskrivas i nästa avsnitt finns det på grund av det förändrade säkerhetspolitiska läget och inriktningen på det civila försvaret särskild anledning för myndigheter att kartlägga och försöka begränsa sitt beroende till privata tjänsteleverantörer.[40]

37 Kalix kommun, ”Rapport IT-attacken socialförvaltningen Kalix kommun. En summering av arbetet före, under och efter it attacken som drabbade kommunen den 16 december 2021”, s. 8.

38 SOU 2020/21:30, s. 63.

39 Se MSB, publ. MSB2179, ”När kriget kom nära – årsrapport it-incidentrapportering 2022”, s. 43 och 51.

40 Se MSB, publ. MSB2179, ”När kriget kom nära – årsrapport it-incidentrapportering 2022”, s. 48.

3. Nytt säkerhetspolitiskt läge ökar behovet av robusthet

3.1 Inledning

Vi har ovan beskrivit hur den digitala transformationen av offentlig förvaltning har gjort denna mindre robust. Dessutom befinner sig Sverige i en mycket ansträngd säkerhetspolitisk situation och det finns ett behov av att snabbt öka motståndskraften i alla delar av det civila försvaret, inte minst på det digitala området.

I avsnitt 4 nedan kommer vi att beskriva de lagkrav som gäller för myndigheter inom totalförsvaret och vilka skyldigheter dessa innebär i beredskapshänseende.

För att bättre förstå de utmaningar som det civila försvaret står inför och de överväganden som ligger till grund för de lagkrav vi redogör för i avsnitt 4 kan det underlätta att först kort beskriva inriktningen i svensk försvarspolitik så som denna har kommit att utvecklas sedan det kalla krigets slut.

Inriktningen för den svenska försvarspolitiken har allt sedan 1900-talets början beslutats av riksdagen i särskilda försvarsbeslut. För att illustrera utvecklingen i svensk försvarspolitik kommer vi nedan att kort redogöra för innehållet i de sju senaste försvarsbesluten, vilka omfattar en försvarsbeslutsperiod om 33 år.[41] Vi delar upp dessa i två tidsepoker, ”den eviga fredens tid” och ”nutid”.

3.2 Den eviga fredens tid

I försvarssammanhang kallas ibland tiden mellan det kalla krigets slut och Rysslands annektering av Krim år 2014 för den eviga fredens tid. 1992 års försvarsbeslut markerar början på denna period. I och med Berlinmurens fall 1989 och Sovjetunionens upplösning 1991 ansågs hotet om ett storskaligt krig mellan öst och väst i Europa ha upphört. Samtidigt förde Sovjetunionens upplösning med sig ett mycket osäkert säkerhetspolitiskt läge vars konsekvenser både på lång och kort sikt var svåra att överblicka. Under den eviga fredens inledande år var regeringen mycket medveten om de försvarspolitiska risker som den nya världsordningen förde med sig.

Följande beskrivning ur förarbetena till 1992 års försvarsbeslut fångar det osäkra politiska läge som rådde i kalla krigets efterdyningar men som också kommit att prägla det säkerhetspolitiska klimatet fram till idag:[42]

41 1992 års försvarsbeslut (prop. 1991/92:102), 1996 års försvarsbeslut (prop. 1995/96:12, 1996/97:4, 1997/98:1D6), 2000 års försvarsbeslut (prop. 1999/2000:30), 2004 års försvarsbeslut (proposition 2004/05:5 och 2004/05:43), 2009 års förvarsbeslut (prop. 2008/09:140), 2015 års försvarsbeslut (prop. 2014/15:109) och försvarsbeslutet 2020 (prop. 2020/21:30).

42 Försvarsbeslut 1992, prop. 1991/92:102, s .19.

Sovjetunionens upplösning är en händelse av historiska dimensioner. När den gamla unionen i december 1991 formellt avskaffades, innebar detta inte blott slutet för den kommunistiska, hårt centralstyrda stat som skapades efter revolutionen 1917. Efter nästan 400 år av expansion har den ryska huvudmaktens område i Europa med ens reducerats till att i sina huvuddrag motsvara utsträckningen vid slutet av 1500-talet. I den forna supermaktens ställe har femton nya stater uppstått, med djupa inre problem, svaga eller outvecklade demokratiska strukturer och en betydande konfliktpotential sinsemellan. Vid sidan av den ojämförligt största nya staten, Ryssland, framträder Ukraina som en helt ny europeisk stat med ungefär samma yta och folkmängd som Frankrike. Vilka säkerhetspolitiska följder denna utveckling kan komma att få är det ännu inte möjligt att överblicka. Klart står emellertid att de måste bli vittgående, såväl ur ett europeiskt som ett globalt perspektiv.

Mot bakgrund av detta säkerhetspolitiska läge, och den ekonomiska situation som Sverige befann sig i under den så kallade 90-talskrisen, beslutades att försvar mot ett angreppskrig mot svenskt territorium inte längre skulle vara den främsta grunden för hur det svenska totalförsvaret dimensionerades.[43]

Sverige påbörjade därmed vad som skulle bli en drygt 20 år lång omställningsperiod från ett invasionsförsvar till ett insatsförsvar. Under de kommande fyra försvarsbesluten, 1996, 2000, 2004 och 2009 neddimensionerades försvaret betydligt och det värnpliktsystem som tidigare varit den huvudsakliga källan för försvarets personalförsörjning ersattes med en väsentligen mindre personalstyrka som var anställd eller kontraktsanställd.

Vad avser det civila försvaret anmärks redan i 1992 års försvarsbeslut att samhällets ökande komplexitet medför att försvarsmakten blir allt mer beroende av att den infrastruktur och materialförsörjning som det civila samhället tillhandahåller har en sådan robusthet och flexibilitet att den trots störningar kan möjliggöra en mobilisering av försvarsmakten. I flera försvarsbeslut under den eviga fredens tid, i vart fall inledningsvis, varnade regeringen för att en ökande komplexitet, privatisering och globalisering innebar risker i robusthetshänseende.[44]

Inte minst på området för den offentliga digitala transformationen varnades det redan i tidiga regeringsbeslut för att en ordentlig risk- och sårbarhetsanalys i princip saknades för det civila försvaret. I 1996 års försvarsbeslut angav regeringen:

43 Prop. 1991/92:102, s. 10.

44 Se exempelvis Försvarsbeslut 1996, prop. 1995/96:12, s. 90 där regeringen dels varnar för att den pågående privatisering och bolagisering minskar möjligheterna till en god beredskap.

> *Det svenska samhället är utomordentligt beroende av väl fungerande IT- system. Den svenska IT-strukturen utmärks av att den ofta är avreglerad och i vissa avseenden decentraliserad. Det finns mot denna bakgrund starka skäl att analysera sårbarheter över ett hotspektrum som täcker området från enskilda aktörers dataintrång till organiserade storskaliga angrepp samt söka säkerställa nödvändigt skydd.*[45]

Dessa varningar till trots kan konstateras att mycket lite gjordes för att öka myndigheters, näringslivets och frivilligsamhällets möjligheter att verka för ett mer robust civilt försvar. Tvärtom ledde den eviga fredens tid till en etappvis nedmontering av den centrala planeringen av det civila försvaret. I och med 2004 års försvarsbeslut avvecklades i praktiken det civila försvaret i sin helhet.

Den eviga fredens tid medförde ett nytt fokus för den civila beredskapen, från ett civilt försvar till en beredskap inför fredstida kriser. Tanken var att en ökad robusthet inför fredstida kriser också skulle ge ett mer motståndskraftigt samhälle vid höjd beredskap. I realiteten ledde dock denna nya orientering till att planeringen av det civila försvaret prioriterades bort.

Ansvarsprincipen är en central princip för organiseringen av det civila försvaret och innebär att den som har ett bestämt verksamhetsansvar i fredstid också ska ha det under höjd beredskap och krig, förutsatt att verksamheten ska bedrivas under sådana förhållanden.[46] Ansvarsprincipen ska i grunden vara styrande för planeringen inom det civila försvaret och den kräver att de berörda aktörerna under fredstid vidtar de åtgärder som är nödvändiga för att kunna bedriva verksamheten under höjd beredskap.[47]

Under den eviga fredens tid användes dock denna princip ofta som ett skäl för minskad central styrning och finansiering av det civila försvaret. I ett allt mer komplext samhälle gjorde regering och riksdag det övriga civilsamhället successivt allt mer ansvarigt för det civila försvarets upprätthållande och planering. Vidare gavs civilsamhället det huvudsakliga ansvaret för att finansiera detta arbete inom ramen för sin ordinarie verksamhet.

Den eviga fredens tid präglades således av en nedrustning och en avveckling av det civila försvaret. Det skulle dröja fram till 2015 års försvarsbeslut innan planeringen av det civila försvaret återupptogs.

---

45 Prop. 1996/97:4, s. 174.

46 Se t.ex. prop. 2014/15:109, Försvarspolitisk inriktning, Sveriges försvar 2016-2020, s. 62 och 104.

47 SOU 2022:57, s. 79.

3.3 Nutid

Så här sammanfattar 2020 års försvarsbeslut det nu rådande säkerhetspolitiska läget:

> *Det säkerhetspolitiska läget i Sveriges närområde och i Europa har över tid försämrats. Ett väpnat angrepp mot Sverige kan inte uteslutas. Det kan inte heller uteslutas att militära maktmedel eller hot om sådana kan komma att användas mot Sverige. Sverige blir oundvikligen påverkat om en säkerhetspolitisk kris eller väpnad konflikt uppstår i Sveriges närområde. Totalförsvarets förmåga behöver därför fortsätta stärkas.*[48]

Det vi här väljer att kalla nutid är tiden från 2015 års försvarsbeslut och framåt. Rysslands annektering av Krim blev ett abrupt uppvaknande för svensk försvarspolitik och markerade slutet på den eviga fredens tid.

Planeringen av det civila försvaret återupptogs i och med 2015 års försvarsbeslut och även 2020 års försvarsbeslut innehåller tydliga och omfattande satsningar på det civila försvaret. Det insatsförsvar som under den eviga fredens tid har varit helt dominerande för den försvarspolitiska inriktningen ska ställas om till ett försvar som tydligare inriktas mot den nationella försvarsdimensionen.

Inte minst Rysslands invasion av Ukraina har visat betydelsen av en robust civil infrastruktur som är motståndskraftig även vid en längre ihållande invasion av svenskt territorium.

Som bland annat framgår av 2020 års försvarsbeslut ska det civila försvaret prioriteras och Sveriges förmåga att hantera höjd beredskap och ytterst krig stärkas på bred front. Det gäller inte minst de viktigaste samhällsfunktionerna såsom ordning och säkerhet, skydd av civilbefolkning, hälso- och sjukvård, livsmedel och dricksvatten, finansiell beredskap, transporter, energiförsörjning samt elektroniska kommunikationer och post.[49] Även investeringar för att stärka arbetet med säkerhetsskydd och cybersäkerhet ingår i satsningen.

Som framhålls i samma beslut behöver myndigheter och andra verksamheter av betydelse för Sveriges säkerhet vidta förebyggande åtgärder för att minska sårbarheter och skydda sin verksamhet.[50]

2015 års försvarsbeslut är det första där cyberhot på allvar diskuteras som ett antagonistiskt angrepp som kan hota en stats handlingsfrihet och ytterst dess suveränitet.[51] I vissa fall, som när ett IT-angrepp ger upphov till fysiska skador kan det enligt försvarsbeslutet vara att betrakta som ett väpnat angrepp.

48 Prop. 2020/21:30, s. 26.

49 Prop. 2020/21:30, s. 28-29.

50 Prop. 2020/21:30, s. 28-29.

51 Prop. 2014/15:109, s. 41.

Sårbarheterna i dagens globala IT-system anges vidare vara en av vår tids mest komplexa utmaningar och för att upprätthålla en hög nivå av cybersäkerhet i Sverige måste samhällsviktiga funktioner och kritiska IT-system kunna skyddas mot angrepp.

Utgångspunkten för planeringen av totalförsvaret, inklusive dess civila del, bör enligt försvarsbeslutet 2020 vara att under minst tre månader kunna hantera en säkerhetspolitisk kris i Europa och Sveriges närområde som innebär allvarliga störningar i samhällets funktionalitet samt krig under del av denna tid. Detta är en ambition som kan förefalla högt ställd i förhållande till det svenska civila försvarets förutsättningar men samtidigt lågt ställd i förhållande till den rådande säkerhetspolitiska situationen.

I 2020 årsförsvarsbeslut fastställs följande mål för det civila försvaret.

1) Värna civilbefolkningen.
2) Säkerställa de vktigaste samhällsfunktionerna.
3) Upprätthålla en nödvändig försörjning.
4) Bidra till det militära försvarets förmåga vid väpnat angrepp eller krig i vår omvärld.
5) Upprätthålla samhällets motståndskraft mot externa påtryckningar och bidra till att stärka försvarsviljan.
6) Bidra till att stärka samhällets förmåga att förebygga och hantera svåra påfrestningar på samhället i fred.
7) Bidra till förmågan att delta i internationella fredsfrämjande och humanitära insatser.[52]

Sammanfattningsvis kännetecknas försvarsbesluten 2015 och 2020 av stora satsningar på civilförsvaret och ett återtagande av den centrala planeringen av detta försvar. Samtidigt understryks att ansvarsprincipen fortsatt gäller även om den nu ska tillämpas inom ramen för en mer sammanhållen planering av det civila försvaret.

Det ska skapas en struktur för ansvar, ledning och samordning inom civilt försvar på central, högre regional, regional och lokal nivå. Den strukturen ska sedan tydliggöra och möjliggöra det enskilda ansvar som varje aktör inom ramen för det civila försvaret har att axla.

3.4 Sammanfattning

Det civila försvaret är den civila verksamhet som myndigheter, kommuner och regioner samt enskilda, företag och det civila samhället vidtar för att förbereda Sverige för krig. I fredstid utgörs verksamheten av beredskapsplanering och förmågehöjande åtgärder. Under höjd beredskap

52 Prop. 2020/21:30, s. 89.

och då ytterst krig utgörs verksamheten av nödvändiga åtgärder för att upprätthålla målet för civilt försvar.

Den snabba teknikutvecklingen, samhällets komplexitet och de ömsesidiga beroenden som kännetecknar olika samhällsaktörers och samhällsviktiga verksamheters förhållanden till varandra samt den omständighet att Sverige i allt väsentligt avvecklat sitt civila försvar har gjort att vi idag inte ens vet vilka verksamheter eller system som kommer att vara samhällsviktiga vid höjd beredskap. Än mindre vet vi vilka beroenden eller sårbarheter dessa har eller vad som kommer att krävas för att göra dem mer robusta.

Från ett i princip avvecklat civilt försvar ska Sverige nu bygga upp ett civilt försvar dimensionerat för ett invasionskrig. Som vi kommer att se i nästa avsnitt har regeringen i och med *förordningen (2022:524) om statliga myndigheters beredskap* och *förordningen (2022:525) om civilområdesansvariga länsstyrelser*, byggt en grundläggande struktur för fördelningen av det statliga ansvaret för detta arbete. Alla aktörer inom det civila försvaret, oavsett om det handlar om kommuner, regioner, näringsliv eller frivilligaktörer har dock ett omfattande arbete framför sig.

I nästa avsnitt redogörs för delar av Sveriges administrativa beredskap, i form av de regler som fördelar ansvaret för det civila försvaret och vilka skyldigheter som dessa regler ålägger respektive aktör.

4. Lagstiftning för hantering av höjd beredskap och ökade krav på robusthet

4.1 Inledning

I det här avsnittet behandlas de övergripande skyldigheter som enligt lag åvilar olika aktörer inom det civila försvaret. Tyngdpunkten ligger på myndigheters skyldigheter, men även privata aktörers ansvar kommer att beröras.

Vad som avses med höjd beredskap framgår av lagen (1992:1403) om totalförsvar och höjd beredskap. Höjd beredskap är ett samlingsbegrepp och innebär antingen skärpt beredskap eller högsta beredskap, se 1 § i lagen. Regeringen får besluta om höjd beredskap om Sverige är i krigsfara eller om det råder utomordentliga förhållanden på grund av krig utanför Sverige eller av att Sverige varit i krig eller krigsfara. Om Sverige är i krig råder högsta beredskap, se 3 § i lagen.

4.2 Statliga myndigheter

Vad gäller statliga myndigheter finns det i *förordningen (2022:524) om statliga myndigheters beredskap* bestämmelser om de uppgifter som dessa myndigheter har inför och vid fredstida krissituationer och höjd beredskap. Syftet med förordningen är att myndigheterna ska minska sårbarheten i samhället och utveckla en god förmåga att hantera sina uppgifter vid höjd beredskap.[53]

Varje myndighet är skyldig att beakta totalförsvarets krav i sin verksamhet. Myndigheterna ska också planera för att kunna fortsätta sin verksamhet så långt som det är möjligt under höjd beredskap.[54]

Utgångspunkten är alltså att myndigheters verksamhet måste vara tillräckligt robust och ha en planering för att klara de utmaningar som kan förväntas uppstå under höjd beredskap.

Även om skyldigheten omfattar alla statliga myndigheter kommer den naturligtvis att kräva förberedelser och planering i varierande grad och omfattning beroende på vilken myndighet det är fråga om och vilken verksamhet som bedrivs. Verksamheterna vid sådana myndigheter som till exempel Trafikverket, Tullverket, Kustbevakningen eller Polismyndigheten kan tänkas vara extra utsatta och känsliga för störningar under höjd beredskap, samtidigt som deras verksamheter naturligtvis är helt

53 Begreppet ”statliga myndigheter under regeringen” omfattar såväl statliga förvaltningsmyndigheter som statliga affärsverk och domstolar samt AP-fonderna, enligt Statskontorets definition, se: https://www.statskontoret.se/fokusomraden/fakta-om-statsforvaltningen/fakta-om-statsforvaltningen/. Läst den 2023-03-22.

54 Se 10 § i förordningen om statliga myndigheters beredskap.

nödvändiga att upprätthålla i en sådan situation. Här krävs det således omfattande förberedelser och planering för att respektive organisation ska kunna hantera olika tänkbara påfrestningar, det kan handla om beredskap inför såväl cyberangrepp som sabotagehandlingar och rena fysiska attacker.

Detsamma gäller för exempelvis Svenska Kraftnät, Sjöfartsverket och Luftfartsverket, som samtliga är statliga affärsverk vars verksamheter är av stor betydelse för totalförsvaret.

Därutöver finns det enligt förordningen om statliga myndigheters beredskap vissa specifikt utpekade myndigheter, vilka anges i bilaga 1 till förordningen, de så kallade beredskapsmyndigheterna. Det är fråga om myndigheter med ansvar inom en eller flera viktiga samhällsfunktioner och vars verksamhet har betydelse för totalförsvaret.[55] Det finns också särskilda beredskapssektorer vilka framgår av bilaga 2 till förordningen.[56] För varje beredskapssektor finns en sektorsansvarig myndighet medan övriga beredskapsmyndigheter i sektorn ska delta i arbetet.

Det framgår av 11 § förordningen om statliga myndigheters beredskap att personal som är anställd hos en myndighet och som inte tas i anspråk i totalförsvaret i övrigt får krigsplaceras med stöd av anställningsavtalet.

Även länsstyrelserna är viktiga aktörer inom det civila försvaret och de ingår i kretsen av beredskapsmyndigheter enligt förordningen om statliga myndigheters beredskap. För länsstyrelserna finns bestämmelser i *förordningen (2017:870) om länsstyrelsernas krisberedskap och uppgifter vid höjd beredskap*. Av förordningen framgår att länsstyrelsen är högsta civila totalförsvarsmyndighet inom länet, med ett ansvar att verka för att största möjliga försvarseffekt uppnås, se 6 §.

Vidare finns bestämmelser i *förordningen (2022:525) om civilområdesansvariga länsstyrelser*, där det framgår att de länsstyrelser som har ett civilområdesansvar ska ansvara för nödvändig samverkan mellan civilområdena.[57] Civilområdesansvariga länsstyrelser ska verka för att totalförsvaret under höjd beredskap har en enhetlig inriktning och bland annat ta initiativ till att samordna planeringen mellan statliga myndigheter och mellan dessa och försvarsmakten. De civilområdesansvariga länsstyrelserna ska också samverka med Försvarsmakten i frågor som rör totalförsvaret.[58] Under höjd beredskap ska de civilområdesansvariga länsstyrelserna samordna de civila försvarsåtgärderna och i samråd med Försvarsmakten verka för att det militära och civila försvaret samordnas.[59]

---

55 Som exempel på beredskapsmyndigheter kan bl.a. nämnas Affärsverket svenska kraftnät, DIGG, Statens energimyndighet, länsstyrelserna, Trafikverket och Myndigheten för samhällsskydd och beredskap.

56 Beredskapssektorerna är Ekonomisk säkerhet; Elektroniska kommunikationer och post; Energiförsörjning; Finansiella tjänster; Försörjning av grunddata; Hälsa, vård och omsorg; Livsmedelsförsörjning och dricksvatten; Ordning och säkerhet; Räddningstjänst och skydd av civilbefolkningen samt transporter.

57 Länsstyrelserna i Norrbottens, Örebro, Stockholms, Östergötlands, Västra Götalands och Skåne län är civilområdesansvariga länsstyrelser.

58 Se 6 § förordningen (2017:870) om länsstyrelsernas krisberedskap och uppgifter vid höjd beredskap.

59 Se 6 § förordningen (2017:870) om länsstyrelsernas krisberedskap och uppgifter vid höjd beredskap.

4.3 Kommuner och regioner

Vid höjd beredskap ska kommuner och regioner vidta de särskilda åtgärder i fråga om planering och inriktning av verksamheten, tjänstgöring och ledighet för personal samt användning av tillgängliga resurser som är nödvändiga för att de ska kunna fullgöra sina uppgifter inom totalförsvaret.[60] Detta framgår av 7 § lagen om totalförsvar och höjd beredskap.

Närmare bestämmelser om vilka åtgärder som ska vidtas finns i LEH samt FEH.[61]

Bestämmelserna i LEH syftar till att kommuner och regioner ska minska sårbarheten i sin verksamhet och hantera krissituationer i fred. Därigenom ska de också uppnå en grundläggande förmåga till civilt försvar.[62] Kommuner och regioner har vidare en skyldighet att vidta de förberedelser som behövs för verksamheten under höjd beredskap.[63]

Kommuner och regioner ska även ha de planer som behövs för verksamheten under höjd beredskap, av vilka bland annat ska framgå vilken verksamhet som avses att bedrivas vid sådana omständigheter.[64] Av planerna ska också framgå krigsorganisationen och den personal som ingår i denna samt vad som i övrigt behövs för att kommunen eller regionen ska kunna höja sin beredskap och bedriva verksamheten i en sådan situation.[65]

Vid planering och förberedelsearbete inför höjd beredskap bör kommuner och regioner utgå från vissa antaganden om vilka olika typer av händelser som kan komma att inträffa och vilka konsekvenser dessa händelser kan få för invånarna och verksamheten. Det behövs också en analys av det ansvar som kommunerna och regionerna har vid höjd beredskap.

Utgångspunkten är därvid ansvarsprincipen, det vill säga att den aktör som har ansvar för en viss verksamhet eller funktion under normala förhållanden också ska ha ansvaret under höjd beredskap. De lagar som reglerar kommuners och regioners ansvar under fredstid ska således som regel tillämpas även under höjd beredskap. Av det följer till exempel att sådana samhällsviktiga verksamheter som vård, skola och omsorg ska upprätthållas så länge som det är möjligt.

I samband med planering och förberedelser måste kommuner och regioner också identifiera de viktigaste verksamheterna och besluta om hur prioritering ska ske vid höjd beredskap, där resurserna kan förväntas vara begränsade och måste användas på ett sätt som skapar mesta möjliga nytta.

Planeringen bör även omfatta sådana verksamheter som kan tillkomma under höjd beredskap samt behovet av att anpassa befintliga verksamheter

60 Se 7 § lagen (1992:1403) om totalförsvar och höjd beredskap.

61 Se hänvisning i 2 § förordningen (2015:1053) om totalförsvar och höjd beredskap.

62 Se 1 kap. 1 § LEH.

63 Se 3 kap. 1 § LEH.

64 Se 4 § FEH.

65 Se 4 § FEH.

till en ny situation. Till exempel kan de resurser och den inriktning som sjukvården och barnomsorgen kräver behöva ändras eller förstärkas under höjd beredskap.

Varje kommun ska hålla länsstyrelsen underrättad om de beredskapsförberedelser som vidtagits och om övriga förhållanden som har betydelse för det civila försvaret.[66] Varje region ska hålla Socialstyrelsen och MSB underrättade om de beredskapsförberedelser som vidtagits och om övriga förhållanden som har betydelse för det civila försvaret.[67]

7 § lagen om totalförsvar och höjd beredskap får anses ge kommuner och regioner tillräckligt lagstöd för att kunna krigsplacera sådan personal som behövs för en god beredskap.

4.4 Civila aktörer

Som framgått tidigare är det inte bara det offentliga som ingår i det civila försvaret. Vid höjd beredskap ska också de enskilda organisationer och företag som enligt överenskommelse eller på annan grund är skyldiga att fortsätta sin verksamhet i krig vidta de särskilda åtgärder i fråga om planering och inriktning av verksamheten, tjänstgöring och ledighet för personal samt användning av tillgängliga resurser som är nödvändiga för att de under de rådande förhållandena ska kunna fullgöra dessa skyldigheter.[68]

En stor del av den samhällsviktiga verksamhet som bedrivs inom exempelvis energiförsörjning, livsmedelsförsörjning, transporter, hälso- och sjukvård samt kommunal service utförs av representanter för det privata näringslivet. Näringslivet utgör därmed också en viktig del av totalförsvaret.

Vi har ovan beskrivit ansvarsprincipen, det vill säga att den som har ansvar för en verksamhet under normala förhållanden också ska ha det i en krissituation eller under höjd beredskap. Utifrån den principen kan det ofta anses vara både lämpligt och rimligt att enskilda organisationer och företag som har fått förtroendet att bedriva samhällsviktig verksamhet i fredstid också, i så stor utsträckning som möjligt, ska göra det när höjd beredskap råder i samhället.[69]

Vissa näringsidkare är också skyldiga, på begäran av en totalförsvarsmyndighet, att delta i planeringen av totalförsvaret. Detta framgår av *lagen (1982:1004) om skyldighet för näringsidkare, arbetsmarknadsorganisationer m.fl. att delta i totalförsvarsplaneringen*. De näringsidkare som omfattas ska lämna de upplysningar om bland annat personal, lokaler, maskiner och annan utrustning som totalförsvarsmyndigheten behöver

66 Se 6 § FEH.

67 Se 7 § FEH.

68 Se 7 § lagen om totalförsvar och höjd beredskap.

69 Jfr. regeringen som i bl.a. prop. 2020/21:30, Totalförsvaret 2020-2025, s. 134 f. har uttryckt att alla aktörer i totalförsvaret har ansvar för att stärka beredskapen och förmågan att genomföra verksamhet även under kris och ytterst i krig. Det gäller såväl offentliga aktörer som privata företag och ytterst enskilda invånare.

för sitt planeringsarbete samt, om det behövs, i övrigt medverka vid planeringen av de egna uppgifterna inom totalförsvaret.

Vilka myndigheter som är totalförsvarsmyndigheter framgår av en uppräkning i 1 § förordningen om skyldighet för näringsidkare, arbetsmarknadsorganisationer m.fl. att delta i totalförsvarsplaneringen. Om en myndighet som inte är en av de i förordningen angivna totalförsvarsmyndigheterna finner att den för sin totalförsvarsplanering behöver upplysningar eller annan medverkan enligt lagen, ska myndigheten anmäla detta till MSB, som får vidta de åtgärder som myndighetens anmälan föranleder, varefter resultatet på lämpligt sätt ska delges myndigheten.

4.5 Verksamhetsutövare enligt säkerhetsskyddslagen

Säkerhetsskyddslagen (2018:585) har till syfte att skydda särskilt känsliga verksamheter, primärt mot sådana angrepp som spioneri, sabotage, terroristbrott och andra brott. Säkerhetsskyddslagen medför vissa skyldigheter för utövarna som är av intresse för, och påverkar, de berörda organisationernas robusthet i förhållande till antagonistiska hot.

Säkerhetsskyddslagen gäller för utövare av säkerhetskänslig verksamhet, så kallade Verksamhetsutövare. I lagen anges vidare att med ”säkerhetskänslig verksamhet” avses verksamhet som antingen är av betydelse för Sveriges säkerhet, eller omfattas av ett för Sverige förpliktande internationellt åtagande.[70] Det är främst det första ledet som är av intresse för denna rapport, det vill säga verksamhet som är av betydelse för Sveriges säkerhet.

De skyldigheter som framgår av lagen gäller oavsett om Verksamhetsutövaren är en statlig eller kommunal myndighet eller ett privat företag.

4.5.1 Sveriges säkerhet

Vad som närmare avses med ”Sveriges säkerhet” framgår inte uttryckligen av lagen genom någon uppräkning av vilka verksamheter, eller vilka typer av verksamheter, som ska anses säkerhetskänsliga. Ett av skälen till det är att såväl samhället som dess olika hotbilder inte är statiska, utan kommer att förändras över tid. Avsikten är att bestämmelserna i säkerhetsskyddslagen ska kunna vara fortsatt relevanta även i tider av betydande förändring.

Ett annat skäl är att det ur ett säkerhetsperspektiv skulle vara olämpligt att i lagstiftning avslöja alla skyddsvärda verksamheter i Sverige.[71]

Viss vägledning finns dock i lagens förarbeten. Där konkretiseras vissa kriterier för bedömningen av om en verksamhet är av betydelse för

70 Se 1 kap. 1 § säkerhetsskyddslagen.

71 Prop. 2017/18:89, s. 42.

Sverige säkerhet (och därmed av en sådan säkerhetskänslig natur att den omfattas av säkerhetsskyddslagen).[72] Först och främst görs en uppdelning mellan Sveriges yttre och inre säkerhet.

Sveriges yttre säkerhet avser den territoriella suveräniteten och den politiska självständigheten. Detta inbegriper framför allt Försvarsmaktens verksamhet, men kan även omfatta verksamheter inom till exempel försvarsindustrin.[73]

Sveriges inre säkerhet rör i sin tur förmågan att upprätthålla och säkerställa Sveriges statsidé avseende funktion, handlingsfrihet och oberoende. Detta avser till stor del skyddet av särskilt kritiska anläggningar, funktioner och informationssystem som är kopplade till Sveriges demokratiska statsskick, rättsväsende och brottsbekämpande förmåga.[74]

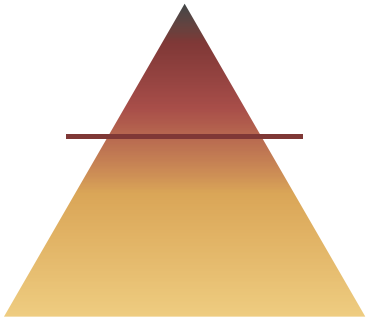
Ytterligare verksamheter som kan ha betydelse för Sveriges säkerhet är samhällsviktiga verksamheter.[75] MSB har definierat vad som utgör samhällsviktig verksamhet på följande sätt: ”*Verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet*”.[76] I detta inbegrips bland annat barnomsorg, utbildning, offentlig förvaltning och personalförsörjning.

Om en direkt koppling skulle göras mellan begreppet samhällsviktig verksamhet och säkerhetskänslig verksamhet enligt säkerhetsskyddslagen skulle med andra ord ett mycket stort antal verksamheter anses utgöra säkerhetskänslig verksamhet. Av förarbetena till säkerhetsskyddslagen framgår dock att de båda begreppen är endast delvis överlappande.

Utgångspunkten är att endast de mest skyddsvärda samhällsviktiga verksamheterna som har ett kvalificerat skyddsbehov ska omfattas av säkerhetsskyddslagstiftningen. Säkerhetsskyddslagen ska i första hand skydda ”*särskilt känsliga verksamheter mot antagonistiska angrepp, till exempel spioneri, sabotage och terroristbrott*”.[77]

Det är med andra ord bara nationellt samhällsviktig verksamhet som omfattas av säkerhetsskyddslagens krav.[78]

Detta förhållande brukar ibland visualiseras med hjälp av följande bild[79]:



Figur 4.1: Förhållandet mellan nationellt samhällsviktig verksamhet och samhällsviktig verksamhet

72 Se prop. 2017/18:89, s. 44-45.

73 Prop. 2017/18:89, s. 44.

74 Prop. 2017/18:89, s. 44.

75 Prop. 2017/18:89, s. 44-45

76 Se MSB, dnr. 2020-11275, ”Uppdaterad definition samhällsviktig verksamhet”.

77 Se prop. 2017/18:89, s. 39 ff.

78 Se prop. 2017/18:89, s. 39 ff.

79 Bilden är hämtad ur prop. 2017/18:89.

Pyramiden rymmer alla samhällsviktiga verksamheter i Sverige, exempelvis det lokala apoteket, förskolan och stamnätet.

Det är däremot bara i pyramidens övre topp som de nationellt samhällsviktiga verksamheterna finns. Det är dessa som omfattas av säkerhetsskyddslagens krav.

Nationellt samhällsviktiga verksamheter återfinns främst inom följande sektorer[80]:

- Energiförsörjning
- Elektroniska kommunikationer
- Finansiella tjänster (centrala betalningssystem)
- Livsmedelsförsörjning
- Vattenförsörjning
- Transporter

Något förenklat kan det därmed sägas att varken förskolan eller det lokala apoteket omfattas av säkerhetsskyddslagen, medan stamnätet gör det.

Kravet på att en verksamhet ska vara av nationell vikt innebär däremot inte att den måste bedrivas på nationell nivå. Även organisationer som enbart bedriver verksamhet på regional eller kommunal nivå kan ändå anses bedriva säkerhetskänslig verksamhet, beroende på arten av verksamheten i fråga. Detta kan exempelvis vara fallet om en störning i verksamheten kan påverka ett stort antal människor med nationella följdverkningar, eller om människor som påverkas har funktioner i andra verksamheter med direkt betydelse för Sveriges säkerhet.[81]

4.5.2 Skyldigheter för Verksamhetsutövare

Oavsett vilken typ av organisation det är fråga om så medför bestämmelserna i säkerhetsskyddslagen skyldigheter för varje utövare av säkerhetskänslig verksamhet.

Verksamhetsutövare är därför bland annat skyldiga att:

- Genomföra och upprätta en säkerhetsskyddsanalys,
- Planera och vidta nödvändiga säkerhetsskyddsåtgärder baserat på vad som framkommit genom säkerhetsskyddsanalysen, bland annat
  - Anpassa sina informationssystem så att de lever upp till säkerhetsskyddslagstiftningens krav,
- Ingå säkerhetsskyddsavtal med externa leverantörer i vissa fall.[82]

80 Se Säkerhetspolisen, ”Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys”, 2019, s. 13.

81 Se prop. 2017/18:89, s. 42 f.

82 Se 2 kap. 1 § samt 4 kap. 1 § säkerhetsskyddslagen.

Samtliga dessa åtgärder leder i sin tur till en digital robusthet, på så sätt att Verksamhetsutövaren skapar en förståelse för de säkerhetskänsliga värdena i den egna verksamheten och tryggar att säkerheten upprätthålls även i samband med att en utomstående leverantör får tillgång till den.

4.6 Informationssäkerhet

Det finns krav på informationssäkerhet i flera olika regelverk, bland annat säkerhetsskyddslagen, NIS-lagen och förordningen om statliga myndigheters beredskap. Dessa tre regelverk har många likheter men också skillnader, inte minst i hur det skyddsvärda intresset definieras och avgränsas, men också med vilken detaljeringsgrad de reglerar själva informationssäkerhetsarbetet.

För myndigheter som omfattas av säkerhetsskyddslagen har säkerhetspolisen meddelat föreskrifter om hur säkerhetsskyddsarbetet, inklusive säkerhetsskyddsanalys och informationssäkerhet, ska bedrivas.[83] Till skillnad från övriga ovan nämnda regelverk är säkerhetsskyddslagstiftningen inte riskbaserad, utan konsekvensbaserad vilket begränsar Verksamhetsutövarens möjlighet att välja och anpassa skyddsåtgärder till en lämplig skyddsnivå utifrån risken. Om verksamheten är säkerhetskänslig ska de åtgärder som framgår av regleringen tillämpas oberoende av sannolikheten för att risken realiseras.

För myndigheter som, i egenskap av tjänsteleverantör, omfattas av NIS-regleringen finns, utöver NIS-lagen och den tillhörande nationella förordningen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster även ett antal föreskrifter som MSB meddelat.[84]

Föreskrifterna ålägger framförallt tjänsteleverantörer att bedriva ett strukturerat och riskbaserat informationssäkerhetsarbete med stöd av ISO 27001 eller motsvarande, men lämnar inom ramen för detta ett stort utrymme för verksamheten att besluta hur detta ska bedrivas, särskilt vad gäller vilka säkerhetsåtgärder som ska vidtas. I sammanhanget ska nämnas att ett nytt EU-direktiv, även kallat NIS 2-direktivet, med mer detaljerade krav inom informationssäkerhetsarbetet, har antagits och att den svenska lagstiftaren nu arbetar med att införliva direktivet i den svenska lagstiftningen.[85]

För myndigheter som omfattas av förordningen om statliga myndigheters beredskap har MSB meddelat såväl föreskrifter som en vägledning om informationssäkerhet och säkerhetsåtgärder i informationssystem.[86]

---

83 PMFS 2022:1 föreskrifter om säkerhetsskydd.

84 MSBFS 2018:8 föreskrifter och allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster, MSBFS 2018:9 föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster, 2018:10 föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av digitala tjänster och 2018:11 föreskrifter och allmänna råd om frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet.

85 Direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet).

86 MSBFS 2020:6 föreskrifter om informationssäkerhet för statliga myndigheter, MSBFS 2020:7 Föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter, MSBFS 2020:8 föreskrifter om rapportering av it-incidenter för statliga myndigheter och MSB, publ. MSB2032, ”Vägledning - Säkerhetsåtgärder i informationssystem”.

Utöver dessa regelverk finns även internationella standarder för hur informationssäkerhetsarbete bedrivs, främst i form av ISO 27000-serien. Grundläggande för allt informationssäkerhetsarbete är uppdelningen i informationens *konfidentialitet* (att informationen inte tillgängliggörs för obehöriga), *riktighet* (att informationen är korrekt och fullständig, och skyddad mot oönskad förändring) och *tillgänglighet* (åtkomlig och användbar för behörig person vid rätt tillfälle).

Kravet på att kritisk information är tillgänglig för verksamhetens behov är särskilt viktigt. Många allvarliga incidenter handlar just om att kritisk information och systemen för att hantera den blivit otillgängliga, exempelvis på grund av en ransomware-attack.

När informationssäkerhetsarbetet bedrivs bör därför en myndighet som strävar efter robusthet särskilt analysera sådana risker som leder till tillgänglighetsförluster och vilka åtgärder som behöver vidtas för att minska sannolikheten eller konsekvenserna av sådana risker.

Det bör understrykas att åtgärder som minskar *en* sårbarhet samtidigt kan öka en annan. Exempelvis kan redundans i informationslagring genom att lagra information på flera oberoende platser, vilket minskar risken för tillgänglighetsförluster, samtidigt leda till större risk för konfidentialitetsförluster i och med att attackytan för en angripare utökas.

Även om det är den enskilda organisationen som ytterst ansvarar för att hantera sin information, så är det viktigt att förbättra förutsättningarna för att bedriva ett systematiskt informationssäkerhetsarbete på ett mer samordnat sätt.[87] MSB har ett ansvar att stödja och samordna arbetet med samhällets informationssäkerhet, inklusive att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och regioner.[88]

4.7 Sammanfattning

Alla aktörer inom det civila försvaret har i olika utsträckning lagstadgade skyldigheter att delta i totalförsvaret och att planera sin verksamhet för höjd beredskap.

Detta gäller särskilt för offentliga aktörer men också, genom bland annat ansvarsprincipen, för privata aktörer som bedriver samhällsviktig verksamhet.

Säkerhetsskyddslagen gäller lika för alla aktörer som omfattas av den, oaktat om dessa är myndigheter eller privata bolag.

I följande avsnitt kommer det att redogöras för hur myndigheter kan fullgöra dessa skyldigheter, ofta i samverkan med privata leverantörer, inom ramen för myndigheternas digitala transformation. Genom att vidta de föreslagna åtgärderna kan myndigheterna uppnå en ökad robusthet och säkerställa efterlevnad av de lagkrav som gäller för dem.

87 SOU 2021:97, s. 75.

88 11 a § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

5. Åtgärder för robust digital transformation

5.1 Inledning

Som beskrivits i avsnitt 2 innebär den ökade digitala transformationen ett antal utmaningar, nämligen bland annat:

› Utökade digitala leveranskedjor.

› Minskad robusthet som en följd av ökad utkontraktering.

› De digitala systemens inneboende komplexitet.

› Brist på digital suveränitet.

› Bristande IT-kompetens, både internt och på marknaden.

› Växande datamängder.

› En ökad automatisering.

I detta avsnitt presenteras förslag på åtgärder för att hantera dessa utmaningar.

En ökad digital robusthet i offentlig sektor förutsätter en grad av självförsörjande och leverantörsoberoende som hittills inte kännetecknat den digitala transformationen. Ett avgörande inslag i de åtgärder som föreslås nedan är därför hur en upphandlande organisation på bästa sätt kan hantera sina leverantörsberoenden. För att kunna stärka sin digitala robusthet bör en verksamhet även utföra nödvändiga risk- och sårbarhetsanalyser enligt tillämplig lagstiftning.

Detta kan ske genom en sammanhållen process som inkluderar följande steg:

1) Inventering av:
   - samhällsviktiga verksamheter och system, och
   - kritiska leverantörsberoenden och skyddsvärda informationsresurser (inom ramen för eller utanför ”samhällsviktiga verksamheter och system”).
2) Genomförande av risk- och sårbarhetsanalyser, eventuella säkerhetsskyddsanalyser samt ett systematiskt informationssäkerhetsarbete.
3) Vidta lämpliga åtgärder för att:
   - adressera identifierade risker, hot och sårbarheter mot samhällsviktiga verksamheter och system, och
   - öka myndighetens nivå av kontroll och minska sitt leverantörsberoende till kritiska tjänsteleverantörer.

Nedan följer en genomgång av dessa steg, och de krav som bakomliggande lagstiftning ställer.

5.2 Inventering

5.2.1 Samhällsviktiga verksamheter och system

Den första delen av inventeringsarbetet handlar om att identifiera den eller de verksamheter inom myndigheten som är av vikt för det civila försvaret. Avgörande för detta är vilka verksamheter eller system som är samhällsviktiga och som måste kunna upprätthållas även vid höjd beredskap.

Ett annat sätt att uttrycka det är att beredskapsarbetet ska avse sådan verksamhet som bidrar till uppfyllandet av de mål som gäller för det civila försvaret, se avsnitt 3.3 ovan.

Till vägledning för detta inventeringsarbete har MSB tagit fram följande fem skyddsvärden med utgångspunkt i mål beslutade av riksdag och regering:

1) Människors liv och hälsa – Fysisk och psykisk hälsa hos dem som drabbas direkt eller indirekt av en händelse.

2) Samhällets funktionalitet – Funktionalitet och kontinuitet i det som direkt eller indirekt starkt påverkar samhällsviktig verksamhet och därmed får konsekvenser för människor, företag och andra organisationer.

3) Demokrati, rättssäkerhet och mänskliga fri- och rättigheter – Människors tilltro till demokratin och rättsstaten samt förtroende för samhällets institutioner och det politiska beslutsfattandet, ledningsförmåga på olika nivåer, avsaknad av korruption och rättsövergrepp.

4) Miljö och ekonomiska värden – Miljön i form av mark, vatten och fysisk miljö, biologisk mångfald, värdefulla natur- och kulturmiljöer samt annat kulturarv. Ekonomiska värden i form av privat och offentlig egendom samt värdet av produktion av varor och tjänster.

5) Nationell suveränitet – Kontroll över nationens territorium, nationell kontroll över de politiska beslutsprocesserna i landet samt säkrande av nationens försörjning med förnödenheter. Nationell suveränitet är en grundläggande förutsättning för att kunna värna övriga värden.

Utifrån dessa värden kan samhällsviktig verksamhet identifieras. Som angetts ovan är samhällsviktig verksamhet sådan verksamhet eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner vilka är nödvändiga för att upprätthålla dessa skyddsvärden.

MSB har gett ut en vägledning för identifiering av samhällsviktig verksamhet.[89] I denna finns en steg-för-stegmetod för att identifiera sådan verksamhet som bör bli föremål för förmågehöjande åtgärder.

Som ett komplement till sin metodbeskrivning har MSB även gett ut en lista över sådana verksamheter som MSB bedömer är samhällsviktiga inom ramen för följande fjorton huvudsektorer.[90]

1	Barnomsorg och utbildning	8	Information och kommunikation
2	Dricksvattenförsörjning, avlopp och avfall	9	Livsmedelsförsörjning
3	Ekonomisk säkerhet	10	Offentlig förvaltning
4	Energiförsörjning	11	Ordning och säkerhet
5	Finansiella tjänster	12	Personalförsörjning
6	Handel och industri	13	Räddningstjänst och skydd av civilbefolkning
7	Hälsa, vård och omsorg	14	Transporter

Figur 5.1: Lista över verksamheter som MSB bedömer vara samhällsviktiga inom ramen för 14 huvudsektorer

5.2.2 Kritiska leverantörsberoenden och skyddsvärda informationsresurser

Utöver inventeringen av samhällsviktiga verksamheter är det viktigt att identifiera de leverantörer som är kritiska för att upprätthålla myndighetens funktion och verksamhet i händelse av höjd beredskap.

Det kan även finnas andra skyddsvärda informationsresurser som också är kritiska för myndigheten och som identifieras inom ramen för det systematiska informationssäkerhetsarbetet.

När sådana beroenden och informationsresurser har identifierats ska de även ingå som en del i den risk- och sårbarhetsanalys som ska genomföras, se nedan.

I avsnitt 5.4 presenteras en modell för hur en myndighet kan arbeta för att minska sitt beroende gentemot de leverantörer som identifieras i inventeringen.

89 MSB, publ. MSB1408, ”Vägledning för identifiering av samhällsviktig verksamhet” (reviderad oktober 2021).

90 MSB, publ. MSB1844, ”Identifiering av samhällsviktig verksamhet: lista med viktiga samhällsfunktioner”.

5.3 Risk- och sårbarhetsanalyser

5.3.1 Behovet av en risk- och sårbarhetsanalys

Syftet med en risk- och sårbarhetsanalys är att stärka den egna organisationens, och därmed även samhällets, beredskap genom att skapa kunskap om de hot och risker som finns mot den egna verksamheten och att vidta åtgärder för att på bästa sätt skapa robusta system som ”*långsiktigt klarar olika typer av påfrestningar*”.[91]

Skyldighet att genomföra risk- och sårbarhetsanalyser finns i en rad olika lagstiftningar, däribland LEH och förordningen om statliga myndigheters beredskap. Motsvarande skyldighet finns även för Verksamhetsutövare enligt säkerhetsskyddslagen genom skyldigheten att genomföra en säkerhetsskyddsanalys.[92] Vi menar därutöver att myndigheter bör utföra risk- och sårbarhetsanalyser inte bara när det krävs enligt lag utan i alla sammanhang när ett kritiskt leverantörsberoende har identifierats.

5.3.2 Risk- och sårbarhetsanalysens omfattning och innehåll

Det finns olika metoder och modeller för att genomföra risk- och sårbarhetsanalyser.[93] Vilken metod och modell som bör användas beror delvis på vilken lagstiftning som ligger till grund för analysens genomförande.

Kraven på vad en säkerhetsskyddsanalys ska innehålla framgår av 2 kap. 2-9 §§ i Säkerhetspolisens föreskrifter.[94]

På motsvarande sätt har MSB i tre olika föreskrifter angett vad risk- och sårbarhetsanalyser ska innehålla, i förhållande till olika aktörer.

Föreskrift	Mottagare
MSBFS 2015:4 föreskrifter och allmänna råd om landstings risk- och sårbarhetsanalyser	Regioner (landsting)
MSBFS 2015:5 föreskrifter och allmänna råd om kommuners risk- och sårbarhetsanalyser	Kommuner
MSBFS 2016:7 föreskrifter och allmänna råd om statliga myndigheters risk- och sårbarhetsanalyser	Statliga myndigheter (inkluderat särskilda bestämmelser för länsstyrelser)

Figur 5.2 - Föreskriftssammanställning

91 FOI:s modell för risk- och sårbarhetsanalys (FORSA), handbok, 2011, s. 34.

92 2 kap. 1 § säkerhetsskyddslagen.

93 Se exempelvis de modeller som nämns i FOI:s modell för risk- och sårbarhetsanalys (FORSA), handbok, 2011, s. 54.

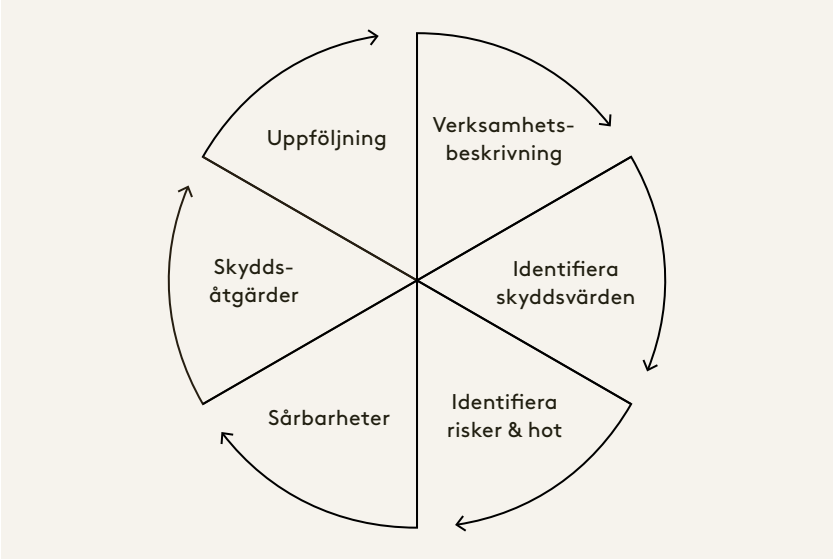
94 PMFS 2022:1.

Kraven på vad en risk- och sårbarhetsanalys ska innehålla bör läsas i ljuset av den bakomliggande lagstiftningens skyddsintressen.

Där säkerhetsskyddslagstiftningen uteslutande fokuserar på risker kopplade till antagonistiska hot, så har LEH och förordningen om statliga myndigheters beredskap en mer heltäckande syn på risker, där samtliga relevanta hot mot den egna verksamheten ska beaktas.

Trots detta är det arbete som ska ske enligt respektive regelverk i stora delar överlappande och det finns därför goda skäl för samordning.[95]

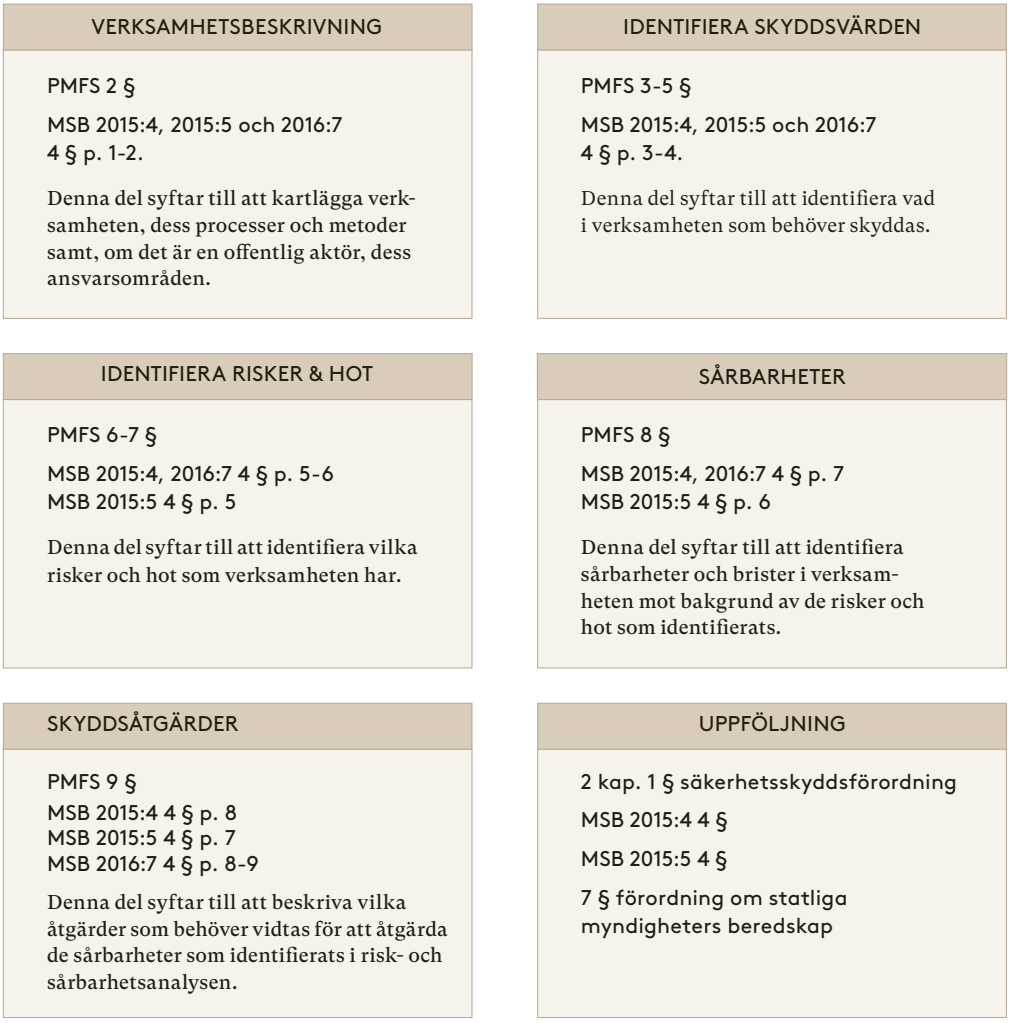
Såväl risk- och sårbarhetsanalyser och säkerhetsskyddsanalyser bygger på följande kontinuerliga och iterativa arbetsprocess:



Figur 5.3: Beskrivning av arbetsprocessen med risk- och sårbarhetsanalyser samt säkerhetsskyddsanalyser

I tabellen nedan framgår de bestämmelser som reglerar stegen i arbetsprocessen för respektive regelverk. I nästa avsnitt beskrivs skillnader och likheter i de olika regleringarna.

95 Se Säkerhetspolisen, ”Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys”, 2019, s. 21, se även 3 § MSBFS 2015:4 och 3 § MSBFS 2015:5 som kräver att arbetet med risk– och sårbarhetsanalyser samordnas med motsvarande arbete som sker enligt annan lagstiftning.



Figur 5.4: Bestämmelser som reglerar respektive steg i arbetsprocessen för risk-och sårbarhetsanalyser samt säkerhetsskyddsanalyser

Verksamhetsbeskrivning

Verksamhetsbeskrivningen är en viktig del i såväl en risk- och sårbarhetsanalys enligt LEH och förordningen om statliga myndigheters beredskap som en säkerhetsskyddsanalys enligt säkerhetsskyddslagen.

I en säkerhetsskyddsanalys ska dock Verksamhetsutövaren särskilt specificera vilka delar av verksamheten som är av betydelse för Sveriges säkerhet utifrån kategorierna Sveriges yttre säkerhet, Sveriges inre säkerhet, nationellt samhällsviktig verksamhet, verksamhet av betydelse för Sveriges ekonomi och verksamhet som kan generera skada på annan säkerhetskänslig verksamhet.[96]

Identifiering av skyddsvärden

Myndigheten måste vidare identifiera sina skyddsvärden. För säkerhetskänslig verksamhet rör detta särskilt identifiering av de uppgifter, tillgångar, anläggningar som verksamheten behöver skydda mot antagonistiska hot.

96 Se 2 kap. 2 § PMFS 2022:1.

Kraven i MSB:s föreskrifter handlar snarare om att myndigheten ska identifiera vilken samhällsviktig verksamhet som finns inom myndighetens geografiska– eller ansvarsområde. Det skyddsvärda är i detta fall vilka verksamheter inom myndighetens områden som behöver kunna bedrivas även vid höjd beredskap.

Identifiering av risker och hot

Efter att ha genomfört en verksamhetsbeskrivning samt en identifiering av aktuella skyddsvärden ska en identifiering ske av de risker och hot som myndigheten står inför.

I detta avseende ska säkerhetsskyddsanalyser innehålla en identifiering av de antagonistiska hot som finns mot verksamheten.[97]

De risk- och sårbarhetsanalyser som ska upprättas enligt LEH och förordningen om statliga myndigheters beredskap innehåller istället krav på att beakta även andra risker som kan påverka den samhällsviktiga verksamheten, exempelvis identifierade kritiska leverantörsberoenden.[98]

Detta innebär att en risk- och sårbarhetsanalys enligt LEH och förordningen om statliga myndigheters beredskap ofta kan innehålla samma genomgång av potentiella antagonistiska hot som en säkerhetsskyddsanalys, men därutöver innehålla ytterligare risker i form av alla ”*extraordinära händelser*” som kan inträffa och hur de kan påverka verksamheten.[99] Detta inkluderar vilka underliggande kritiska beroenden som finns för att samhällsviktig verksamhet ska fungera, till exempel IT, energileveranser eller vattenförsörjning, och att ha en planering för hur en sådan försörjning ska kunna säkerställas även vid allvarliga störningar.

Identifiering av sårbarheter

Efter att ha identifierat vad verksamheten ska skydda och vad den ska skydda mot, ska en identifiering även ske av vilka sårbarheter som finns i förhållande till verksamhetens utformning och de identifierade hoten.

I sårbarhetsbedömningen kan det exempelvis ingå praktiska tester av säkerhetsskyddet, analys av inträffade incidenter och erfarenhetsbaserade bedömningar. Dessa praktiska tester samt andra underlag kan sedan sammanställas och bedömas i syfte att föreslå lämpliga säkerhetsskyddsåtgärder.[100]

Skyddsåtgärder

Inom ramen för det näst sista steget ska konkreta åtgärder vidtas för att förebygga de sårbarheter som har identifierats. Inom området för informationssäkerhet har Säkerhetspolisen gett ut en särskild vägledning som innehåller förslag på åtgärder som kan vidtas för att öka systemens

97 Se och jfr 1 kap. 2 § säkerhetsskyddslagen och 2 kap. 6-7 §§ PMFS 2022:1.

98 Se exempelvis 4 § MSBFS 2015:4.

99 Se 2 kap. 1 § LEH.

100 Säkerhetspolisen, ”Vägledning i säkerhetsskydd – Säkerhetsskyddsanalys”, 2019, s. 21.

säkerhetsskydd. Utöver detta föreslås nedan ett antal åtgärder som kan vidtas för att öka en myndighets digitala robusthet.

Vad som utgör en lämplig åtgärd är naturligtvis helt beroende av den enskilda myndighetens verksamhet, förutsättningar och de sårbarheter som den identifierat. Myndigheters åtgärder måste därför grundas i den egna risk- och sårbarhetsanalysen och någon generell förteckning över lämpliga åtgärder går inte att upprätta.

Uppföljning och uppdatering

För att inte riskera att den egna robustheten minskar över tid måste myndigheten ständigt omvärdera och uppdatera sin risk- och sårbarhetsanalys och säkerhetsskyddsanalys. Förutom att följa upp åtgärder från tidigare analyser och kontrollera att dessa genomförts på ett adekvat sätt måste myndigheten även identifiera nya eller förändrade hotbilder eller sårbarheter. Ett sådant krav på uppföljning och uppdatering följer direkt av såväl LEH, förordningen om statliga myndigheters beredskap som säkerhetsskyddslagen.

För såväl förordningen om statliga myndigheters beredskap som säkerhetsskyddslagen gäller att analyserna ska uppdateras minst vartannat år. Säkerhetsskyddsanalyser ska dock därutöver uppdateras när behov uppstår.[101]

MSB:s föreskrifter för kommuner och regioner innehåller ett mer generellt krav på att risk- och sårbarhetsanalyserna regelbundet ska följas upp. Uppföljning ska rapporteras årligen till länsstyrelsen.[102]

5.3.3 Relation till ledningssystem för informationssäkerhet

Som vi beskrivit ovan är framtagandet av en risk- och sårbarhetsanalys en del av en större iterativ process med ett antal steg. Inom det mer avgränsade området informationssäkerhetsarbete är det vanligt, och för statliga myndigheter obligatoriskt, att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ISO 27001 eller motsvarande.

Denna standard beskriver hur ett ledningssystem för informationssäkerhet, ett så kallat LIS, ska utformas, vilket bland annat omfattar ett analysarbete för att identifiera skyddsvärda informationstillgångar, risker som hotar dessa tillgångar och lämpliga skyddsåtgärder som minskar sådana risker. En sådan analys överlappar en risk- och sårbarhetsanalys, och samma typ av risk kan behöva hanteras med samma skyddsåtgärd både inom ramen för en risk- och sårbarhetsanalys som i ett LIS. Det kan därför vara svårt att veta i vilken utsträckning samma arbete kan

101 Se 2 kap. 1 § säkerhetsskyddsförordning (2021:955) och 7 § förordningen om statliga myndigheters beredskap.

102 Se 5 § i MSBFS 2015:5.

täcka behoven för såväl en risk- och sårbarhetsanalys som för ett LIS, inte minst i vilken ordning som beslut kring skyddsåtgärder tas.

En risk- och sårbarhetsanalys har en mer heltäckande syn på vad som kan utgöra risk än vad en säkerhetsskyddsanalys har. Informationssäkerhetsarbete är ännu mer avgränsat och handlar om vilka hot som kan orsaka skada på informationens konfidentialitet, riktighet och integritet. Samtidigt har ett LIS en detaljerad process för att bedöma vilka säkerhetsåtgärder som ska vidtas med exempelvis förteckningar på relevanta åtgärder för just dessa hot (såsom system för lösenordshantering, nyckelhantering för kryptografiska nycklar, eller säkerhetskopiering av information). Ett LIS kan därför ofta vara både smalare och mer långtgående än en risk- och sårbarhetsanalys.

Samtidigt är krav på informationssäkerhet inte underordnade krav på risk- och sårbarhetsanalyser. Det kan därför vara vanskligt att inordna arbetet med informationssäkerhet som en del av risk- och sårbarhetsanalysen, om man inte fullt ut tar höjd för de informationssäkerhetskrav som finns lagreglerat.[103]

5.4 En modell för att minska leverantörsberoende

När det gäller åtgärder för att minska beroende gentemot kritiska tjänsteleverantörer i form av exempelvis monoberoenden är det lämpligt för myndigheten att arbeta stegvis utifrån en bedömning av hur starkt det aktuella beroendet är och hur pass kritisk den aktuella funktionen är för myndighetens beredskap.

Ju starkare beroende och ju mer kritisk leveransen är för myndigheten, desto fler steg och åtgärder bör myndigheten överväga och implementera för att öka sin kontroll över leverantörens tjänster och höja sin egen robusthet.[104]

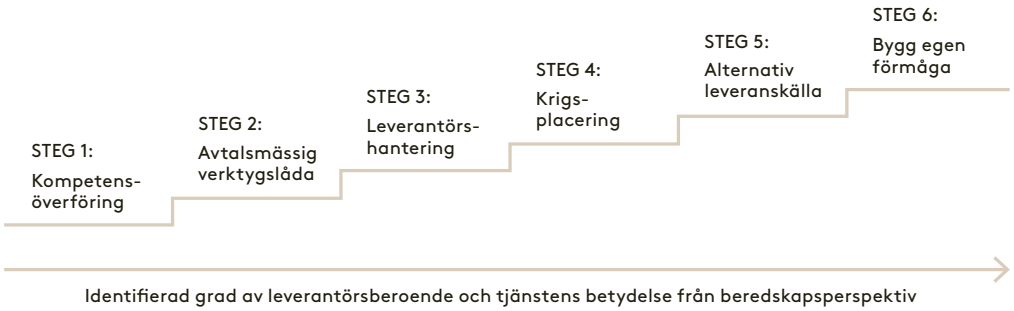
Med andra ord, en viss tjänsts betydelse för myndighetens förmåga att upprätthålla sin verksamhet i händelse av höjd beredskap bör vara dimensionerande för hur ingripande åtgärder som ska vidtas i förhållande till den aktuella tjänsteleveransen.

Vi har utifrån ovanstående principer tagit fram en stegvis modell för att minska leverantörsberoendet, se figur 5.5 nedan.

Pilen i modellen indikerar att myndighetens bedömning av graden av leverantörsberoende i kombination med tjänstens betydelse för verksamheten bör vara styrande för vilka åtgärder och hur många steg i modellen som myndigheten bör implementera.

103 För en mer fullständig bild över hur dessa lagreglerade krav ska samordnas hänvisas till vår tidigare rapport om juridisk informationssäkerhet och dess modell för samordnad juridisk informationssäkerhet, Kahn Pedersens skriftserie 2020:1, Juridisk informationssäkerhet, avsnitt 7.3

104 Se och jfr ”När kriget kom nära – årsrapport it-incidentrapportering 2022”, MSB, 2023, s. 22 f.



Figur 5.5: Vår modell för att minska leverantörsberoenden

Vi tror att ovanstående modell kan användas oavsett vilken typ av tjänst som myndigheten är beroende av, men som framgått ovan är vår erfarenhet att dylika leverantörsberoenden är särskilt vanligt förekommande just i relation till olika IT- och teknikleverantörer.

I det följande kommer vi att gå igenom respektive steg i vår modell.

5.4.1 Steg 1: Kompetensöverföring

Det inledande steget i modellen för minskat leverantörsberoende bygger på att myndigheten ökar sin kunskap och kompetens om de varor och tjänster som den aktuella leverantören tillhandahåller.

Relevant kunskap och kompetens kan naturligtvis erhållas på flera olika, och mer eller mindre ingripande, sätt till exempel genom rekrytering eller inkontraktering (se avsnitt 5.4.6 nedan). Sådana initiativ kräver omfattande investering från myndigheten.

Ett bättre inledande steg för de flesta myndigheter är därför att ta initiativ till så kallad kompetensöverföring från leverantören.

Det finns flera olika metoder att använda för kompetensöverföring. Det vanligaste är att leverantören helt enkelt tillhandahåller sedvanlig utbildning eller fortbildning till beställarorganisationen hos myndigheten.

En annan, mera omfattande åtgärd är att parterna kommer överens om så kallad ”skuggning”, som innebär att anställda från beställarens organisation under viss period skuggar leverantörens anställda för att lära sig arbetet (eller bara stärka beställarens förmåga att förstå och själv kunna utföra samma arbete).

Förfaranden med skuggning är förhållandevis vanliga vid utkontraktering av IT-drift när en avgående leverantör ska lämna över ansvaret för tjänsterna till en annan leverantör eller till beställaren. I andra situationer, till exempel vid byte av IT-system från en leverantör till en annan, kommer skuggning att vara mera kontroversiellt och känsligt för den avgående leverantören. Detta eftersom en stor del av den relevanta informationen och kompetensen potentiellt kommer att utgöra en del av själva IT-systemet och därmed leverantörens immateriella rättigheter eller företagshemligheter. Om man ska arbeta med denna typ av mer omfattande kompetensöverföring är det därför lämpligt att redan i upphandlingen och avtalet inkludera sådana krav och villkor (se vidare avsnitt 5.4.2 nedan).

Den kunskap och information som avslöjas och överförs från leverantör till beställare i samband med en kompetensöverföring är typiskt sett icke-offentlig och utgör ofta leverantörens affärshemligheter. Detta innebär att en eventuell sekretessklausul kan behöva anpassas och möjliggöra för effektiv kunskapsöverföring, exempelvis så att beställaren inte är alltför kringskuren vad gäller hur information från leverantören får användas av beställaren (till exempel att information kan behöva avslöjas för andra leverantörer till beställaren) och att beställaren inte är skyldig att återlämna eller radera sådan information vid avtalets upphörande.

5.4.2 Steg 2: Implementera den avtalsmässiga verktygslådan

För de leverantörsrelationer där det finns ett kritiskt beroende, vilket bedöms vara nödvändigt på kort och lång sikt och där det inte är tillräckligt med enbart kompetensöverföring, behöver myndigheten gå vidare och se till att den genom leverantörsavtalet har adekvat kontroll över den aktuella tjänsteleveransen.

Att tillförsäkra sig adekvat kontroll sker främst genom att myndigheten ser till att relevanta civilrättsliga åtaganden och rutiner har implementerats gentemot leverantören. Det finns ett stort antal avtalsbestämmelser som bör övervägas av myndigheten, och vi kommer i detta avsnitt att gå igenom vissa av dem.

De klausuler och mekanismer i avtalet som vi beskriver nedan kan ses som en slags verktygslåda för myndigheten för att skapa kontroll över den aktuella delen av verksamheten, trots att den utförs genom tjänsteleverans från extern part. Detta innebär inte att alla klausuler nedan är viktiga i alla avtal och för alla tjänsteleveranser. Syftet med detta avsnitt är istället att ge en översikt över de verktyg i avtalet som kan vara relevanta för en myndighet att implementera för att öka sin kontroll över tjänsteleveransen.

Figur 5.6: Klausuler i den avtalsmässiga verktygslådan

Avtalet är en viktig komponent för att åstadkomma kontroll i en leverantörsrelation eller implementera lösningar för en säker och kostnadseffektiv leverans av de tjänster till vilka myndigheten i inventeringsfasen har identifierat ett leverantörsberoende. Ett bra avtal börjar förstås med en väl genomtänkt och detaljerad kravställning och en noggrann upphandlingsprocess. Även om det i vissa fall kan vara möjligt att lägga till denna typ av avtalsbestämmelser i ett befintligt avtal, har myndigheten mycket att vinna på att avtalet innehåller relevanta klausuler från början.

Avtalets omfattning

Frågor om avtalets omfattning och ansvarsfördelningen mellan beställaren och leverantören tillhör de absolut vanligaste tvistefrågorna kopplat till avtal om IT-tjänster och IT-system. Ett vanligt problem är att det uppstår, eller senare uppdagas, en diskrepans mellan å ena sidan myndighetens förväntansbild och kravställning och å andra sidan leverantörens förväntansbild och produkt- eller tjänstebeskrivningar. Det kan då bli en tolkningsfråga om vilket dokument som ska äga företräde.

Det finns olika sätt att reglera avtalets omfattning och frågan är så gott som alltid kopplad till vilken prismodell som tillämpas. Frågor om avtalets omfattning är sällan kontroversiella om leverantören får betalt på löpande räkning, medan detta blir helt centralt om och i den mån beställaren efterfrågar fast pris för ett visst åtagande. Den vanligaste utgångspunkten i ett avtal med fast pris är att leverantörens åtagande uttömmande beskrivs i avtalet och att allt arbete eller all funktionalitet som inte står i avtalet blir tillägg, utanför det överenskomna priset.

En annan utgångspunkt, som alltfler beställare av IT-system och digitala tjänster vill använda, är att istället uttömmande beskriva *beställarens* åtaganden och att det tvärtom är leverantören som ska svara för allt arbete och alla kostnader som inte angivits i avtalet. Denna typ av avtalskonstruktion är många gånger lämplig och önskvärd ur ett beställarperspektiv, men leder ofta till utdragna diskussioner och förhandlingar med leverantören.

I samband med utkontraktering av verksamhet eller processer kan det också vara vanligt med så kallade scope sweepers, det vill säga klausuler som innebär att leverantören ska svara för inte bara sådant arbete som står i avtalet utan även arbete som leverantören, utifrån sin erfarenhet från andra affärer och kunder, borde ha förstått att beställaren avsåg att leverantören skulle utföra eller bekosta. Även sådana klausuler leder ofta till omfattande förhandling med leverantören.

Ytterligare en metod som förekommer för att reglera avtalets omfattning är olika ansvarsmatriser, där parternas respektive åtaganden specificeras på detaljerad nivå. Det kan vara en bra metod, men det är viktigt att notera att utgångspunkten i sådana matriser typiskt sett är att kunden svarar för eventuella åtgärder som inte beskrivs i matrisen eller där det finns gråzoner kring ansvarsfördelning.

En öppen förhandling mellan beställare och leverantör kring ansvarsfördelning tvingar parterna att klargöra sina förväntansbilder. En sådan diskussion har ett egenvärde genom att den ofta kan förebygga framtida oenighet.

Det finns alltså många olika sätt att genom avtalet förebygga oenighet och tvister om avtalets omfattning. Denna fråga är mycket viktig ur ett beredskaps- och robusthetsperspektiv, eftersom det kan finnas möjlighet, beroende på avtalets innehåll och utformning, för leverantören att ställa in och stoppa sin prestation i en tvistesituation, till exempel om myndigheten håller inne sin betalning till leverantören. Det är en situation som naturligtvis inte får eller kan tillåtas inträffa, om myndigheten har ett kritiskt beroende till den aktuella leverantören.

Tolkningsföreträde

Tydlighet är självfallet viktigt inte bara vid beskrivningen av avtalets omfattning utan även för avtalet i övrigt. Även om avtalets bestämmelser har tänkts igenom noga är det i praktiken svårt att undanröja alla potentiella otydligheter och vissa motstridigheter är därför oundvikliga.

Därför bör myndighetens uppfattning ges företräde vid tolkningen av avtalet och en sådan regel också skrivas in i avtalet. Det är inte ovanligt att den ena partens uppfattning ges företräde i enskilda frågor, till exempel angående klassificeringen av incidenter i ett supportavtal, men för att gardera sig mot eventuella otydligheter i stort menar vi att en generell reglering om tolkningsföreträde ofta bör övervägas. Detta i synnerhet när det är fråga om avtal som rör tjänsteleveranser med högt leverantörsberoende. I sådana avtal bör det skrivas in att myndighetens skäliga uppfattning alltid ska ges företräde vid en tolkning av avtalet.

För att en klausul om tolkningsföreträde ska vara skälig krävs typiskt sett att den kombineras med olika slags begränsningar. Exempelvis är det vanligt att rättigheten begränsas till en tillfällig period, till exempel under tid som tvist eller oenighet föreligger, och att myndigheten åtar sig att erlägga ersättning till leverantören, inklusive ränta, om det senare slås fast att myndighetens tolkning var felaktig.

Flexibilitet

På samma sätt som en tydlig metod och reglering om avtalets omfattning är viktig, ska inte heller vikten av en flexibel och förutsebar mekanism för hantering av ändringar underskattas. En balanserad mekanism för hantering av ändringar i till exempel avtalets omfattning och prissättning ger myndigheten en nödvändig flexibilitet under avtalets löptid.

Frågan om ändringar kompliceras av det generella förbudet mot väsentliga ändringar av upphandlade avtal och sådana ändringshanteringsprocesser måste därför utformas och anpassas till de förutsättningarna, se vidare om detta i avsnitt 6.3 nedan.

En fråga som behöver övervägas särskilt är hur nya eller ändrade lagkrav under avtalstiden ska hanteras. Detta är särskilt relevant just i fråga om säkerhet och beredskap, eftersom nya och uppdaterade lagkrav regelbundet uppställs från lagstiftaren och andra normgivare. Det är vanligt att beställare i både offentlig sektor och i näringslivet uppställer strikta krav i upphandling och avtal på att leverantören alltid ska implementera och bekosta alla ändringar som krävs för att uppfylla sådana nya och ändrade lagkrav under avtalstiden.

Huruvida detta är rimligt, och huruvida en leverantör verkligen bör eller kan åta sig ett sådant ansvar, är ofta beroende av hur många av leverantörens kunder som påverkas av ett visst lagkrav. Om kravet exempelvis härrör från ny lagstiftning som påverkar alla eller många av leverantörens kunder, till exempel dataskydd, är det rimligt att leverantören ska bära denna risk och därmed utföra nödvändigt arbete och stå för alla eventuella merkostnader. Om kravet istället härrör från lagstiftning som bara påverkar en enskild kund, är det istället ofta rimligt att leverantören ges ersättning för sina merkostnader för att efterleva det nya eller ändrade lagkravet.

Vi ser att frågor om ändringshantering, och inte minst den kommersiella riskfördelningen för nya och ändrade krav under avtalstiden, blir allt vanligare i takt med att många verksamheter omfattas av fler och fler lag- och myndighetskrav. I en föränderlig värld är det naturligtvis avgörande för en upphandlande organisation att säkerställa en adekvat och skälig process och hantering av nya krav. Detta behöver också beskrivas tydligt och utförligt i avtalet, så att både kunder och leverantörer ges rätt förutsättningar och incitament att säkerställa regelefterlevnad.

Tidplan och hantering av försening

Om det finns implementeringsmoment i avtalet, såsom i projektavtal där leverantören ska leverera eller utveckla en lösning till myndigheten, är det viktigt att parterna kommer överens om en tydlig tidplan för projektets genomförande och att avtalet innehåller lämpliga mekanismer för att hantera leverantörens försening. Mekanismer som vite och så kallade step-in-rättigheter som ger beställaren en rätt att färdigställa projektet på leverantörens risk och bekostnad bör övervägas. Någon form av ekonomisk sanktion vid leverantörens försening bör alltid finnas med och för verksamhetskritiska leveranser med en pressad tidplan behöver beställaren även ges en step-in-rättighet.

Det bör dock nämnas att det finns många olika mekanismer, utöver förseningsviten och step-in-rättigheter, som kan användas för att säkerställa rätt beteende och incitament i ett projekt. Både betalningsplan kopplad till milstolpar i projektet och, kanske framförallt, utformningen av ersättningsmodell för den efterföljande drift- och förvaltningsfasen efter slutfört projekt kan vara minst lika effektiva som förseningsvite.

Avtalsuppföljning och samverkan

Avtalsuppföljning och en väl genomtänkt modell för samverkan under avtalstiden är avgörande för digital robusthet. Detta hänger nära samman med processer för leverantörshantering, se steg 3 i vår modell (avsnitt 5.4.3 nedan).

Immateriella rättigheter

Som framgått ovan spelar leverantörers ensamrätt till underliggande datorprogram en avgörande roll för myndighetens leverantörsberoende. Genom avtalet upplåter leverantören typiskt sett en nyttjanderätt och licens till myndigheten att få använda datorprogrammet på de villkor som uppställs i avtalet.

En central del i alla IT-avtal är därför avtalets bestämmelser om immateriella rättigheter. Särskilt viktig är omfattningen och utformningen av licensbestämmelsen i avtalet. För myndigheten är det viktigt att kunna förlita sig på att man kommer att kunna använda leverantörens lösning under en överskådlig tid, typiskt sett under avtalstiden men ibland även efter utgången av denna. I de fall då leverantören ska vidareutveckla eller anpassa den lösning som tillhandahålls, eller utveckla något nytt som är tänkt att tillfalla myndigheten, är det viktigt för myndigheten att överväga hur immateriella rättigheter till sådant resultat ska fördelas mellan parterna. Detta kan till exempel ske genom överlåtelse eller licensupplåtelse.

Andra aspekter som är viktiga att ha i åtanke vid utformandet och förhandlandet av en licens, förutom licensens omfattning i tid och vad det är som licensieras, är om licensen ska kunna återkallas, om den är global, eller om beställarens användningsrätt är begränsad till ett angivet territorium eller till särskilda delar av beställarens verksamhet. Det är också viktigt huruvida licensen är förenad med en särskild licensavgift.

Oavsett hur en licensbestämmelse är utformad är den till lite hjälp för myndigheten om leverantören inte längre har praktisk möjlighet att tillhandahålla lösningen, till exempel till följd av leverantörens konkurs eller att krig i Sverige eller i omvärlden medför hinder i leverantörens försörjningskedja. Ett sätt att gardera sig mot denna risk är att ingå ett separat avtal om källkodsdeponering med leverantören. Genom en deponering av källkoden hos en oberoende tredje part, exempelvis Stockholms Handelskammare, kan myndigheten säkra tillgång till leverantörens immateriella rättigheter även vid sådan händelse.

För att kunna möjliggöra fortsatt drift behöver myndigheten dock ha nödvändig kompetens, antingen inom den egna verksamheten eller i form av en alternativ leverantör som snabbt kan ta över tillhandahållandet av tjänsten. I dessa fall är det viktigt med en väl utformad exit-bestämmelse (se mer om detta nedan).

Omställningsfasen vid avtalets upphörande borde i de flesta fall vara kortare om leverantörens lösning bygger på öppen källkod. Det är dock svårt att dra några generella slutsatser i detta avseende, utan det beror helt och hållet på vad det är för typ av lösning som tillhandahålls och förekomsten av samt kompetensen hos potentiella andra leverantörer av liknande lösningar på marknaden.

Ett sätt att avtalsvägen underlätta överföreningen av kompetens från leverantören till beställaren är dels att inkludera processer för kompetensöverföring (se avsnitt 5.4.1), dels se till så att avtalet inte innehåller några så kallade non-solicitation-klausuler som förbjuder eller inskränker beställarens möjligheter att rekrytera personal från leverantören.

Särskilt om rätten att använda dokumentation

Alla former av IT-lösningar behöver beskrivas på olika nivåer av detaljering för att dessa lösningar ska kunna förvaltas och underhållas. Det kan vara alltifrån installationsanvisningar, systembeskrivningar, driftmanualer till slutanvändarhandledningar. Vilken slags dokumentation som en myndighet får ta del av är som regel beroende av lösningens karaktär och hur den säljs. Som regel kan sägas att en SaaS-tjänst åtföljs av dokumentation med fokus på slutanvändaren medan dokumentationen

för en licensierad mjukvara installerad i kundens IT-miljö istället kan bestå av systembeskrivningar eller driftmanualer.

Dokumentation är, precis som programkod, normalt ett upphovsrättsligt skyddat verk. En leverantör som erbjuder en lösning med dokumentation har sannolikt även ensamrätten till denna dokumentation. På samma sätt som att myndigheten behöver säkra upp att den har rätt att använda själva lösningen under överskådlig framtid, behöver myndigheten även försäkra sig om att ha tillgång till och rätt att använda nödvändig dokumentation till lösningen, inklusive att framställa nya kopior efter behov.

I vissa fall kan det finnas behov för myndigheten att under en övergångsperiod kunna fortsätta använda just dokumentationen även efter att lösningen slutat nyttjas, exempelvis i syfte att säkerställa en ordnad övergång till ny leverantör eller lösning.

Beroende på lösningens karaktär och komplexitet kan detta vara lika centralt som att säkra tillgång till lösningens källkod. Om myndigheten planerar för ett framtida scenario där man själv, eller en tredje part på konsultbasis, förvaltar och vidareutvecklar lösningen behöver man även säkerställa att man har rätt att ändra i dokumentationen när lösningen utvecklas.

Hantering av konfidentiell information

En närliggande fråga är hur en offentlig beställare ska kunna uppnå skydd för både sin konfidentiella information och kanske framförallt vad beställaren får göra med leverantörens konfidentiella information. Det är till exempel viktigt att se till så att avtalet inte innehåller bestämmelser som ålägger myndigheten att lämna tillbaka all leverantörens konfidentiella information vid avtalets upphörande, om sådan information omfattar för myndigheten viktig know-how.

En sådan bestämmelse är väldigt vanlig i de flesta avtal och tjänar, om den är ömsesidig, till att skydda beställaren lika mycket som leverantören. Om myndigheten ska fortsätta använda systemet efter avtalets upphörande, är det dock viktigt att se till att en sådan bestämmelse inte omfattar till exempel instruktioner till beställaren om hur lösningen fungerar eller hur den bör underhållas. Avtalsbestämmelser som säkrar kompetensöverföring till beställaren under avtalstiden blir annars verkningslösa om all sådan information måste återlämnas vid avtalets slut.

Skiljelinjen mellan av beställaren förvärvad kompetens och leverantörens konfidentiella information i övrigt är dock svår att dra i praktiken. Ett sätt att undanröja eventuella oklarheter i denna del är att uttryckligen specificera den typ av information som ska kvarbli hos beställaren vid avtalets upphörande. En sådan lista ska dock inte göras uttömmande.

Det är viktigt att uppmärksamma att *data* inte anses kunna vara föremål för äganderätt enligt svensk rätt och som utgångspunkt inte träffas av tillämplig lagstiftning om immateriella rättigheter. Det är dock möjligt att avtalsvägen reglera rätten till data, vilket är ett annat skäl till att sekretessklausulen måste utformas med stor omsorg för att skapa rätt kontroll och minska leverantörsberoendet.

Planering inför avtalets upphörande

Den avtalsreglering som kanske tydligast hänger samman med att minska leverantörsberoendet, ytterst genom återtagande av verksamhet genom inkontraktering, är klausuler för avveckling av avtalet och samarbetet vid avtalets upphörande, så kallad exit.

En god exit-planering bör påbörjas redan vid kravställning och inför en planerad upphandling av en leverantör som bedöms medföra ett leverantörsberoende. Om sådana krav och förberedelser inte inkluderats i det ursprungliga avtalet, utan myndigheten istället önskar tillföra dylika bestämmelser under löpande avtalstid, eller ännu värre i samband med själva avvecklingen, kommer dessa frågor vara betydligt mer svårförhandlade.

Avtalets exit-regleringar bör innehålla åtminstone de bestämmelser och åtaganden som anges i avsnitt 5.4.6. En särskilt viktig aspekt att fånga upp i detta sammanhang är hur återlämningen av kundens data och konfidentiella information ska hanteras i samband med avtalets upphörande. Som vi har varit inne på ovan är det viktigt att myndigheten tillåts behålla sådan data och information som är viktig för den fortsatta användningen av lösningen.

Avtalstid

Även regleringen om avtalstid kan användas som ett sätt att säkra kontinuitet under avtalets löptid. Avtalstiden bör vara noga genomtänkt för att täcka myndighetens behov under en överskådlig tid, och även innehålla lämpliga förlängningssituationer. Det kan exempelvis vara lämpligt att inkludera särskild reglering som automatiskt förlänger avtalstiden vid händelse av regeringsbeslut om höjd beredskap.

Det är också viktigt att noga överväga leverantörens möjligheter att säga upp avtalet i förtid. Alltför generösa uppsägningsmöjligheter minskar naturligtvis avtalets tillförlitlighet och robusthet, medan alltför strikta och begränsade uppsägningsmöjligheter kan påverka såväl anbudsgivarens benägenhet att lämna anbud som leda till onödiga riskpremier i prisvillkoren. Det finns en risk att alltför begränsade uppsägningsmöjligheter för leverantören kan anses oskäliga vid en eventuell domstolsprövning.

På liknande sätt som beskrivs ovan om leverantörens stoppningsrätt vid tvist eller oenighet, bör myndigheten också se upp för regleringar som ger leverantören rätt att ta sig ur avtalet vid exempelvis myndighetens bristande betalning, till exempel innehållen betalning av tvistig faktura.

Servicenivåer (SLA) och incitament

Att mäta och följa upp kvaliteten i en komplex tjänsteleverans är alltid viktigt. I avtal där det finns ett högt leverantörsberoende är det sannolikt ännu viktigare. Sådan kvalitetsmätning och uppföljning görs typiskt sett i form av ett så kallat Service Level Agreement (SLA) som innehåller både mätpunkter, ibland kallat KPI:er, avtalade nivåer och konsekvenser av om nivåerna inte nås.

Att utforma ett ändamålsenligt SLA är bland de viktigaste avtalsmässiga åtgärderna som en beställare bör vidta för att upprätthålla kontroll över sina viktiga leverantörer. Även om detta är ett område som inte är direkt lagreglerat och där det finns utrymme för kreativitet hos myndigheten, är det också viktigt att inse att många leverantörer och branscher tillämpar standardiserade mätpunkter och metoder för att mäta kvalitet i leveransen. Om man som myndighet vill införa andra eller innovativa mätpunkter i ett SLA så kan det leda till både omfattande förhandling och eventuellt prispåslag, vilket dock kan vara rimligt för båda parter, beroende på avtalstyp och leveransobjekt.

Beroende på vilken typ av tjänst som avses, är vanliga mätpunkter i SLA för IT-tjänster tillgänglighet, svarstid, åtgärdstid, återställningstid och inställelsetid.

När det gäller konsekvenser av att leverantören misslyckats med att nå avtalade nivåer i ett SLA, är det vanligaste att det finns uttryckliga viten eller förutbestämda prisavdrag i avtalet. Många gånger kan även andra konsekvenser, såsom åtgärdsplaner, vara minst lika viktiga från ett beställarperspektiv. Vår erfarenhet är dock att ekonomiska påföljder och konsekvenser, såsom viten och prisavdrag, är mest effektiva för att påverka leverantörens beteende och leveranskvalitet.

Avslutningsvis kan nämnas att det kan övervägas att kombinera ekonomiska påföljder i ett SLA med incitament för leverantören att leverera på en högre nivå än den avtalade nivån. Sådana incitament kan vara ett sätt för en myndighet att öka chanserna för att leverantören prioriterar sin leverans till myndigheten, vilket förstås påverkar även tillförlitlighet och robusthet i leveransen på ett positivt sätt.

Påföljdsmekanismer

Liksom olika typer av incitamentsmodeller kan vara ett sätt att styra leverantörens beteende, kan en väl genomtänkt påföljdskatalog vara ett sätt att avskräcka leverantören från att bryta mot avtalet. Syftet är att uttryckligen reglera de faktiska konsekvenserna av ett avtalsbrott och specificera vilka påföljder som ska vara tillgängliga för beställaren.

När en påföljdskatalog formuleras är det viktigt att komma ihåg att svensk civilrätt innehåller omfattande bakgrundsrätt om påföljder, det vill säga det kan i vissa fall vara förmånligt för en myndighet och beställare att *inte* uttryckligen reglera en viss påföljd i avtalet utan istället förlita sig på bakgrundsrätten.

De vanligaste påföljderna att överväga i ett civilrättsligt avtal är sannolikt fullgörelse, vite, skadestånd och uppsägning. Det kan också finnas skäl att kunna begära till exempel prisavdrag eller påkalla step-in-rättighet. Det kan dessutom vara lämpligt att uttryckligen reglera rätten för beställaren att hålla inne betalningen vid leverantörens avtalsbrott.

En vanlig förhandlingsfråga är om de påföljder som uttryckligen nämns i avtalet ska vara *exklusiva* eller om beställaren ska kunna påkalla även andra påföljder, till exempel skadestånd eller uppsägning. I denna fråga har olika praxis utvecklats i olika branscher och på olika marknader. Vår erfarenhet är att påföljder normalt är icke-exklusiva i

många IT-avtal, särskilt med svenska leverantörer, medan det motsatta gäller för systemleveranser i industrin och även i relation till utländska IT-leverantörer.

Force majeure

Avtalsbestämmelser om force majeure tar sikte på situationer där en händelse utanför en avtalsparts kontroll medför att denne förhindras att fullgöra sina avtalsförpliktelser. En force majeure-klausul kan innebära att den förhindrade parten befrias från att fullgöra sin avtalsförpliktelse, åtminstone under den tid som force majeure består, eller att den förhindrade parten befrias från eventuellt skadeståndsansvar till följd av avtalsbrott. Regler om force majeure är vanligt förekommande i IT-leveransavtal. I dessa avtal befriar force majeure vanligtvis den förhindrade parten från att fullgöra sina avtalsförpliktelser. Force majeure förekommer även i svensk och utländsk rätt, men då oftast i form av bestämmelser som undantar en avtalsbrytande part från skadeståndsansvar för en skada som ligger utanför partens kontroll.[105]

Varken lagstiftaren eller Högsta domstolen har gett någon närmare vägledning om vilken status eller funktion som force majeure ska anses ha i svensk rätt. Det är exempelvis oklart om force majeure kan åberopas trots avsaknad av en uttrycklig avtalsreglering eller om det är möjligt att avtala om att force majeure aldrig ska vara en befrielsegrund.

Vår uppfattning är dock att den rimligaste och mest närliggande utgångspunkten är att det råder avtalsfrihet i fråga om force majeure som befrielsegrund. En annan sak är att force majeure kan vara en rättsregel i bakgrundsrätten och därmed ha en utfyllande funktion i avtal som saknar bestämmelser om ansvar för avtalsbrott på grund av händelser utanför den avtalsbrytande partens kontroll.

Med detta sagt ser vi en risk för att det skulle kunna anses oskäligt att en avtalspart som förhindras att fullgöra en avtalsförpliktelse på grund av händelser utanför partens kontroll ändå ska hållas ansvarig. En sådan bestämmelse skulle stå i motsats till (dispositiv) lagstiftning, vanligt förekommande standardavtal och sedvänja på marknaden, och eventuella allmänna avtalsrättsliga principer om force majeure och/eller kontrollansvar. I en sådan situation kan bestämmelsen alltså bli föremål för jämkning, eller lämnas utan avseende, enligt 36 § Avtalslagen (1915:218).

Det går inte att säga att det alltid är skäligt att avtala om att force majeure-händelser inte ska ha befriande verkan, men inte heller att det alltid vore oskäligt. Detta skapar en påtaglig osäkerhet i att ”tvinga” en leverantör att prestera också i händelse av force majeure, men ger samtidigt en möjlighet att utforma avtalsvillkor och omständigheterna vid avtalets ingående på ett sådant sätt att det ändå kan anses skäligt att upprätthålla också mycket betungande avtalsvillkor.

Vi menar att det går att mitigera de omständigheter och argument som en leverantör sannolikt skulle göra gällande för att få ett avtalsvillkor

105 Se t.ex. 27 § köplagen (1990:931). För en mer utförlig genomgång, se Axhamn, J., Nyström, B. & Svensson, O. (red.), Ändrade förhållanden (2022, version 1, JUNO), s. 92 ff. Därtill förekommer force majeure i olika internationella regelverk, såsom Unidroit.

som begränsar möjligheten att åberopa force majeure jämkat. Sådana överväganden bör göras utifrån de aspekter som vanligtvis tillmäts betydelse vid bedömningen av ett avtalsvillkors (o)skälighet.

› **Pris**.[106] Det är ytterst leverantören som avgör sitt anbudspris. Upphandlande organisationer har, av upphandlingsrättsliga skäl, mycket svårt att styra leverantörers prissättning, särskilt i fråga om hur låga priser leverantören får lämna.[107] Det finns däremot inga hinder mot att uppmana leverantören att ta höjd för denna avtalsmässiga risk vid beräkningen av prissättningen.

  Ett alternativ är att leverantören ges en rätt till ytterligare ersättning i händelse av att den måste prestera under force majeure, antingen som en på förhand bestämd summa eller som en funktion av avtalets eller avtalsprestationens värde.[108]

› **Tidsmässig möjlighet att överväga avtalet**.[109] Upphandlande organisationers avtalstecknande föregås vanligen av ett annonserat förfarande enligt upphandlingslagarna. Redan av denna anledning kommer leverantören att ha god tid på sig att granska avtalet i dess helhet, ställa frågor inom ramen för ”Frågor och svar” och överväga betydelsen av att inte ha möjlighet att åberopa force majeure som befrielsegrund.[110]

› **Transparens (både i utformning och placering)**[111] **samt medvetet risktagande**[112]. Genom att särskilt framhålla avtalsbestämmelsens existens och funktion, och i övrigt utforma den på ett förståeligt sätt, blir det tydligt för leverantören att den inte kommer att kunna åberopa vissa former av force majeure som befrielsegrund. Leverantören kan även uppmanas att särskilt beakta bestämmelsen innan den beslutar sig för att lämna anbud eller vid beräkningen av sitt anbudspris. På detta sätt blir leverantören medveten om det risktagande som det innebär att lämna anbud och sedermera teckna det aktuella avtalet, och ges därmed möjlighet att prissätta denna risk.

---

106 Se prop. 1975/76:81, s. 119 samt SOU 1974:83, s. 152 f.

107 HFD 2018 ref. 50, HFD 2020 ref. 24 och HFD 2022 ref. 41.

108 Se prop. 1975/76:81, s. 127, där föredraganden uttalar följande: Har parterna räknat med möjligheten att förhållandena ändras och kommit överens om vem av dem som skall stå för risken för oförutsedda händelser, är det som regel inte påkallat att jämka avtalet när sådana händelser inträffar, särskilt om den part som har tagit på sig ansvaret har kompenserats härför genom andra avtalsvillkor som är till hans fördel.

109 Se NJA 1982 s. 613.

110 Se 11 kap. LOU respektive LUF samt 9 kap. LUFS.

111 Se NJA 1997 s. 524. Se även Ramberg, J. & Ramberg, C, Allmän avtalsrätt (2019, version 11, JUNO), s. 220 med vidare hänvisningar.

112 Se NJA 1979 s. 483 samt prop. 1975/76:81, s. 119. Se även Munukka, J., Lag (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område 36 §, underrubrik 3.3.5, Lexino 2020-08-28, samt Grönfors, K. & Dotevall, R., Avtalslagen (2018-09-11, version 5A, JUNO), kommentaren till 36 § i avsnittet 27.

› **Ensidig bestämmanderätt.**[113] Detta tar främst sikte på situationer där den ena parten ensidigt kan försätta motparten i ett slags ”limbo”, exempelvis i form av ”*force-majeure-klausuler som tillåter den ena parten att vid force-majeure under en längre tid bestämma om han vill stå kvar vid avtalet eller häva det, samtidigt som den andra parten är bunden att avvakta hans beslut*”.[114] Det är emellertid inte detsamma som att avsaknaden av en force majeure-klausul är mer betungande för den ena parten, det avgörande synes vara att leverantören inte behöver avvakta den upphandlande organisationens beslut. Att avtala bort force majeure ger motsatt effekt, nämligen att parternas avtalsenliga förpliktelser gäller oavsett eventuella omständigheter utanför parternas kontroll.

› **Parternas styrkeförhållande.**[115] Det ligger i upphandlingsrättens natur att den upphandlande organisationen är förhindrad att endast teckna avtal med leverantörer av viss storlek eller med viss organisatorisk eller juridisk styrka, i fråga om exempelvis möjlighet att kritiskt granska avtal. I vissa fall, särskilt i större upphandlingar, kan det i någon mån bli självreglerande att endast ”jämbördiga” leverantörer deltar till följd av högt ställda kvalificeringskrav.

  Å andra sidan kan även objektivt sett jämbördiga motparter vara i ett underläge på grund av det upphandlingsrättsliga regelverkets särart. Möjligheterna att påverka avtalets innehåll är typiskt sett små och leverantörer hänvisas vanligtvis till ”Frågor och svar” för att ge eventuella synpunkter på eller förslag till ändringar av avtalsvillkor.

  Genom att i större utsträckning tillämpa förhandlade förfaranden där möjligheten till förhandling tillvaratas bör denna risk kunna minska. Det kan dock förekomma avtal med ett mindre avtalsvärde, men där det ändå är nödvändigt att avtala bort force majeure. I dessa fall är risken för att parternas styrkeförhållande inverkar på (o) skälighetsbedömningen ofrånkomlig, varför det uppstår ett särskilt behov av mitigerande åtgärder i övrigt.

› **Force majeurebegränsningens omfattning.** Slutligen påverkar det sannolikt en skälighetsbedömning huruvida en begränsning av leverantörens möjlighet att åberopa force majeure är onödigt långtgående. Om syftet med force majeurebegränsningen är att säkerställa leverans även vid höjd beredskap kan det finnas skäl att tydliggöra att andra force majeuregrunder såsom exempelvis strejk eller naturkatastrofer fortfarande kan ha en befriande verkan. På detta sätt tydliggörs att begränsningen är välavvägd och anpassad till myndighetens behov inom ramen för det aktuella avtalet.

---

113 Se prop. 1975/76:81, s. 118. Se även Munukka, J., Lag (1915:218) om avtal och andra rättshandlingar på förmögenhetsrättens område 36 §, underrubrik 3.3.5, Lexino 2020-08-28, och däri angivna rättsfall, samt Grönfors, K. & Dotevall, R., Avtalslagen (2018-09-11, version 5A, JUNO), kommentaren till 36 § i avsnittet 10.

114 Prop. 1975/76:81, s. 118.

115 Prop. 1975/76:81, s. 105 och106. Se även bl.a. NJA 1988 s. 230, NJA 1992 s. 290, NJA 1992 s. 782, NJA 2009 s. 408 samt SOU 1974:83, s. 28.

Detta minskar risken för att bestämmelsen skulle anses oskälig, den är inte mer betungande än vad som är absolut nödvändigt.

Vid utformning av Force Majeure-bestämmelser finns det två huvudsakliga skolor, den ena exemplifierar vad som kan utgöra en Force Majeure-händelse medan den andra uttömmande räknar upp dessa händelser. En uttömmande uppräkning är ofta till en beställares fördel men vår bedömning är att det föreligger avsevärt högre risk för jämkning av ett upphandlat avtal vid en uttömmande än vid en exemplifierande uppräkning.

Revisionsmöjligheter

Slutligen bör myndigheten ha rätt att kontrollera att leverantören efterlever avtalet. Detta åstadkoms normalt genom att myndigheten ges en rätt att genomföra regelbundna inspektioner av leverantörens verksamhet. Dessa bestämmelser kan utformas på olika sätt men bör alltid innefatta en rätt för beställaren att kontrollera leverantörens uppfyllelse av lagkrav och myndighetens interna riktlinjer. Dessa klausuler bör synkroniseras med myndighetens generella arbete med leverantörshantering och avtalsuppföljning, se avsnitt 5.4.3.

Sammanfattning

Som framgått ovan finns många olika verktyg i avtalet att använda för en myndighet som vill minska sitt leverantörsberoende. Ett bra och väl genomtänkt avtal är därmed ett viktigt steg på vägen mot ett leverantörsoberoende.

Från ett beredskapsperspektiv är det dock, utöver implementationen av ovanstående verktyg, också viktigt att överväga konsekvenserna av om leverantören inte klarar av att, eller inte vill, uppfylla sina avtalsförpliktelser. En sista utväg i alla avtal är att få saken prövad i domstol eller skiljenämnd, men en rättsprocess kan ibland vara en klen tröst för en beställare som är beroende av lösningen eller tjänsten.

En process kan nämligen dra ut på tiden och vissa fall kan det även, beroende på i vilket land leverantören har sitt säte, vara svårt att få domen verkställd. Att få rätt i sak är alltså förvisso viktigt men det viktigaste för en offentlig beställare, och då särskilt en offentlig beställare som står i ett starkt beroendeförhållande till leverantören, är trots allt att få lösningen eller tjänsten levererad.

Ett bra avtal är alltså nödvändigt, men inte tillräckligt, för att minska leverantörsberoendet. Det är därför viktigt att även beakta andra, mer praktiska, aspekter än vad som framgår av parternas avtal. Sådana åtgärder beskrivs närmare i de efterföljande stegen i vår modell för att minska leverantörsberoendet.

5.4.3 Steg 3: Implementera processer för leverantörshantering

Leverantörshantering eller leverantörsstyrning är ett samlingsbegrepp för processer och arbetsrutiner för att på ett strukturerat och enhetligt sätt samverka, mäta och följa upp en leverantörs avtalsprestation. Med andra ord är det fråga om en utvecklad form av avtalsuppföljning, där de primära syftena och drivkrafterna från beställarens sida generellt anses vara förbättrad kostnadskontroll och ökad kvalitetssäkring avseende leverantörens prestation. Uppföljning av SLA är normalt ett viktigt inslag i processer för leverantörshantering.

Det finns både direkta och indirekta fördelar från ett beredskapsperspektiv med att systematiskt följa upp sina leverantörer genom en etablerad metod för leverantörshantering. En strukturerad och systematisk process förutsätter och ställer nämligen krav på:

› Ett väl utvecklat avtal, där parterna exempelvis enats om samverkansformer, mätpunkter, kvalitetsnivåer och konsekvenser av avvikelser från sådana nivåer.

› En nära och regelbunden kontakt mellan beställaren och leverantören under hela avtalstiden.

› Att beställarens kunskap och kompetens om leverantörens varor och tjänster, och sannolikt den aktuella marknaden, stärks, vilket över tid kan innebära en ökad grad av kontroll och egen förmåga hos beställaren.

Det finns många olika modeller och processer för att arbeta med leverantörshantering och någon enhetlig standard har inte etablerats varken i offentlig förvaltning eller inom näringslivet. Behovet av en sådan standard har dock framförts vid olika tidpunkter, exempelvis av branschföreningar inom teknikområdet.[116]

Det viktiga i detta sammanhang är inte valet av modell eller metod för leverantörshantering, utan att understryka vikten av att faktiskt arbeta på detta sätt med alla kritiska tjänsteleverantörer. Vi menar att en välutvecklad modell för leverantörshantering och tillhörande strukturerade processer är nödvändiga för att hantera, värdera och ytterst begränsa myndighetens beroende av kritiska leverantörer. Det innebär i förlängningen att ett sådant arbetssätt också är viktigt för myndighetens möjligheter att kunna upprätthålla god beredskap och förberedelse inför ett förändrat omvärldsläge.

Kort sagt, strukturerad och systematisk leverantörshantering är en av flera förutsättningar för en robust digital transformation.

116 Se t.ex. rapporten ”Leverantörer av samhällsnytta – en analys av IT-och telekombranschen och den offentliga marknaden” utgiven av IT- och telekomföretagen inom Almega (numera Tech Sverige) i september 2020.

5.4.4 Steg 4: Krigsplacering

Även om avtal och samverkansprocesser är effektiva sätt för en myndighet att minska sitt leverantörsberoende, är det som ovan nämnts inte alltid tillräckliga lösningar. Steg 4 och framåt i vår modell för minskat leverantörsberoende bygger därför på åtgärder som myndigheten kan vidta utan vare sig avtalsstöd eller medverkan från leverantören.

En robust samhällsviktig verksamhet kräver bland annat att den personal som är nödvändig för utförandet av verksamheten är tillgänglig under höjd beredskap. Detta kan säkerställas genom att sådan personal krigsplaceras.

Krigsplacering sker genom att personal som är nödvändig för upprätthållande av en totalförsvarsviktig verksamhet anmäls till Plikt- och prövningsverket. Genom en sådan anmälan kan den aktuella personalen förklaras vara tagen i anspråk vilket kan motverka intressekonflikter och dubbelplacering om den aktuella personen är eller i framtiden skulle bli tagen i anspråk av någon annan totalförsvarsverksamhet.

Det finns inget principiellt hinder mot att krigsplacera personal som arbetar hos en privat leverantör till en myndighet. För att detta ska vara möjligt måste dock en anmälan till Plikt- och prövningsverket göras av leverantören. Denne måste i sin tur bli ålagd en skyldighet att göra en sådan anmälan för personal som är nödvändig för totalförsvaret, exempelvis genom det avtal som leverantören har med den aktuella myndigheten.

Många IT-tjänster tillhandahålls med resurser i form av till exempel fysisk infrastruktur eller anställda specialister som är placerade hos leverantören, till exempel i ett datacenter eller i en global supportfunktion. Dessa funktioner är ofta placerade utanför Sveriges gränser varför krigsplacering inte framstår som ett gångbart alternativ om inte detta kompletteras med ytterligare åtaganden, exempelvis avseende viss personals geografiska placering, säkerställande av källkodsåtkomst och förbud mot ”remote”-access.

5.4.5 Steg 5: Alternativ leveranskälla

Som ovan framgått handlar de inledande stegen i vår modell om åtgärder som baseras på civilrättsliga åtaganden och leverantörens aktiva deltagande.

Ett av skälen till att de senare stegen i vår modell är, och behöver vara, frikopplade från avtalet och från leverantörens aktiva deltagande, är att det finns flera situationer när det kan vara otillräckligt ur ett beredskapsperspektiv att enbart förlita sig på civilrättsliga åtaganden i relation till en kritisk leverantörsrelation.

Exempel på sådana omständigheter och situationer kan vara:

› När leverantören eller dess moderbolag lyder under utländsk jurisdiktion, samt

› när leverantören har andra, avsevärt större kunder än myndigheten och i synnerhet om sådana kunder kan förväntas ha hårdare ekonomiska sanktioner i sina avtal.

I båda dessa situationer utgör avtalade rättigheter och skyldigheter nödvändiga, men inte tillräckliga, åtgärder för att säkerställa en robust digital transformation. Det går nämligen inte att utesluta möjligheten att en sådan leverantör medvetet kommer att välja, mer eller mindre tydligt för beställaren, att prioritera ned avtalsenlig leverans till myndigheten.

Om och i den utsträckning leverantören har mer att förlora, kommersiellt eller strategiskt, på att leverera till myndigheten, finns åtminstone en risk för att leverantören de facto inte kommer uppfylla sina åtaganden. En sådan inställning kan kläs i andra ord och med juridisk argumentation från leverantören, såsom att force majeure eller ”omöjlighet” att leverera föreligger på grund av ny lagstiftning i utländsk jurisdiktion.

Oaktat den rättsliga argumentationen så är resultatet detsamma från myndighetens perspektiv: den för myndigheten nödvändiga tjänsteleveransen uteblir på grund av ett ensidigt agerande från leverantören. Detta ensidiga agerande kan mycket väl utgöra avsiktligt avtalsbrott från leverantören och föranleda rättsliga åtgärder från myndigheten. Detta påverkar dock inte den centrala frågan: hur säkerställer myndigheten fortsatt verksamhet även i ett sådant scenario?

Eftersom digital transformation ofta är tätt sammankopplad med ett ökat tjänste- eller leverantörsberoende, menar vi att en robust syn på digital transformation även kräver att myndigheten beaktar risken för att leverantören inte uppfyller sina avtalade åtaganden. Kort sagt, robust digital transformation innebär att myndigheten också måste förbereda sig på att hantera ett scenario där leveransen från en kritisk tjänsteleverantör uteblir.

Vi menar därför att myndigheten så långt som möjligt behöver ha både beredskap och förmåga att fullgöra sitt uppdrag även utan leverans från kritiska leverantörer. Det innebär att det i vissa fall kan vara relevant och nödvändigt för myndigheten att säkerställa en alternativ leveranskälla (steg 5) eller till och med bygga egen förmåga (steg 6).

För tjänsteleveranser där det finns en fungerande marknad med flera konkurrerande leverantörer är upphandlad beredskap en åtgärd som bör övervägas som ett sätt att säkra alternativa leveranskällor, se vidare avsnitt 6.2 nedan om upphandlad beredskap.

För tjänsteleveranser där det inte finns någon alternativ leverantör, till exempel på grund av att myndigheten är beroende av tjänster som bara kan utföras av en enda leverantör eller som är tätt sammankopplade till en ensamrätt som endast en leverantör innehar, så krävs andra åtgärder.

Det kan då vara fråga om att myndigheten kan behöva en eller flera av följande åtgärder, beroende på vari det aktuella leverantörsberoendet ligger:

› ”Skapa” en relevant marknad inför en framtida upphandling som ska kunna leda till högre grad av robusthet, till exempel genom att:

  – Ersätta befintliga digitala tjänster eller system med andra lösningar eller system baserat på öppen mjukvara, eller

  – Tillsammans med andra svenska kunder ställa krav på en lokal support- och serviceorganisation som levereras med svenska resurser.

› Säkerställa självständig tillgång till det material till vilket leverantören har en ensamrätt, till exempel genom licens eller källkodsdeponering.

5.4.6 Steg 6: Bygg egen förmåga

Det sjätte och sista steget i vår modell för minskat leverantörsberoende är att myndigheten helt enkelt avlägsnar sitt beroende genom att bygga egen förmåga att utföra de aktuella tjänsterna i egen regi. Vi vill understryka att detta naturligtvis inte är möjligt och knappast heller lämpligt för alla typer av leverantörsberoenden. För vissa IT-tjänster, till exempel förvaltningstjänster av proprietära IT-system där det inte bedöms önskvärt att byta system, kommer det sannolikt inte vara möjligt att helt avlägsna leverantörsberoendet. För andra tjänster med högt leverantörsberoende, till exempel utkontrakterad IT-drift är det istället fullt möjligt för en myndighet att bygga en egen förmåga, om myndigheten bedömer det nödvändigt och lämpligt.

I praktiken är det svårt och tidskrävande för en myndighet att bygga egen kompetens för att ersätta en befintlig leverantör till vilken myndigheten har ett starkt leverantörsberoende. Det tar ofta lång tid och medför stora kostnader för myndigheten att bygga upp tillräcklig egen kompetens, infrastruktur och förmåga att kunna driva en tidigare utlagd verksamhet i egen regi. Generellt är det nog så, att ju länge en verksamhet eller process varit utkontrakterad till en tjänsteleverantör, desto svårare är det i regel för myndigheten att själv ta över denna.

Det kanske vanligaste sättet att bygga egen förmåga är att ta över verksamheten från den befintliga leverantören. I sådana sammanhang talar man normalt om inkontraktering eller *insourcing*. För att genomföra en inkontraktering krävs normalt utförliga och omfattande förberedelser och investeringar från myndigheten.

För inkontraktering krävs också noggrann och omfattande avtalsreglering med den leverantör som tidigare har utfört den aktuella verksamheten eller processen åt myndigheten. Detta görs vanligtvis genom att olika bestämmelser från verktygslådan (se avsnitt 5.4.2 ovan) implementeras redan i utkontrakteringsavtalet. I detta sammanhang kan särskilt nämnas exit-klausulerna, som åtminstone bör innehålla:

- Åtagande för leverantören att underlätta och stötta inkontraktering, typiskt sett genom konsulttjänster, för vilka leverantören får extra betalt.
- Åtagande för leverantören att genomföra utbildningar och insatser för kompetensöverföring till myndigheten.
- En detaljerad planering för hur den utkontrakterade verksamheten ska kunna återföras till myndigheten.
- Överlämnande av relevant data, dokumentation, källkod, material och sådana produkter som krävs för att bedriva den utkontrakterade verksamheten i egen regi.
- Destruktion av myndighetens material på lämpligt sätt.
- Ekonomisk konsekvens, till exempel vite, för leverantören om denne försenar eller försvårar inkontraktering.

Utöver ovanstående avtalsbestämmelser, krävs också noggrann utformning av avtalsklausuler avseende sekretess och immateriella rättigheter för att kunna genomföra en inkontraktering på ett ordnat och kontrollerat sätt.

Avslutningsvis kan nämnas att ett alternativ till inkontraktering för drift i egen regi, och som sannolikt ökar myndighetens stabilitet och robusthet i samma utsträckning som inkontraktering, är samordnad statlig drift, det vill säga att en myndighet utför en viss verksamhet eller process som en tjänst till många andra myndigheter. Ett exempel på detta är Statens servicecenter, som tillhandahåller lönehantering, HR och ekonomi till andra myndigheter. Samordnad drift har också diskuterats mycket rörande IT-drift, där Försäkringskassan och vissa andra myndigheter numera har i uppdrag att tillhandahålla sådana tjänster till andra myndigheter.[117]

5.5 Sammanfattning

Sammanfattningsvis är det tydligt att robust digital transformation ställer mycket höga krav på den upphandlande organisationen. Det kräver omfattande resurser, kompetens och tid inte enbart för att kunna uppfylla tillämpliga lagkrav om säkerhetsskydd och beredskap utan också för att minska myndighetens kritiska leverantörsberoenden. Det kräver också omfattande avtalsarbete och leverantörsförhandlingar.

Vi har i detta avsnitt försökt beskriva hur en myndighet genom en sammanhållen process samtidigt och parallellt kan möta både lagkrav på myndigheten avseende säkerhet och beredskap och skapa bättre, hållbara och mera kontrollerade leverantörsrelationer. Om detta arbete görs sammanhållet är vi övertygade om att en sådan process kommer att stärka myndighetens digitala robusthet.

117 SOU 2021:97, s. 21 ff.

Det är ingen tvekan om att uppbyggnaden av ett nytt civilt försvar och Sveriges uppvaknande i frågor om beredskap kan komma i konflikt med myndigheters pågående digitala transformation. Det krävs därför att regeringen klargör hur myndigheter ska prioritera mellan dessa båda målsättningar, samt att berörda tillsynsmyndigheter utfärdar mer vägledning och föreskrifter i dessa frågor.

Hos myndigheter ser vi också att det kommer att bli nödvändigt att på ledningsnivå etablera en strategi för hur myndigheten ska förhålla sig till olika verksamhetsrisker och potentiella sårbarheter utifrån ett beredskapsperspektiv och kopplat till digital transformation.

Det kan inte uteslutas att viss digital transformation måste saktas ned eller ta ett steg tillbaka för att myndigheten ska kunna säkerställa sitt uppdrag i händelse av krig eller höjd beredskap.

6. Upphandlad beredskap

6.1 Inledning

Upphandlingslagarna är förfarandelagar och innebär naturligtvis vissa begränsningar i hur myndigheter får ingå avtal med leverantörer.

Det som ofta förbises är dock att upphandlingslagarna även skapar möjligheter och ett betydande mått av handlingsfrihet för upphandlande organisationer, bland annat för att det finns särskilda förfaranden, krav, kriterier och avtalstyper, vilka i och för sig är reglerade men inte obligatoriska att använda. Normalt innebär dessa bestämmelser att en upphandlande organisation inte är tvungen att välja ett visst handlingsalternativ, men att om myndigheten ändå väljer alternativet måste det göras på det sätt som upphandlingslagarna föreskriver.

Exempelvis är en upphandlande organisation inte tvungen att upphandla ramavtal eller dynamiska inköpssystem för att tillgodose sina inköpsbehov, men om myndigheten ändå väljer att göra det måste det ske i enlighet med upphandlingslagarnas bestämmelser om ramavtal respektive dynamiska inköpssystem. Även då finns det emellertid oftast olika handlingsalternativ att välja inom ramen för de tillämpliga bestämmelserna.

Det finns också en lång rad olika ageranden och beslut vilka inte alls eller endast i begränsad omfattning regleras i upphandlingslagarna. Det gäller bland annat flera av de kommersiella ställningstaganden som en upphandlande organisation gör inför, under och efter en upphandling. Exempel på detta är genomförande av en behovsanalys, det vill säga vad som behöver anskaffas eller en analys av hur anskaffningen ska ske, exempelvis genom ny upphandling, genom avrop på befintligt ramavtal eller genom att bygga egen förmåga att tillgodose ett visst behov.

Man kan också tänka sig en analys av vilken kommersiell modell som ska tillämpas, exempelvis köp, hyra, leasing eller någon form av tjänsteleverans, och en analys av vilken typ av leverantörsrelation det handlar om, det vill säga om det handlar om en verksamhetskritisk leverans som kräver ett nära samarbete med leverantören och stort engagemang från den upphandlande organisationen eller om det är möjligt för myndigheten att överlåta mer av ansvaret till leverantören och istället ta en mer traditionell beställarroll.

Det faktum att upphandlingslagarna inte bara reglerar den upphandlande organisationens skyldigheter, utan även skapar möjligheter och att mycket av det som utgör kärnan i en affärstransaktion i stora delar inte alls omfattas av upphandlingslagarna, innebär sammantaget att en upphandlande organisation har ett betydande mått av handlingsfrihet.

Myndigheten kan med andra ord utforma sina upphandlingar på ett sätt som är kommersiellt väl avvägt för den enskilda affären och dess betydelse för myndighetens verksamhet. Att använda detta handlingsutrymme är förstås inte bara lämpligt, utan många gånger helt nödvändigt,

men blir ofta särskilt betydelsefullt i upphandlingar som helt eller delvis syftar till att stärka det civila försvarets beredskap.

Nedan följer några exempel på sådana vägval, beslut och ageranden från en upphandlande organisations sida, vilka innebär ett nyttjande av den handlingsfrihet som upphandlingslagarna ger, och som kan vara särskilt lämpliga att överväga i upphandlingar som avser eller berör civil beredskap.

Det bör understrykas att redogörelsen är exemplifierande. Vidare bör framhållas att alla åtgärder inte passar för alla typer av anskaffningar och att det därför är viktigt att i varje enskilt fall noga överväga både lämpligheten och lagligheten av de åtgärder som en upphandlande organisation önskar vidta för att tillgodose verksamhetens behov.

Nedan redogörs också för de särskilda regleringar som finns i upphandlingslagarna och som enligt vår mening möjliggör för upphandlande organisationer att ta särskilda beredskapshänsyn inom ramen för sitt upphandlingsförfarande.

Vår genomgång utgår ifrån de tre huvudsakliga upphandlingslagarna, det vill säga LOU, LUF och LUFS.

Av dessa tre lagar är det av naturliga skäl LUFS som erbjuder flest uttryckliga möjligheter att ta beredskapshänsyn inom ramen för ett upphandlingsförfarande. Vår bedömning är emellertid att det, utifrån de grundläggande principerna, är fullt möjligt att ta motsvarande hänsyn även enligt LOU och LUF, så länge det är motiverat med hänsyn till upphandlingsföremålet.

6.2 Upphandla fler leverantörer än vad som normalt krävs

Ett sätt att upphandla för civil beredskap, det vill säga att tillgodose behoven av leveranssäkerhet och redundans i avtal som ska försörja det civila försvaret vid höjd beredskap, kan vara att upphandla fler leverantörer än i andra typer av upphandlingar. Därigenom kan risken för leveransproblem minskas för det fall en av leverantörerna skulle falla från på grund av obestånd eller av annan anledning skulle sakna förmåga att fullgöra avtalet, exempelvis vid höjd beredskap. I en sådan situation hjälper det nämligen inte att avtalet kanske innehåller långtgående leveransförpliktelser, eller sanktioner som vite för försenad eller utebliven leverans.

Om leverantören helt enkelt *inte kan* leverera det som den upphandlande organisationen behöver för sin verksamhet är det en klen tröst att det finns avtalsrättsliga sanktioner att använda. För särskilt viktiga avtal finns det därför anledning för upphandlande organisationer att inte bara försöka utforma sina avtal på ett sätt som möjliggör hantering av redan uppkomna problem, utan att även på förhand strukturera anskaffningen så att risken för att problem överhuvudtaget ska uppkomma minskar, eller i vart fall sprids ut på flera leverantörer.

Att upphandla flera leverantörer, trots att endast en leverantör under normala omständigheter skulle vara tillräcklig för att tillgodose den upphandlande organisationens behov, kan därför vara en metod att förebygga leveransproblem i samband med höjd beredskap.

Ett sätt att ingå avtal med flera leverantörer inom ramen för samma upphandling kan vara att tillämpa upphandlingslagarnas bestämmelser om uppdelning av kontrakt i mindre delar på ett strategiskt sätt, i syfte att fördela risker.

För upphandlingar som genomförs enligt LOU och LUF finns det uttryckliga möjligheter för en upphandlande organisation att bestämma om en och samma leverantör får lämna anbud på, eller tilldelas, en, flera eller alla delar av en upphandling.[118]

Bestämmelserna innebär att det är möjligt att göra undantag från principen om att kvalificerade anbudsgivare har rätt att lämna anbud respektive principen om att avtal alltid ska tilldelas den anbudsgivare som inkommit med det bästa anbudet i varje del. Istället kan den upphandlande organisationen tillse att flera leverantörer får var sin del av kakan. Vi bedömer att upphandlande organisationer kan använda sig av dessa bestämmelser i syfte att förebygga leveransproblem i samband med höjd beredskap eller kris.

I LUFS finns inga motsvarande bestämmelser. I bilaga IV till LUFS-direktivet, där kraven på vad ett meddelande om upphandling, en annons, ska innehålla, framgår dock följande:

> *Om kontrakten är uppdelade i flera delar ska det anges om de ekonomiska aktörerna kan lämna anbud på en, flera eller alla delar.*[119]

Det kan därför antas att det som är möjligt enligt LOU och LUF avseende uppdelning av kontrakt också är tillåtet enligt LUFS.

Ett annat sätt att ingå avtal med flera leverantörer inom ramen för samma upphandling kan vara att upphandla ett ramavtal och anta mer än en ramavtalsleverantör. För att ett sådant arbetssätt verkligen ska medföra ökad leveranssäkerhet i händelse av höjd beredskap krävs dock i många fall att den upphandlande organisationen använder en delvis annan metodik för fördelningen av de kontrakt som ska tilldelas än vad som annars normalt är fallet.

Många upphandlande organisationer arbetar idag, för att säkra leveranser, med ramavtal med flera leverantörer i rangordning. Ett problem med detta är att de leverantörer som är rangordnade på andra plats eller lägre ofta inte får tillräckligt många avrop för att få kostnadstäckning för de investeringar som krävs för att kunna hålla beredskap för det fall högre rangordnade leverantörer inte kan leverera.

---

118 4 kap. 13–16 §§ LOU respektive 4 kap. 11–15 §§ LUF.

119 Detta var även ordningen enligt 2004 års upphandlingsdirektiv för den klassiska sektorn och försörjningssektorerna, dvs. att det framgick av bilagor till direktiven att det skulle framgå av annonsen om anbudsgivare skulle tillåtas lämna anbud på en, flera eller alla delar.

Dessutom kan det under sådana förhållanden antas att lägre rangordnade leverantörers intresse av att prioritera leveranser till den upphandlande organisationen i händelse av en bristsituation är lågt om myndigheten inte framstår som en viktig kund. Detta alldeles oavsett vad som eventuellt står om sådan prioritering i ramavtalet.

Detta innebär sammantaget att den upphandlande organisationen inte utan vidare kan räkna med att få leveranser från lägre rangordnade leverantörer, för det fall den leverantör som är rangordnad på första plats skulle bli förhindrad att utföra leveranser.

Om myndigheten däremot redan vid upphandlingen av ramavtalet ser till att dela upp ramavtalet, så att varje antagen leverantör får någon del, kommer det att vara lättare för myndigheten att arbeta med aktiv avtalsförvaltning och använda avropsvolymer för att skapa incitament för leverantörerna att vara redo att bidra med ytterligare leveranser i händelse av höjd beredskap. Samtidigt får var och en av leverantörerna möjlighet till kostnadstäckning för sina investeringar.

På detta sätt kan myndigheten försäkra sig om att den har tillgång till leverantörer som den har en upparbetad relation med och som snabbt kan träda in och hantera en ökad avropsvolym om någon av de andra leverantörerna skulle bli förhindrade att leverera, eller om behoven skulle öka med anledning av höjd beredskap.[120]

Om ett avtal avseende ett visst upphandlingsföremål delas upp i flera mindre avtal skapas en större spridning av kapacitet hos leverantörskollektivet. Det kan leda till fler lämpliga leverantörer och det kan även, särskilt för rikstäckande avtal eller andra avtal som omfattar stora delar av landet, användas som ett sätt att geografiskt sprida ut viss kapacitet.

Nackdelen kan vara en ökad administrativ börda med fler avtal att förvalta och det innebär typiskt sett både högre transaktionskostnader och högre priser jämfört med en enda stor leverantör som garanterar hela det aktuella behovet. En avvägning måste därför göras i det enskilda fallet.

6.3 Ändrings- och optionsklausuler

Ett annat sätt att upphandla beredskap kan vara att upphandla avtal som redan från början är utformade för att kunna anpassas, det vill säga ändras, till de förändrade förhållanden och behov som kan bli följden av höjd beredskap eller kris.

LOU och LUF ger, genom bestämmelserna i 17 kap. LOU respektive 16 kap. LUF, möjlighet att i vissa fall ändra befintliga avtal utan att behöva genomföra en ny upphandling.

I LUFS finns inga motsvarande bestämmelser. Mycket talar dock för att i vart fall en del av de bedömningar som ska göras enligt LOU:s och LUF:s ändringsbestämmelser kan läggas till grund även för att motivera att en

120 För en mer detaljerad redogörelse för olika fördelningsnycklar för ramavtal med flera leverantörer se Ramavtal i offentlig upphandling – några frågor av betydelse för tolkning och tillämpning, Advokatfirman Kahn Pedersens rapport 2017:1, avsnitt 3.

upphandlande organisation avstår från ny upphandling i fall då LUFS är tillämplig.[121]

Bestämmelserna om kompletterande beställningar och ändringar till följd av oförutsedda omständigheter är visserligen sannolikt möjliga att använda i vissa fall av höjd beredskap eller kris, men med tanke på de rekvisit som måste vara uppfyllda för att bestämmelserna ska vara tillämpliga framstår det som vanskligt för en upphandlande organisation att lägga dem till grund för sin beredskapsplanering.

Bestämmelserna om ändringar med stöd av ändrings- eller optionsklausuler ger däremot upphandlande organisationer möjlighet att på förhand, i samband med att avtal utformas, skapa utrymme för att göra de ändringar som krävs för anpassning till de förändrade förhållanden och behov som kan bli följden av höjd beredskap. Bestämmelserna om ändringar med stöd av ändrings- eller optionsklausuler är därför bättre lämpade för upphandlingar som avser det civila försvaret.

För att en ändring av ett upphandlat avtal med stöd av en ändrings- eller optionsklausul ska vara möjlig krävs att följande förutsättningar är uppfyllda:

- Klausulen ska ha angetts i något av upphandlingsdokumenten i den ursprungliga upphandlingen.
- Klausulen ska klart, exakt och entydigt beskriva under vilka förutsättningar som den kan tillämpas.
- Klausulen ska ange omfattningen och arten av ändringarna som kan komma att göras.[122]

I skälen till upphandlingsdirektiven anges att ändrings- och optionsklausuler ska vara en möjlighet för att ändra avtal i efterhand, men att sådana klausuler inte ska få ge de upphandlande organisationerna en obegränsad frihet.[123]

Vår bedömning är att en väl genomförd beredskapsplanering bör kunna resultera i tydliga åtgärder och åtaganden som ska gälla för leverantören vid höjd beredskap. En ändrings- eller optionsklausul som anger att leverantören ska åläggas vissa specificerade skyldigheter vid höjd beredskap och hur dessa skyldigheter då ska ersättas bör enligt vår mening vara fullt möjlig att utforma på ett sätt som är förenligt med upphandlingslagarna och de principer som styr dessa. En sådan genomtänkt användning bör bland annat innefatta en bedömning av vilka förändringar som

121 EU-domstolen har i sin dom i målet C-454/06, Pressetext Nachrichtenagentur uttalat att en kontraktsändring som endast är en tillämpning av bestämmelser i ursprungskontraktet inte utgör en ändring av de väsentliga villkoren i kontraktet, se punkterna 60 samt 68 och 69. Vidare har EU-domstolen i målet C-549/14, Finn Frogne uttalat att en ändring av ett kontrakt inte kan ske om inte ”denna ändring hade angetts i villkoren i det ursprungliga kontraktet”, se punkt 30 samt jfr. i detta fall även HFD 2016 ref. 85. Även om EU-domstolens uttalanden är från tiden innan de nuvarande bestämmelserna om tillåtna ändringar trädde i kraft bör de i dessa delar fortfarande anses vägledande i fråga om vilka ändringar som är tillåtna, särskilt mot bakgrund av att de nuvarande bestämmelserna om ändringar av kontrakt delvis tillkommit i syfte att kodifiera EU-domstolens praxis på området, jfr. skäl 107 till dir. 2014/24/EU.

122 Se 17 kap. 10 § LOU och 16 kap. 10 § LUF.

123 Se skäl 111 till LOU-direktivet och skäl 117 till LUF-direktivet.

kan behöva göras i avtalet, det vill säga vad som behöver fungera annorlunda vid höjd beredskap eller kris jämfört med normalläget.

Det kan exempelvis finnas anledning att överväga ändrings- eller optionsklausuler som kan aktiveras successivt vartefter läget förändras, eller alternativa ändrings- eller optionsklausuler som kan tillämpas olika beroende på vad som inträffar.

I likhet med att upphandla fler leverantörer än vad som normalt skulle upphandlas kan detta innebära vissa nackdelar i form av exempelvis ökade kostnader till följd av att leverantörerna behöver få kostnadstäckning för de investeringar som krävs för att kunna hålla beredskap för det fall ändrings- och optionsklausulerna behöver aktiveras.

Det kan exempelvis handla om att produktions- eller transportutrustning, eller annan infrastruktur behöver anskaffas och därefter upprätthållas. I vart fall delvis kan dock sådana kostnader delas mellan den upphandlande organisationen och leverantörerna, genom att en del av den tillkommande ersättningen för leverantörerna betalas först om ändrings- eller optionsklausulerna aktiveras.

6.4 Uteslutning, kvalificeringskrav, utvärderingskriterier och särskilda kontraktsvillkor

Det finns många olika sätt för en upphandlande organisation att påverka och beakta olika egenskaper, både hos leverantörerna och hos föremålet för upphandlingen. Organisationen kan tillämpa uteslutningsgrunderna i upphandlingslagarna på leverantörer som misskött sig eller som har missförhållanden i sin verksamhet.

Kvalificeringskrav kan användas för att säkerställa en tillräcklig lägstanivå på de leverantörer som kan komma ifråga för att tilldelas avtal, med avseende på behörighet att utöva yrkesverksamhet, ekonomisk och finansiell ställning, eller teknisk och yrkesmässig kapacitet.

Vidare kan det i en teknisk specifikation ställas krav på egenskaper som varan, tjänsten eller byggentreprenaden ska ha.

Vid tvåstegsförfaranden kan dessutom ytterligare ett urval göras bland de kvalificerade leverantörerna, så att de leverantörer som bedöms bäst lämpade bjuds in till anbudsgivning.

Tilldelningskriterierna som den upphandlande organisationen använder i upphandlingen syftar till att fastställa vilket av anbuden som bäst uppfyller organisationens behov och önskemål, såsom de kommit till uttryck i upphandlingens utvärderingsmodell.

Den upphandlande organisationen kan också genom avtalsvillkorens utformning, bland annat med så kallade särskilda kontraktsvillkor, säkerställa att endast leverantörer som åtar sig att arbeta i enlighet med avtalsvillkoren kommer i fråga för att tilldelas avtal och att fullgörandet av avtalet också sker i enlighet med dessa villkor.

Nedan presenteras några upphandlingsrättsliga verktyg som står till upphandlande organisationers förfoganden för att införa beredskapsvillkor i sina upphandlingar. Vi går igenom dessa i ordningen uteslutning, kvalificeringskrav, utvärderingskriterier och särskilda kontraktsvillkor.

6.4.1 Uteslutning på grund av brister i beredskapshänseende

I 11 kap. 2 § 4 p. LUFS anges att den som har gjort sig skyldig till allvarligt fel i yrkesutövningen genom att exempelvis inte ha iakttagit sina skyldigheter i fråga om informationssäkerhet eller försörjningstrygghet vid ett tidigare kontrakt kan bli föremål för uteslutning. Försörjningstrygghet är inte definierat men får uppfattas som en leverantörs förmåga att upprätthålla en ändamålsenlig leverans även vid höjd beredskap, krig eller andra ”svåra förhållanden”.[124] Vår bedömning är att försörjningstrygghet och beredskapsarbete i detta sammanhang är utbytbara begrepp.

LUFS medger således tydligt stöd för att utesluta leverantörer som i tidigare kontrakt inte fullgjort sina åtaganden och skyldigheter i beredskapshänseende.

LOU och LUF saknar denna uttryckliga uteslutningsgrund för brister avseende försörjningstrygghet och beredskapsarbete. Det kan emellertid konstateras att uteslutningsgrunden för leverantörer som visat allvarliga eller ihållande brister i fullgörandet av något väsentligt krav i ett tidigare kontrakt enligt LOU, LUF eller LUFS även kan träffa brister vad avser beredskap.

Uteslutning enligt en sådan grund kräver dock att bristerna föranlett att det tidigare kontraktet sagts upp eller att skadestånd eller liknande påföljder aktualiserats. Det kan dock antas att den typen av brister också kan anses omfattas av den mer generellt formulerade uteslutningsgrunden för allvarligt fel i yrkesutövningen i LOU och LUF.[125]

För att understryka allvaret i den upphandlande organisationens och leverantörens gemensamma beredskapsarbete kan organisationen, i sina avtal med leverantörer, påminna om att brott mot avtalets beredskapsbestämmelser betraktas som väsentliga och som allvarligt fel i yrkesutövningen och kan föranleda uteslutning i kommande upphandlingar.

6.5 Beredskapskrav som kvalificeringskrav

LUFS erbjuder goda möjligheter för upphandlande organisationer att ställa beredskapskrav som kvalificeringskrav i upphandling.

---

124 Se prop. 2010/11:150 s. 129.

125 Se 13 kap. 3 § tredje punkten LOU samt 13 kap. 4 § tredje punkten LUF.

Enligt 12 kap. 2 § LUFS får en upphandlande organisation ställa krav på en lägsta nivå för en anbudsgivares, eller anbudssökandes, tekniska och yrkesmässiga kapacitet. Dessa krav ska dock vara förenliga med de bestämmelser som framgår av 12 kap. 8-16 §§ LUFS och uppställda kapacitetskrav ska ha ett samband med kontraktsföremålet och stå i proportion till detta. Myndigheten ska i annonsen ange vilka uppgifter som ska lämnas av en leverantör för att styrka sin tekniska och yrkesmässiga kapacitet.

12 kap. 11 § LUFS innehåller en förteckning av de uppgifter som kan krävas men det framgår samtidigt att denna förteckning inte är uttömmande.[126] I förteckningen anges bland annat att myndigheten, som bevis på att en anbudsgivare klarar uppställda beredskapskrav, får kräva uppgifter om de försörjningskällor som leverantören förfogar över för att fullgöra kontraktet, samt uppgifter om leverantörens förmåga att tillgodose ökade behov till följd av en kris eller att garantera underhåll, modernisering och anpassningar av den utrustning som är föremål för upphandlingen.

Enligt 12 kap. 11 § 11 p. LUFS får en upphandlande organisation vidare kräva bevis om leverantörens förmåga att behandla, lagra och överföra säkerhetsskyddade uppgifter på den skyddsnivå som krävs av organisationen.

Det är vår bedömning att LUFS bestämmelser ger tillräckligt stöd för att som kvalificeringskrav i en upphandling kräva att anbudsgivare eller anbudssökande ger in en komplett beskrivning av den utrustning och de materiella samt personella resurser som krävs för att fullgöra ett visst kontrakt även vid höjd beredskap.

Det bör noteras att sådan information typiskt sett kan antas ingå i en sådan risk- och sårbarhetsanalys som åligger myndigheter att genomföra (beskrivet i avsnitt 5.3 ovan). Om beredskapskrav ställs som kvalificeringskrav i en upphandling framstår det som lämpligt att utforma dem som krav på en risk- och sårbarhetsanalys, inspirerade av den som myndigheten enligt tillämplig lagstiftning har att upprätta.

Möjligheterna att begära in motsvarande bevisning och ställa motsvarande kvalificeringskrav är inte lika tydlig enligt LOU. Dels är LOU:s bevisförteckning i 15 kap. 11 § inte exemplifierande utan ger tvärtom intryck av att vara uttömmande. Dels innehåller förteckningen inte samma hänvisningar som LUFS vad avser exempelvis bevis för att tillgodose ökade behov till följd av en kris. Det är därför mindre tydligt i LOU i vilken utsträckning som beredskapskrav kan ställas som kvalificeringskrav.

Upphandlande organisationer som arbetar enligt denna lag bör därför överväga om inte beredskapskraven istället ska ställas på något annat sätt, såsom exempelvis utvärderingskriterier eller särskilda kontraktsvillkor.

126 Se i detta avseende 12 kap. 11 § LUFS som anger ”Den upphandlande myndigheten eller enheten ska i annonsen om upphandling ange vilka av de uppgifter som anges i andra stycket som den har valt och vilka andra uppgifter som måste tillhandahållas.”. Motsvarande formulering finns i det bakomliggande LUFS-direktivet, se artikel 42.5 som anger: ”Den upphandlande myndigheten eller enheten ska i meddelandet om upphandling ange vilka av de uppgifter som anges i första punkten som den har valt och vilka andra uppgifter som måste tillhandahållas.”

Enligt 14 kap. 1 § LUF får en upphandlande organisation fastställa objektiva villkor för uteslutning och kvalificering och ska i så fall se till att dessa villkor är tillgängliga för de presumtiva leverantörerna. Om den upphandlande organisationen ställer sådana krav som avses i 14 kap. 1 § LOU, det vill säga krav på behörighet att utöva yrkesverksamhet, krav på ekonomisk och finansiell ställning eller krav på teknisk eller yrkesmässig kapacitet, ska den iaktta de bestämmelser som framgår av 14 kap. 1-5 §§ LOU, det vill säga de bestämmelser som enligt LOU reglerar hur kvalificeringskrav får ställas.

Upphandlande organisationer som tillämpar LUF får alltså ställa samma typer av kvalificeringskrav som LOU tillåter, men LUF tillåter även andra kvalificeringskrav. Den enda uttryckliga begränsningen för sådana krav är att de är objektiva och att de är tillgängliga för presumtiva leverantörer.

Den mest rimliga tolkningen av detta utrymme är att en upphandlande organisation får uppställa vilka objektiva kvalificeringskrav den vill, i vart fall så länge som dessa har någon form av koppling till det kontrakt som ska tilldelas.[127]

Detta betyder att de beredskapskrav som är möjliga att ställa upp enligt LUFS även är möjliga att uppställa enligt LUF.

6.6 Beredskapskrav som utvärderingskriterier

Vad avser det tilldelningskriterium som anges i 13 kap. 1 § LUFS, det vill säga att myndigheten vid bedömningen av vilket anbud som är det ekonomiskt mest fördelaktiga, ska ta hänsyn till olika kriterier som är kopplade till föremålet för kontraktet, till exempel försörjningstrygghet.

Motsvarande bestämmelse för upphandling enligt LOU och LUF anger att tilldelningskriterier ska ha en anknytning till det som anskaffas och hänföra sig till upphandlingsobjektet under något skede av dess livscykel. Vidare anges att tilldelningskriterierna ska säkerställa en effektiv konkurrens och inte ge den upphandlande organisationen obegränsad valfrihet.[128]

Beredskapskriterier som har en tillräcklig koppling till kontraktet enligt LUFS klarar också detta test enligt övriga lagar. Det är således ingen skillnad i möjligheten att uppställa tilldelningskriterier avseende beredskap lagarna emellan.

Med tanke på anbudsgivares relativt omfattande möjligheter att själva fritt bestämma sina anbudspriser,[129] kan det dock vara olämpligt att an

127 Se Arrowsmith och Maund ”CSR in the Utilities Sector and the Implications of EC Procurement Policy: A Framework for Debate” kap. 11 i Arrowsmith och Kunzlik, Social and Environmental Policies in EC Procurement Law: New Directives and New Directions och Arrowsmith, The Law of Public and Utilities Procurement, Volume 2, 3 uppl., s. 414 ff.

128 Se 16 kap. 2 § LOU respektive 15 kap. 2 § LUF.

129 Se HFD 2018 ref. 50, HFD 2020 ref. 24 samt HFD 2022 ref. 41.

vända förekomsten av, eller inriktningen på, olika beredskapsåtgärder som tilldelningskriterier. Detta eftersom kvalitativa tilldelningskriterier som utvärderas mot anbudspriset alltid innebär att den anbudsgivare som offererar ett tillräckligt lågt anbudspris kan vinna upphandlingen utan att uppfylla de kvalitativa tilldelningskriterierna.

Med andra ord kan en anbudsgivare, om beredskapsaspekter utvärderas mot anbudspriset, avstå från att offerera sådana beredskapsåtgärder som inte är obligatoriska eller offerera otillräckliga beredskapsåtgärder, men trots det vinna upphandlingen, om anbudsgivaren bara offererar ett tillräckligt lågt anbudspris. Detta är förstås en olycklig konsekvens.

Samtidigt kan utvärderingskriterier vara lämpliga för att uppmuntra leverantörer att komma med egna förslag på beredskapsinitiativ och premiera de leverantörer som är villiga att göra särskilt långtgående åtaganden i detta avseende. Utvärderingskriterier är således lämpliga för att motivera leverantörsdrivna initiativ även på beredskapsområdet.

Sådana aspekter av föremålet för upphandlingen som är nödvändiga för den upphandlande organisationens verksamhet bör dock typiskt sett inte utvärderas utan istället göras till obligatoriska krav, exempelvis som särskilda kontraktsvillkor.

6.7 Beredskapskrav som särskilda kontraktsvillkor

I 7 kap. 12 § LUFS anges att en upphandlande organisation får ställa särskilda villkor för hur ett kontrakt ska fullgöras, så kallade särskilda kontraktsvillkor. Särskilda kontraktsvillkor är avtalsvillkor och behöver således uppfyllas först när kontraktet fullgörs.[130] Anledningen till att de regleras i upphandlingslagarna är emellertid att villkoren är sådana att leverantörens lösningar för att kunna uppfylla de särskilda kontraktsvillkoren kan behöva kontrolleras och bedömas redan i samband med upphandlingen. De särskilda kontraktsvillkoren kan särskilt avse underentreprenad, informationssäkerhet eller försörjningstrygghet.

Det är således tydligt att en upphandlande organisation enligt LUFS får ställa särskilda kontraktsvillkor som avser informationssäkerhet och försörjningstrygghet men även att andra särskilda kontraktsvillkor får ställas.

I 7 kap. 13-15 §§ LUFS framgår särskilda krav på informationssäkerhet som den upphandlande organisationen får ställa. Dessa inbegriper uttryckliga föreskrifter om att organisationen får ställa krav på hur leverantören och dess underleverantörer ska hantera säkerhetsskyddsklassificerade uppgifter.

I 7 kap. 16-17 §§ LUFS anges att den upphandlande organisationen i upphandlingsdokumenten ska ange sina krav på försörjningstrygghet och de krav på dokumentation som organisationen uttryckligen kan ange att anbuden ska innehålla för att bedöma leverantörens förmåga att uppfyl-

130 Jfr. bland annat C-295/20, *Sanresa*, där EU-domstolen påpekade att det kan vara oproportionerligt att kräva att de särskilda kontraktsvillkoren är uppfyllda redan vid anbudsgivningen.

la dessa krav. Bland dessa krav kan särskilt nämnas krav på att anbudsgivaren ska visa hur organiseringen och lokaliseringen av dess försörjningskedja gör det möjligt att uppfylla kraven på försörjningstrygghet.

Vidare kan det begäras en utfästelse om att ändringar i försörjningskedjan under genomförandet av kontraktet inte kommer att inverka skadligt på uppfyllandet av krav om försörjningstrygghet.

Det kan också krävas dokumentation från anbudsgivaren om att denne, i enlighet med villkor som parterna ska komma överens om, kommer att upprätthålla den kapacitet som krävs för att tillmötesgå den upphandlande organisationens eventuellt ökade behov till följd av en kris samt utföra underhåll, modernisering och anpassningar av den utrustning som är föremål för upphandlingen.

Det är också möjligt att kräva ett åtagande om att i tid informera den upphandlande organisationen om varje förändring i anbudsgivarens organisation, försörjningskedja eller industriella strategi som kan påverka anbudsgivarens skyldigheter gentemot den upphandlande organisationen.

Slutligen kan ett åtagande krävas om att, i enlighet med villkor som parterna ska komma överens om, förse den upphandlande organisationen med allt som behövs för produktion av reservdelar, komponenter, särskilda tillbehör och särskild testutrustning, inklusive ritningar, licenser och instruktioner, för den händelse anbudsgivaren inte längre kan tillhandahålla denna utrustning.

Vår bedömning är att LUFS, genom dessa bestämmelser, tillåter långtgående krav för att säkerställa en god beredskap i leveransen och för att kontrollera dessa krav i en upphandling.

Det är också tydligt att en upphandlande organisation kan ställa krav på att leverantören ska utöka sina leveranser vid höjd beredskap eller krig.

Enligt 17 kap. 1 § LOU respektive 16 kap. 1 § LUF får upphandlande organisationer ställa särskilda miljömässiga, sociala, arbetsrättsliga och andra villkor för hur ett kontrakt ska fullgöras. Den enda begränsning som gäller för dessa villkor är att de ska ha en koppling till kontraktsföremålet.

På samma sätt som vi kunde konstatera avseende kvalificeringskrav kan det således konstateras att alla särskilda kontraktsvillkor som är tillåtna enligt LUFS också torde vara tillåtna enligt LOU och LUF.

6.8 Sammanfattning

På det hela taget innehåller upphandlingslagstiftningen flera olika möjligheter att inkorporera beredskapshänsyn i såväl upphandlingsförfarandet som det efterföljande ramavtalet eller kontraktet.

I takt med att en allt större del av Sveriges grundläggande förvaltning och samhällsbärande infrastruktur lagts ut på entreprenad ökar behovet av att inkludera leverantörer i myndigheternas beredskapsarbete. Enligt vår mening har upphandlingslagstiftningen och inte minst Sveriges upphandlare en viktig roll i denna centrala del av det civila försvaret.

Om Advokatfirman Kahn Pedersen

Kahn Pedersen är en advokatbyrå helt inriktad på specialiserad affärsjuridik. Vi åtar oss uppdrag enbart inom våra två verksamhetsområden Digital och Public. Se www.kahnpedersen.se för mer information om vår verksamhet.

Författarna till denna rapport är:

Magnus Ehn, Senior Specialist

Christian Hybbinette, Partner

Olle Lindberg, Senior Associate

Daniel Lundqvist, Partner

Staffan Malmgren, Legal Technology Officer

Michael Nevinson, Senior Associate

Tina Njezic, Associate

Erik Olsson, Partner

Johanna Palm, Associate

Kristian Pedersen, Partner

Viktor Robertson, Senior Specialist

www.kahnpedersen.se
ISBN 978-91-986495-3-6