FSPOS

Nya förutsättningar för krisberedskap

231211

FSPOS AG Analys

2023-12-11

Sammanfattning

Denna PM syftar till att beskriva nya förutsättningar för krisberedskapen. Detta omfattar nya hot och risker, men även inriktningar och krav som ställs på samhällets sammantagna krisberedskap liksom på enskilda aktörers. Rysslands invasion av Ukraina 2022 underströk att beredskapsarbetet behöver accelereras, vilket märks i antalet utredningar, nya lagar och andra underlag som introducerats det senaste året. Innehållet i denna PM ska därför betraktas som en beskrivning av läget oktober 2023 avseende områden som har, eller inom kort kan få, relevans för krisberedskapsarbetet i finansiell sektor. Beskrivningarna har hållits relativt kortfattade, med källhänvisningar för fördjupade läsningar. Som komplement har en mindre intervjustudie genomförts med några aktörer inom finansiell sektor, med utgångspunkt i de beskrivna områdena. Intervjuerna syftar till att fånga exempel på aktörers förhållningssätt till utveckling av krisberedskapen.

Den främsta nya förutsättningen är den strukturreform för civil beredskap som genomfördes 2022. Reformen utgår från att krisberedskapen och det civila försvaret ska vara ömsesidigt förstärkande. I rådande hotbild ingår dessutom gråzonsproblematik, där omfattande samhällsstörningar behöver kunna hanteras av krisberedskapens strukturer. Utöver den säkerhetspolitiska utvecklingen påverkas hotbilden av samhälls- och teknikutvecklingen i stort. Digitaliseringen har bidragit till nya och effektivare tjänster, inte minst i finansiell sektor. Samtidigt innebär det nya sårbarheter, direkt såväl som genom leverantörs- och ägarförhållanden. Informations- och cybersäkerhetsarbetet är därför av avgörande betydelse för funktionaliteten i sektorn. Dessutom är finansiella tjänster beroende av fysisk infrastruktur, vilken kan skadas antingen avsiktligt eller oavsiktligt. Exempel på det sistnämnda är genom extrema väderhändelser.

I och med strukturreformen underströks finansiella sektorns viktiga roll för att upprätthålla samhällets funktionalitet också vid kriser, genom skapandet av beredskapssektorerna Finansiella tjänster och Ekonomisk säkerhet. Den breda hot- och riskbilden, tillsammans med finansiella sektorns roll, innebär att det etablerade arbetet med operativa risker och upprätthållandet av finansiell stabilitet fortsatt är viktigt, men inte tillräckligt för en väl fungerande beredskap för fredstida kriser, höjd beredskap eller ytterst krig. Det finns en rad olika regelverk som berör finansiella sektorns motståndskraft och omfattar olika aktörer, men det är myndigheter som har ett övergripande ansvar för att säkerställa civil beredskap. Arbete pågår för att tolka vad detta innebär. Centralt i arbetet är sektorns verksamheter som bedöms vara samhällsviktiga. Utifrån detta kommer fler aktörer att omfattas av olika former av uppgifter, såsom deltagande i planering och rapportering. Regelverk, vägledningar och annat stöd kommer att fortsätta utformas allteftersom. Tillkommande behov, såsom upprättande av ett system för försörjningsberedskap, liksom ett troligt Nato-medlemskap, behöver också inordnas i beredskapsarbetet. För försörjningsberedskapen är upprätthållandet av fungerande betalningsförmedling avgörande för att säkerställa flödet av samhällsviktiga varor och tjänster. Natos prioriterade förmågor för civil motståndskraft framhåller däremot inte explicit finansiella tjänster.

Representanter från sektorn lyfter i intervjuerna behovet av att fortsätta diskutera de nya förutsättningarna inom finansiell sektor och hur kan de omhändertas, såväl enskilt inom varje organisation, som i samverkan. Intervjuerna har gett viss vägledning om vad som kan vara mest angeläget att börja med.

SAMMANFATTNING 2

1 INLEDNING 5

1.1 SYFTE OCH AVGRÄNSNING 5
1.2 GENOMFÖRANDE 6
1.3 LÄSANVISNING 7

2 OM KRISBEREDSKAP 7

2.1 MÅL, SKYDDSVÄRDEN OCH SAMHÄLLSVIKTIG VERKSAMHET 8
2.2 FREDSTIDA KRISER OCH ALLRISKPERSPEKTIVET 8
2.3 PRINCIPER OCH FÖRMÅGOR FÖR KRISHANTERING 9
2.4 EN DEL AV CIVIL BEREDSKAP 9

3 EN DIFFUS OCH KOMPLEX HOT- OCH RISKBILD 10

3.1 CYBERHOT 11
3.2 UTKONTRAKTERING, TREDJEPARTSRISKER OCH UTLANDSBEROENDE 12
3.3 KLIMATRELATERADE RISKER OCH HOT 13
3.4 GRÅZONSPROBLEMATIK OCH HYBRIDKRIGFÖRING 14
3.5 NATIONELLA RISK- OCH SÅRBARHETSBEDÖMNINGEN 2023 (NRSB-2023) 14
3.6 HOTBILDSBEDÖMNING FÖR SVERIGES BANKER 15

4 STRUKTURREFORMEN FÖR KRISBEREDSKAP OCH CIVILT FÖRSVAR 15

4.1 BEREDSKAPSFÖRORDNINGEN (2022:524) 16
4.1.1 TOLKNING AV SEKTORSANSVARIGA MYNDIGHETERS ROLL, ANSVAR OCH MANDAT 17
4.2 UTVECKLING AV BEREDSKAPSFÖRMÅGA 17
4.2.1 PLANERINGSINRIKTNING FÖR CIVIL BEREDSKAP 17
4.2.2 PLANERING FÖR CIVIL BEREDSKAP: PROCESS OCH METOD 18
4.2.3 UTVECKLING AV FÖRMÅGA FÖR KRISBEREDSKAP OCH CIVILT FÖRSVAR 19
4.3 SAMHÄLLSVIKTIG VERKSAMHET I FINANSIELL SEKTOR 19
4.4 EN MODELL FÖR SVENSK FÖRSÖRJNINGSBEREDSKAP 21

5 BEREDSKAP AVSEENDE BETALNINGAR 22

5.1 RIKSBANKSLAG (2022:1568) 22
5.2 STATEN OCH BETALNINGARNA 22
5.3 EN NY LAG OM CLEARING OCH AVVECKLING AV BETALNINGAR 23

6 NATOS ARBETE MED CIVIL BEREDSKAP 24

6.1 SAMARBETE KRING CIVIL BEREDSKAP 24
6.2 NATOS BASKRAV FÖR RESILIENS 25

7 IT-, INFORMATIONS- OCH CYBERSÄKERHET 25

7.1 OFFENTLIGA INITIATIV TILL STÖD FÖR ÖKAD CYBERSÄKERHET 25
7.1.1 NATIONELL STRATEGI FÖR SAMHÄLLETS INFORMATIONS- OCH CYBERSÄKERHET 25
7.1.2 NATIONELLT CYBERSÄKERHETSCENTER (NCSC) 26
7.1.3 INFOSÄK- RESPEKTIVE IT-SÄKKOLLEN 26
7.2 NYA REGELVERK 27
7.2.1 DORA: DIGITAL OPERATIONAL RESILIENCE ACT 27
7.2.2 CER OCH NIS2 28
7.2.3 KRAV VID UTKONTRAKTERING 29
7.2.4 ARTIFICIELL INTELLIGENS, AI 30
7.3 MYNDIGHETERS IT-DRIFT 31
7.3.1 UTKONTRAKTERING AV MYNDIGHETERS IT-DRIFT 31
7.3.2 EN SAMORDNAD OCH SÄKER STATLIG IT-DRIFT 31

8 ANDRA SÄKERHETSASPEKTER 32

8.1 NY SÄKERHETSSKYDDSLAGSTIFTNING 32
8.2 UTLÄNDSKA DIREKTINVESTERINGAR OCH ÄGARFÖRHÅLLANDEN 34

9 INTERVJUSTUDIE MED AKTÖRER I FINANSIELL SEKTOR 34

9.1 HOTBILD 35
9.1.1 FÖRMÅGEUTVECKLING MOT DEN BREDDADE HOTBILDEN 36
9.2 STRUKTURREFORMEN 36
9.2.1 STRUKTUREN ÄR UNDER UTVECKLING 36
9.2.2 BRIST PÅ MANDAT OCH MÖJLIG ROLLKONFLIKT 38
9.3 SAMVERKAN INFÖR OCH VID FREDSTIDA KRISER 38
9.4 BETALNINGAR 39
9.5 NATOS ARBETE MED CIVIL BEREDSKAP 40
9.6 CYBERSÄKERHET 40
9.7 SÄKERHETSSKYDD 41

10 SLUTORD 41

10.1 RESILIENS FÖR ATT OMHÄNDERTA DET BREDDADE PERSPEKTIVET? 42
10.2 NYA, OMFATTANDE OCH SPRIDDA KRAV BEHÖVER TOLKAS 42
10.3 SAMVERKAN FÖR EN GOD KRISBEREDSKAPSFÖRMÅGA 43

11 REFERENSLISTA 45

BILAGA 1: INTERVJUGUIDE 49

1 Inledning

Det finansiella systemet spelar en viktig roll för Sveriges ekonomi, med viktiga samhällsfunktioner såsom upprätthållandet av finansiell stabilitet, förmedling av betalningar, försäkringar och sparande.[1] För att upprätthålla dessa viktiga funktioner krävs såväl förebyggande arbete som en effektiv krishantering. Sedan finanskrisen 2008 synliggjorde brister i systemet har en rad åtgärder vidtagits, såsom förändringar i regelverk och i den tillsyn som ska säkra finansiell stabilitet. EU införde 2014 *Krishanteringsdirektivet* (BRRD)[2] i syfte att stärka bankernas motståndskraft och säkerställa att systemviktiga bankers samhällsviktiga verksamheter kan upprätthållas vid en kris.[3] Det finns också en tydligare rollfördelning och ett samarbetsforum för finansiell stabilitet, mellan Finansdepartementet, Riksbanken, Finansinspektionen och Riksgäldskontoret.[4]

Systemet för finansiell stabilitet och därtill kopplad krishantering riktar sig mot kriser som uppstår i, direkt drabbar och/eller hanteras av aktörer inom finansiell sektor. Finansiella tjänster pekades 2017 ut av Myndigheten för samhällsskydd och beredskap (MSB) som ett av sju prioriterade områden för att öka hela samhällets robusthet.[5] Finansiella sektorns betydelse för svensk beredskap poängterades ytterligare 2022, i och med ny lagstiftning som pekade ut finansiella tjänster och ekonomisk säkerhet som beredskapssektorer, det vill säga sektorer inom vilka det bedrivs samhällsviktiga verksamheter som är av särskild betydelse att upprätthålla i fredstida krissituationer, höjd beredskap och ytterst krig. Det är i denna kontext, som en del av samhällets motståndskraft, som den finansiella sektorns krisberedskap betraktas i denna PM.

Samhälls- och teknikutvecklingen har inneburit att viktiga samhällsfunktioner i högre grad är beroende av varandra och att en störning lätt sprids mellan sektorer och behöver hanteras i samverkan. Till detta kommer självfallet det senaste decenniets försämring av det säkerhetspolitiska läget i Sveriges närområde. I takt med omvärlds-, samhälls- och teknikutvecklingen har en rad regelverk och inriktningar tillkommit för att förtydliga roller och vägleda arbetet med att stärka samhällets beredskap. Det finns därför ett behov av att redogöra för förutsättningarna för finansiella sektorns krisberedskapsförmåga.

1.1 Syfte och avgränsning

Denna PM syftar till att beskriva förändringar i hotbild, regelverk och inriktningar, nationellt såväl som i EU, som innebär nya förutsättningar för krisberedskapen i finansiell sektor. Arbetet har genomförts med ett brett anslag, där inte bara fastslagna inriktningar och regelverk beskrivs, utan även pågående utredningar att fortsätta följa. Alla aktörer berörs inte, åtminstone inte direkt, av allt som beskrivs i PM:n och ibland berörs aktörer på olika sätt, beroende på roll i systemet. Målet är en sektorsgemensam bild över de viktigaste förändringarna som påverkar finansiella sektorns aktörer och deras arbete med krisberedskap. PM:en avser därmed utgöra en basplatta för utveckling av krisberedskapsarbetet i sektorn, dels aktörsinternt dels i samverkan. För att få

---

[1] *MSB (2023), Lista med viktiga samhällsfunktioner – Utgångspunkt för att stärka samhällets beredskap*

[2] *Europaparlamentets och rådets direktiv 2014/59/EU. De förändringar som antagits och införlivats i svensk rätt har getts samlingsnamnet "Bankpaketet".*

[3] *Se exempelvis Riksbanken (2019), Bankpaketet – på väg till Sverige*

[4] *Finansiella stabilitetsrådet (2016), Överenskommelse om samarbete avseende finansiell stabilitet och krishantering*

[5] *MSB (2017) Nationella risk- och förmågebedömningen 2017. Övriga områden är energiförsörjning, livsmedel (inkl. dricksvatten), transporter, hälso- och sjukvård samt omsorg, finansiella tjänster, information och kommunikation, samt skydd och säkerhet.*

en bild av hur finansiella sektorns aktörer ser på arbetet med att omhänderta dessa nya förutsättningar, genomfördes även en mindre intervjustudie med ett urval aktörer.

Denna PM fokuserar på krisberedskap, det vill säga på arbetet för att förebygga att fredstida krissituationer uppstår, att minska sårbarheten om de inträffar och att stärka förmågan att hantera dem, om de ändå uppstår. I en promemoria framtagen inom FSPOS våren 2023 fokuserades på planeringsförutsättningar för civilt försvar/totalförsvar, det vill säga på förmåga att hantera händelser och fortsätta verka under höjd beredskap och krig.[6] Då det inte alltid går att dra en tydlig gräns mellan dessa områden kommer viss överlapp att förekomma. Eftersom nuvarande inriktning är att bygga beredskapsförmåga att hantera fredstida kriser till höjd beredskap och ytterst krig – det vill säga civil beredskap - går det inte alltid att skilja ut de krav som ställs just på krisberedskapen. Därför kommer det i rapporten att användas begrepp som civil beredskap, beredskapsområdet, beredskapsförmåga och så vidare där det just är arbetet för att hela hotskalan som beskrivs.

Beredskapsområdet är också under stark utveckling och en rad utredningar, lagar och planeringsunderlag kommer det närmaste året att fastställas. Alla dessa kan inte omhändertas i denna PM, men ambitionen är att beakta underlag som offentliggjorts senast oktober 2023.

Några ord behöver även sägas om titeln på promemorian. Vad som anses utgöra nya förutsättningar är inte självklart. Ett medvetet val har gjorts att inte ha en tidsgräns för vad som anses vara nytt, utan att snarare beskriva de områden som bedöms ha stor påverkan på krisberedskapsarbetet i nuläget. Målgruppen är aktörer inom FSPOS, vilket inte är homogen grupp. Vissa aktörer kommer redan vara väl insatta i flera av de områden som beskrivs och därför inte betrakta dem som nya.

1.2 Genomförande

Underlaget till denna PM utgörs av två huvudsakliga källtyper. Innehållet bygger till största delen på olika skriftliga underlag, såsom inriktningar, regelverk och analyser. Urvalet har stämts av och kompletterats i dialog med en referensgrupp, bestående av representanter från olika delar av den finansiella sektorn. Vissa underlag hanterar generella beredskapsrelaterade frågor, medan andra specifikt handlar om funktioner inom finansiell sektor. Referensgruppen har bistått med synpunkter på hur promemorian ska bli så relevant som möjligt för aktörerna i finansiell sektor.

I dialog med referensgruppen beslutades att genomföra en mindre intervjustudie, för att samla in ett antal röster från sektorn angående vad man känner till om de nya förutsättningarna och hur man förhåller sig till dem. Studien ämnar också bidra med en framtidsspaning avseende synen på vad som kommer att vara viktigt, samt utmaningar och framgångsfaktorer i anpassningen av beredskapsarbetet. Nio aktörer med god spridning i sektorn bidrog till intervjustudien, efter förslag från referensgruppen. Intervjuerna hade ett semistrukturerat upplägg och utgick från de områden som identifierats i den första delen av denna PM. Inför intervjuerna togs en intervjuguide med frågeställningar fram, vilken anpassades något efter typ av aktör, såsom exempelvis myndighet eller privat aktör. En generisk intervjuguide återfinns i bilaga 1. Respondenterna uppmanades att ge sin personliga syn som inte nödvändigtvis behövde vara förankrad i organisationen. Intervjustudien utger sig därför inte för att representera sektorn som helhet utan just vara ett sätt att fånga några tankar som finns i sektorn. Dessutom

[6] *FSPOS (2023) Aktuella planeringsförutsättningar för finansiella sektorns arbete med civilt försvar*

intervjuades en representant från MSB för att bidra med tankar om finansiella sektorns behov och utmaningar för att bidra till samhällets motståndskraft.

1.3 Läsanvisning

Det rådande omvärldsläget, liksom den snabba teknikutvecklingen, har medfört en rad nya regelverk och inriktningar på en bredd av områden som har bäring på krisberedskap. Överskådlighet över en bredd av områden har behövts balanseras mot den detaljnivå som krävs för att bidra till ökad kunskap. PM:en har därför en struktur som medger att läsaren kan välja ett specifikt område för att skaffa sig en överblick inom just detta och få källhänvisningar till fortsatt läsning. För en översikt över aktuella områden hänvisas till innehållsförteckningen.

PM:en inleds med två kapitel som avser ge en grundläggande förståelse för krisberedskap och dess grundläggande strukturer (kapitel 2) och den breda hot- och riskbilden (kapitel 3). Därpå följer i kapitel 4–8 en genomgång av olika underlag som tillsammans beskriver olika aspekter av de nya förutsättningarna för krisberedskapen. Vissa av dessa är specifika för finansiella sektorn, medan andra är generella för krisberedskapens olika aktörer. Ambitionen är ändå att så långt som möjligt beskriva tillämpningen för finansiell sektor.

I kapitel 9 redogörs för intervjustudien strukturerad med utgångspunkt i tidigare beskrivna områden, innan PM:en avslutas i kapitel 10 med några övergripande områden som finansiella sektorn skulle kunna arbeta vidare med.

2 Om krisberedskap

Kraven på svensk beredskapsförmåga ställs utifrån hotbilden och dess utveckling, traditionellt utifrån det militära hotet. Det svenska totalförsvaret bygger på erfarenheter från andra världskriget och på tanken är att det moderna kriget drabbar hela samhället och att såväl militära som civila resurser behöver mobiliseras för att klara försvarsansträngningarna. Efter det kalla krigets slut räknade man dock inte längre med något militära hot mot Sverige som nation och totalförsvarsplaneringen ansågs därmed inte längre nödvändig. Försvarsmaktens resurser reducerades väsentligt och det militära försvaret verksamhet inriktades i stället mot fredsfrämjande internationella insatser. Under denna tid började ett utvidgat säkerhetsbegrepp att diskuteras som även omfattade samhällets och människors säkerhet och inte enbart nationens.[7,8] Det innebar att även andra hot än de militära uppmärksammades. Civila aktörers beredskap, krisberedskapen, inriktades mot att främst hantera olika fredstida hot mot samhällets funktionalitet. I detta kapitel beskrivs kortfattat krisberedskapens grunder. Kapitlet avslutas med att kortfattat beskriva den nya inriktningen, att krisberedskapen är en del av det som idag av MSB kallas civil beredskap, handlar om förmågan att förebygga och hantera fredstida krissituationer, krigsfara och ytterst krig.

---

[7] *Begreppet mänsklig säkerhet lanserades 1994 av FN i Human Development Report i syfte att bredda det traditionella säkerhetsbegreppet. Mänsklig säkerhet delades in i sju områden, bland annat ekonomisk säkerhet, matsäkerhet och hälsosäkerhet. Begreppet beskrivs av Robert Egnell i Mänsklig säkerhet 2017, Vad är mänsklig säkerhet? (manskligsakerhet.se)*

[8] *Den så kallade "Köpenhamnsskolan" presenterade ett nytt analysramverk i Buzan, Barry, Wæver, Ole & Wilde, Jaap de (1998). Security: a new framework for analysis.*

2.1 Mål, skyddsvärden och samhällsviktig verksamhet

Regeringen har formulerat målet för samhällets krisberedskap:[9]

- att minska risken för olyckor och kriser som hotar vår säkerhet och
- att värna människors liv och hälsa samt grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter genom att upprätthålla samhällsviktig verksamhet och hindra eller begränsa skador på egendom och miljö då olyckor och krissituationer inträffar.

Dessutom bör arbetet med krisberedskap bidra till att minska lidande och konsekvenser av allvarliga olyckor och katastrofer i andra länder. Av målen framgår att det förutom krishantering ingår såväl förebyggande, förberedande som återställande perspektiv. Till detta ska läggas utvärdering och lärande, i en iterativ process.

I målet ovan beskrivs det som kallas samhällets skyddsvärden. Samhällsviktig verksamhet är en central del av beredskapsarbetet och beskrivs enligt följande: *"Den verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet."*[10]

2.2 Fredstida kriser och allriskperspektivet

En rad begrepp har använts för att beskriva de händelser som krisberedskapen ska hantera; svåra påfrestningar på samhället i fred, extraordinära händelser och som i 6§ i den nya beredskapsförordningen (2022:524); fredstida krissituationer. Dessa karakteriseras av att de avviker från det normala, drabbar många människor, stora delar av samhället eller hotar grundläggande värden samt att de innebär en allvarlig störning eller en överhängande risk för en allvarlig störning av viktiga samhällsfunktioner, och kräver samordnade och skyndsamma åtgärder från flera aktörer. Myndigheten för samhällsskydd och beredskap (MSB) använder begreppet samhällsstörning, för att poängtera att krisberedskapen ska hantera företeelser och händelser som hotar eller skadar det som ska skyddas i samhället.[11]

Det finns i nuläget inget dimensionerande scenario eller formulerade resultatmål som krisberedskapen ska utformas efter, utan den ska ha ett så kallat allrisk-perspektiv för att kunna hantera en bredd av olika händelser.[12] Genom risk- och sårbarhetsanalyser (RSA) - lagstadgade för statliga myndigheter, kommuner och regioner - identifieras och prioriteras oönskade händelser att skapa förmåga att hantera utifrån sannolikhets- och konsekvensbedömningar.[13]

---

[9] *Se exempelvis budgetpropositionen för 2021Prop. 2020/21:1 Utgiftsområde 6.*

[10] *6§ Förordning (2022:524) om statliga myndigheters beredskap*

[11] *MSB (2018), Gemensamma grunder för samverkan och ledning vid samhällsstörningar: sammanfattning*

[12] *Se MSB 2014-1942 Övergripande inriktning för samhällsskydd och beredskap, s. 13 ff.*

[13] *Förordning (2022:524) om statliga myndigheters beredskap respektive Lag (2006:544) om kommuners och regioner åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.*

2.3 Principer och förmågor för krishantering

Vid samhällsstörningar ska krishanteringen förhålla sig till tre grundläggande principer; ansvarsprincipen som anger att samma ansvarsförhållanden som i normaltillstånd så långt som möjligt ska råda också vid störningar, närhetsprincipen som säger att samhällsstörningar ska hanteras där de inträffar och av de som är närmast berörda och likhetsprincipen, det vill säga att organisationen inte ska förändras mer än nödvändigt. Ibland räcker dock inte de ordinarie strukturerna till och störningar kan behöva hanteras av en särskild krisorganisation. Det kan handla om att det finns behov av att snabba upp beslutsprocesser eller beakta flera perspektiv. I tillägg talar man även om den så kallade utökade ansvarsprincipen, det vill säga att aktörer ska ge stöd till och samverka med berörda aktörer i krishanteringen.

Beroende på typ av kris och utifrån de stora beroenden som finns mellan samhällssektorer kan krishanteringen kräva insatser av olika aktörer, såväl offentliga som privata och organisationer. MSB har identifierat generella förmågor för aktörsgemensam krishantering; samverkan och ledning, kriskommunikation och resurshantering.[14] Genom samverkan och/eller ledning ska en aktörsgemensam inriktning utarbetas, så att samordning av de insatser som görs får störst effekt. Till stöd finns ett framtaget ramverk, *Gemensamma grunder för ledning och samverkan vid samhällsstörningar*.[15] Ramverket är utvecklat i samverkan med olika samhällsaktörer, såsom kommuner, regioner, myndigheter, frivilliga organisationer och företag. För att de beskrivna arbetssätten ska fungera krävs en etablerad samverkan även i vardagen.

2.4 En del av civil beredskap

Det senaste decenniet har inneburit en negativ säkerhetspolitisk utveckling i vårt närområde. Behovet av att – återigen – inkludera ett väpnat angrepp i hotbilden har blivit påtagligt. Samtidigt behöver krisberedskapen kunna förebygga och hantera händelser som skulle kunna utgöra förberedelser för ett sådant angrepp. MSB betonar i rapporten *Civilt försvar mot 2030, ett totalförsvar i balans* att ett integrerat arbete med krisberedskap och civilt försvar nu krävs för att inkludera alla slags samhällsstörningar, inklusive väpnat angrepp. Begreppet civil beredskap har därför återtagits, men omfattar alltså inte bara beredskapsplanering inför ett väpnat angrepp utan ska beskriva beredskapsförmåga att hantera såväl fredstida kriser, höjd beredskap och ytterst krig.

I Sverige går en skarp juridisk skiljelinje mellan fred och krig, eller snarare mellan fred och regeringens beslut om höjd beredskap.[16] Vid krig eller krigsfara kan regeringen besluta att särskilda regelverk, bland annat de så kallade fullmaktslagarna, ska träda i kraft och medge ett annat handlingsutrymme för att hantera det krävande läget.[17] Händelser i en gråzonssituation, den diffusa övergången mellan fred och krig, ska dock hanteras inom det fredstida regelverket och av krisberedskapens strukturer. Detta ställer krav på en krisberedskapsförmåga som kan möta såväl icke-antagonistiska hot (olyckor och naturkatastrofer) som antagonistiskt orsakade

---

[14] *MSB (2021), Övningsinriktning för bevakningsansvariga myndigheter på nationell och regional nivå avseende samverkansövningar under 2022–2026, MSB 2021-06744*

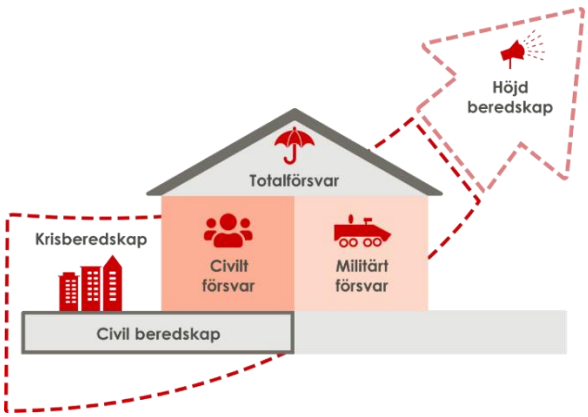
[15] *Gemensamma grunder för samverkan och ledning vid samhällsstörningar: sammanfattning. Under sommaren 2023 kunder synpunkter lämnas i ett öppet remissförfarande för att vidareutveckla ramverket.*

[16] *I Sverige finns inte den möjlighet att utlysa undantagstillstånd som vissa länder har, vilket debatterades under Coronapandemin.*

[17] *Se 13 § i förordningen om totalförsvar och höjd beredskap.*

händelser; olika former av öppna och dolda påtryckningar, cyberattacker och informationsoperationer. Likaså krävs förmåga att identifiera och möta underrättelseverksamhet.

MSB illustrerar byggstenarna för svensk beredskap i kris och krig enligt Figur 1 nedan.[18]



Figur 1: Illustration av hur krisberedskap, civilt försvar, och totalförsvar hänger ihop. (MSB, 2022)

3 En diffus och komplex hot- och riskbild

Den förmåga aktörer behöver ha för att minska risken för och konsekvenserna av störningar styrs dels av de hot som föreligger, dels av krav på processer för att identifiera och omhänderta risker och hot.[19] För att upprätthålla motståndskraften behöver hot- och riskbilden kontinuerligt omprövas.

I finansiell sektor finns omfattande regelverk och riktlinjer för hantering av risker. Man pratar om operativa risker, marknadsrisker, kreditrisker och försäkringsrisker. Finansinspektionen ger ut föreskrifter för och arbetar med tillsyn avseende styrning, riskhantering och kontroll. Genom dessa kravställs vad aktörer i den finansiella sektorn behöver göra för att motverka att störningar uppstår och för att upprätthålla verksamhet om de ändå uppstår.[20] Att upprätthålla finansiell stabilitet är vidare en förutsättning för att undvika kriser i det finansiella systemet. Enligt avsnitt 0 är dock krisberedskapens målsättning mer omfattande och handlar om säkerhet, samhällets funktionalitet och grundläggande behov. Vid samhällsstörningar krävs ofta ett gemensamt och samordnat agerande mellan aktörer, inte sällan utanför den egna sektorn. Även om dessa störningar kan ha sitt ursprung i risker som identifierats i finansiell sektor, behöver krisberedskapsarbetet beakta ett bredare spektrum av händelser och hot.

De senaste åren har en rad händelser inträffat som ställt höga krav på samhällets sammantagna krisberedskap. Coronapandemin innebar störningar i alla samhällssektorer samtidigt, antingen direkt eller genom komplexa samband, såväl i Sverige som globalt. Globaliseringen innebär en

---

[18] *MSB (2022), Civilt försvar mot 2030 – ett totalförsvar i balans*

[19] *I många sammanhang används begreppen hot och risk synonymt, men ibland görs en åtskillnad; hoten är det som kan ha en negativ påverkan på det som ska skyddas, medan risken är resultatet av en hotanalys med bedömningar av hur sannolikt det är att scenariot inträffar samt vilka konsekvenserna skulle bli, se exempelvis MSB (2016), MSB:s föreskrifter för statliga myndigheters risk- och sårbarhetsanalyser, MSBFS 2016:7. I kapitlet används de begrepp som används i de källor varifrån informationen hämtats.*

[20] *Konsoliderad version: Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker och Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut. I 6 kap. 2 § lagen (2004:297) om bank och finansieringsrörelse finns bestämmelser om riskhantering.*

flexibilitet när det gäller att hantera störningar, men även att störningar i omvärlden kan sprida sig till Sverige. Pandemin visade hur beroende samhällets funktionalitet är av att de internationella handelsflödena hålls i gång. Även behovet av att planera för uthållighet i krishanteringen blev tydligt. Samtidigt uppvisades en stor omställningsförmåga, vilket inneburit viktiga lärdomar att ta med i kommande beredskapsarbete. Bara under sommaren 2023 såg vi också att olika väderrelaterade händelser orsakade eller riskerade att orsaka samhällsstörningar, såväl torka med risk för skogsbränder, som höga flöden, översvämningar och skred. Detta är fenomen som bedöms öka till följd av klimatförändringarna. Till detta kommer störningar som initieras med uppsåt, av olika anledningar. Cyberattacken 2021, som fick Coops kassasystem att haverera, visade på en sårbarhet som kan uppkomma till följd av ett leverantörsberoende. Under sommaren beslutade också Säkerhetspolisen att höja terrorhotnivån, bland annat till följd av reaktioner på en rad koranbränningar och påverkanskampanjer.[21] I dessa bedömningar vägs även omständigheter som kan påverka hotets utveckling in, däribland finansiering av terrorism, där finansiella sektorn omfattas av olika regelverk.[22,23]

I hotbilden ingår således såväl antagonistiska som icke-antagonistiska hot; klimatförändringar, naturkatastrofer, pandemier, terrorism, cyberangrepp, påverkanskampanjer, organiserad brottslighet med mera. Till följd av negativ säkerhetspolitisk utveckling i vårt närområde, det vill säga Rysslands invasion av Ukraina, inbegrips även ett väpnat angrepp i hotbilden. Detta är något som primärt hanteras i arbetet med civilt försvar, men ett angrepp kan föregås av så kallad gråzonsproblematik, med olika former av omfattande störningar på det civila samhället.

Beskrivna hot kan antingen direkt eller genom en beroendekedja orsaka samhällsstörningar. Hotbilden brukar därför beskrivas som både diffus och komplex. Nedan beskrivs hot- och riskbilden utifrån olika underlag som belyser olika perspektiv, dels risker som direkt påverkar det finansiella systemet, dels den bredare hotbild som behöver beaktas i arbetet med samhällets krisberedskap.

3.1 Cyberhot

Finansiella sektorn har med teknikutvecklingen genomgått stora förändringar och är starkt beroende av fungerande elförsörjning och elektroniska kommunikationer. Finansiell sektor är även sammankopplad och infrastrukturen koncentrerad, vilket innebär både en risk för att spridning av en störning och att funktionaliteten påverkas i brist på redundans. Det säkerhetspolitiska läget innebär en större risk för allvarliga driftstörningar, något som kan få omfattande negativa effekter för samhället i stort.

Cyberrisker inbegrips numera i begreppet operativa risker och den riskhantering som aktörer i finansiella sektorn omfattas av.[24] Med cyberrisk menas kombinationen av sannolikhet för och konsekvenser av cyberincidenter.[25] Riksbanken gav sommaren 2023 ut ett memo som resonerar kring cyberrisker som både direkta som indirekta hot mot finansiell stabilitet. Exempel på det förstnämnda är störningar som drabbar centrala IT-system till vilka det inte finns alternativ för att leverera en ekonomisk funktion. Ett indirekt hot utgörs av det beroende som finns av andra

---

[21] *Säkerhetspolisen har beslutat om höjd terrorhotnivå - Regeringen.se, hämtad 231101*

[22] *Nationellt centrum för terrorhotbedömning - Säkerhetspolisen (sakerhetspolisen.se), hämtad 231105*

[23] *Penningtvätt och finansiering av terrorism | Finansinspektionen, hämtad 231105*

[24] *Exempelvis 6 kap. 2 § lagen (2004:297) om bank och finansieringsrörelse och Finansinspektionens föreskrifter 2014:1 och 2014:4*

[25] *Begreppet beskrivs i FSPOS (2021), Identifiering och värdering av cyberrisker*

samhälleliga funktioner och deras IT-resurser, exempelvis avseende elförsörjning. Det påpekas också att alla störningar som påverkar det så viktiga förtroendet för det finansiella systemet negativt också kan hota den finansiella stabiliteten. [26]

Cybersäkerhet tillägnas ett eget kapitel i Betalningsutredningens betänkande.[27] Utredningen beskriver cyberattacker som en särskild operativ risk i det att de är avsiktliga och troliga. Metoderna blir alltmer sofistikerade och därmed svåra att hindra. De kan även vara dolda i systemen, ibland under en längre tid innan problemen blir uppenbara. Utvecklingen mot fler fintechföretag i betalningsekosystemet[28] gör det än mer sammanflätat och att risken för spridning ökar. Cyberattacker kan riktas mot banker och betalningsinfrastruktur, men även mot den digitala infrastrukturen. Attacker mot enskilda företag kan orsaka konsekvenser på systemnivå då betalningsinfrastrukturen är mycket koncentrerad, med ett fåtal större företag som svarar för en betydande del av betalningsflödena.

3.2 *Utkontraktering, tredjepartsrisker och utlandsberoende*

En annan risk som ofta kopplas till cybersäkerhetsområdet, men som kan uppkomma på andra områden, är det som kallas tredjepartsrisker. Att använda sig av underleverantörer eller outsourcing/utkontraktering (eller utlagd verksamhet) har flera fördelar såsom kostnadseffektivitet - dock kvarstår ansvaret för riskhantering. Leverantören kan i sin tur lägga ut denna verksamhet till en annan leverantör, vilket ökar riskexponeringen och försvårar god styrning och kontroll.

Utkontraktering av betalningsinfrastruktur har vissa fördelar utifrån ett säkerhetsperspektiv, bland annat kan tredjepartsleverantörer ha större resurser och kommersiella drivkrafter att tillhandahålla robusta tjänster jämfört med om sådana tjänster produceras av infrastrukturföretagen själva. Det som försvåras är tillsynen för att säkerställa regelefterlevnad hos tredjepartsleverantörer, särskilt om de inte omfattas av finansiell reglering eller agerar från tredjeland (eller både och).

En trend avseende digitala värdekedjor är att de har blivit komplexa, beroende av tredjeparsleverantörer, men även omfattar verksamhet i utlandet. Större, samordnade resurser kan skapa god motståndskraft, men ett utlandsberoende kan även innebära utmaningar för nationell säkerhet när det gäller tillträde till och skydd av inhemsk samhällskritisk infrastruktur och viktiga känsliga datauppgifter, i fredstida kriser och ytterst krig.[29]

Utländska investeringar i verksamhet som bedrivs i Sverige har också fördelar, såsom tillförsel av kapital och möjligt bidrag till sysselsättning och tillväxt. Under Coronapandemin identifierades dock en risk för att nyckelteknologier reas ut när värderingen på företagen minskar, samtidigt som behovet av kapital ökar snabbt. Strategiska teknikbolag riskerar bli uppköpta till underpris av bulvaner för fientliga stater. Detta var något man såg under eurokrisen

---

[26] *Riksbanken (2023), Staff Memo Cyberrisker och finansiell stabilitet*

[27] *Kapitel 12, Cybersäkerhet i betalningsekosystemet, Staten och betalningarna, SOU 2023:16. Beredskapsdelarna som utredningen beskriver behandlas PM:en i kapitlet Beredskap avseende betalningar.*

[28] *Fintech, Financial Technology, används för att beskriva IT-teknologi utvecklar lösningar för behov inom finansbranschen. Utredningen använder begreppet betalningsekosysem för de sätt som finns att betala, de aktörer som är involverade och kopplingarna mellan dem.*

[29] *Betalningsutredningen resonerar kring detta i slutbetänkandet Staten och betalningarna, SOU 2023:16*

(2012–2013), då strategiska bolag och infrastrukturella tillgångar i såväl Sverige som i andra europeiska länder förvärvades.

3.3 Klimatrelaterade risker och hot

MSB publicerade 2023 en studie vars syfte var att översiktligt analysera hur klimatförändringar, klimatanpassning och klimatomställning kan påverka förmågeutvecklingen inom civil beredskap fram till mitten av 2000-talet. Påverkan på möjligheten att tillhandahålla finansiella tjänster belyses inte explicit, däremot finns resonemang kring försörjning av el och elektroniska kommunikationer – något som finansiella tjänster är beroende av. Bland annat beskrivs att klimatförändringarnas konsekvenser på elnät främst kan härledas till förändrade is- och snöförhållanden, temperaturförändringar och ett ökat antal översvämningar, ras och skred som påverkar infrastrukturen. Redan nu beror 85 % av avbrotten i elförsörjningen på väderrelaterade händelser. Även den ökade risken för vegetationsbränder kommer sannolikt att i ännu större omfattning påverka telekommunikation och elförsörjning.[30]

Dessutom kan fysisk risk uppstå till följd av klimatförändringar som minskar olika tillgångars värde. Försäkringsbolag kan behöva betala ut stora belopp och bankers säkerhet kan minska i värde till följd av extrema väderhändelser. Denna och andra risker tas upp i Riksbankens fördjupning avseende klimatrelaterade risker som utkom 2021. Detta då dessa på olika sätt kan skapa finansiella risker för det finansiella systemet och därmed hota den finansiella stabiliteteten. I fördjupningen belyses även de finansiella risker som kan uppstå till följd av omställningen till en fossilfri ekonomi. Politiska beslut för att öka takten ändrar förutsättningarna på specifika marknader och kan få konsekvenser för prissättningen på de finansiella marknaderna. Finansiella risker kan då uppstå på grund av osäkerhet om tillgångarnas framtida värde.[31]

Finansinspektionen hör till de myndigheter som enligt förordning (2018:1428) om myndigheters klimatanpassningsarbete ska göra en klimat- och sårbarhetsanalys av hur klimatförändringarna påverkar på myndighetens verksamhet. Myndigheten redovisade 2021 sin analys och formulerade mål på området.[32] Där konstateras att klimatförändringarna ger upphov till stora fysiska och därmed ekonomiska risker, både sett till deras möjliga omfattning och hur de negativa effekterna kan slå. I PM:en illustreras fysiska risker som kan uppkomma, både till följd av långsammare förändringar av klimatet och av extrema väderhändelser. Påverkan på finansiella företag kan också ske direkt eller genom effekter på icke-finansiella företag och på samhället. Exempelvis kan direkta skador på reala tillgångar uppstå, tillgången till råvaror och resurser kan bli begränsad, tillgångars marknadsvärde kan förändras och företags kostnader och intäkter kan påverkas. Detta kan i sin tur påverka såväl kreditrisker, marknadsrisker, försäkringsrisker som operativa risker. FI konstaterar att oavsett vilka risker det rör sig om behöver finansiella företag identifiera och hantera dessa inom ramen för sin verksamhet.

---

[30] *MSB (2023, Förändringar, anpassning och omställning Nya perspektiv och utmaningar för civil beredskap i ett föränderligt klimat, MSB2178*

[31] *Riksbanken (2019), Klimatrelaterade risker är en källa till finansiella risker, fördjupning i Finansiell stabilitetsrapport 2019_2*

[32] *Finansinspektionen (2021), Finansinspektionens klimatanpassningsarbete, FI dnr 21-13007*

3.4 Gråzonsproblematik och hybridkrigföring

Försvarsberedningen skriver i Allvarstid, den säkerhetspolitiska rapporten 2023, att ett väpnat angrepp mot Sverige inte kan uteslutas.[33] I händelse av höjd beredskap aktiveras det civila försvaret. Dock ingår i hotbilden så kallad gråzonsproblematik, som brukar beskrivas som ett läge mellan krig och fred, med omfattande samhällsstörningar. Situationen präglas av osäkerhet och det kan vara svårt att utröna händelsernas orsaker. Terrorgrupper och organiserad brottlighet kan också agera ombud för en fientlig stat. En utmaning är att det kan bli för stort fokus på de enskilda händelserna och att de inte läggs ihop till en korrekt lägesbild över flera samhällssektorer. Därigenom kan antagonisten förhindra att motparten eskalerar situationen och inleder krigsförberedelser. Syftet kan också vara att öva eller demonstrera vissa förmågor. Gråzonsstrategier är inte ett nytt fenomen, men den informationsteknologiska utvecklingen har inneburit nya möjligheter. En bredd av icke-militära maktmedel används framför allt riktat mot samhällets funktionalitet, vilket också benämns hybridkrigföring. Det kan röra sig om påverkanskampanjer, fysiskt sabotage, cyberattacker, manipulering av marknader, hot och påtryckningar mot beslutsfattare med mera.[34] Genom angrepp i cyberdomänen kan kritiska samhällsfunktioner störas och cyberattacker är numera en integrerad del av modern krigföring. Rysslands storskaliga invasion av Ukraina 2022 föregicks av omfattande cyberattacker mot ukrainsk digital infrastruktur, såväl som mot myndigheter och samhällsviktiga företag. Även informationspåverkan, sabotage, spionerі, kriminalitet och terrorism kan utföras genom angrepp i cyberdomänen, vilket innebär en ökad bredd av såväl möjliga angripare, som potentiella mål.

För att möta gråzonshot krävs i första hand icke-militära motmedel och en god förmåga att upprätthålla samhällets funktionalitet. Robustare försörjningssystem ger ökad motståndskraft, samtidigt som det verkar avskräckande på en angripare och bidrar till det som kallas tröskeleffekten. Det innebär att det förebyggande och förberedande arbetet inte bara påverkar effekten av hoten om de genomförs, utan även bidrar till att påverka hotbilden i sig.

3.5 Nationella risk- och sårbarhetsbedömningen 2023 (NRSB-2023)

MSB har i uppdrag av regeringen att göra nationella risk- och sårbarhetsbedömningar.[35] Uppdraget innebär att bedöma särskilt allvarliga hot och risker och identifiera sårbarheter både på övergripande samhällsnivå och per beredskapssektor.

MSB konstaterar i NRSB-23 att den föränderliga och mångfacetterade samhällsutvecklingen medför en bred och komplex hot- och riskbild. Då det pågår ett flertal uppdrag med väpnat angrepp i fokus, inriktades NRSB-23 i stället på fredstida kriser. MSB har i riskbedömningen identifierat 17 oönskade händelser som experter bedömt utgör de allvarligaste hoten mot Sverige. Bland att nämns att sabotage mot kritisk infrastruktur och IT-incidenter kan leda till avbrott i utbetalningar. Även flera andra identifierade händelser skulle, direkt eller indirekt, kunna påverka finansiell sektor, såsom solstormar som slår ut satellittjänster, elnätsammanbrott som

---

[33] *Försvarsberedningen (2023), Allvarstid. Försvarsberedningens säkerhetspolitiska rapport, Ds 2023:19*

[34] *För en utförligare beskrivning av gråzonsproblematiken, se Jonsson (2018) Typfall 5: utdragen och eskalerande gråzonsproblematik. Komplettering av hotbildsunderlag i utvecklingen av civilt försvar, FOI Memo 6338. I Jonsson mfl (2023) Gråzonslägen i krig och fred illustreras i tolv scenarier hur antagonistiska gråzonshot skulle kunna gestaltas, nu och i framtiden, i olika konfliktnivåer, i samspel med olika slags kriser (ekonomi, miljö, klimat, olyckor osv.) och samhällsförändringar (internationalisering, digitalisering, polarisering osv.). Scenarierna utforskar även antagonistiska gråzonshot före, under och efter en krigssituation. I Jonsson (2018) Gråzonsproblematik och hybridkrigföring – påverkan på energiförsörjning, FOI-R--4590-SE, beskrivs gråzonsproblematiken utifrån påverkan på en samhällsviktig sektor.*

35 Tidigare gjordes nationella risk- och förmågebedömningar (NRFB) med fokus på utveckling av förmåga.

medför att bankomater och betalsystem slutar fungera, dammhaveri och terrordåd.[36] Sårbarhetsbedömningen redovisar egenskaper eller förhållanden som gör samhället sårbart om identifierade händelser skulle inträffa och är därmed sekretessbelagd. Bedömningarna redovisas sektorsvis och på övergripande samhällsnivå, åtföljt av ett urval av vidtagna och planerade åtgärder för att minska riskerna.[37]

3.6 Hotbildsbedömning för Sveriges banker

Bankerna gör årliga bedömningar av hot- och riskbilden, som underlag för att stärka säkerheten. I bedömningen för 2023 återfinns hot mot såväl personal och verksamhet, som mot Sveriges säkerhet.[38]

Svenska banker utgör en betydande del av den baltiska finansiella infrastrukturen, vilket med hänsyn till rådande säkerhetspolitiska förhållanden bedöms kunna öka hotbilden. I rapporten beskrivs dock att ryska hotaktörer inte i någon större omfattning har genomfört cyberattacker mot västerländska banker sedan invasionen av Ukraina. Däremot kunde man tidigt 2023 se en ökning av överbelastningsattacker, i samband med Koranbränningarna, attacker som bland annat drabbade banker. Rapporten tar även upp risken för att bankerna utnyttjas i illegal verksamhet och bidrar till ytterligare säkerhetsproblematik, såsom finansiering av terrorism. Det finns starka incitament att placera en insider på en bank för att genomföra bedrägerier och/eller penningtvätt, vilket i och med det säkerhetspolitiska läget kan vara intressant även för statsaktörer.

4 Strukturreformen för krisberedskap och civilt försvar

I Försvarsberedningens rapport *Motståndskraft – inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025* identifierades en rad brister i den civila beredskapsstrukturen.[39] Med utgångspunkt i dessa, samt i att utveckling av det civila försvaret ska bygga på krisberedskapens processer, genomfördes strukturutredningen.[40] Utifrån utredningens betänkande trädde 2022 en myndighetsreform för civilt försvar och krisberedskap i kraft, för att bidra till:[41]

- ökad tydlighet kring roller och ansvarsfördelning
- stärkt motståndskraft i de viktigaste samhällsfunktionerna
- stärkt samverkan med det privata näringslivet
- förbättrade möjligheter till riktade geografiska insatser
- kraftsamling kring arbetet inför och vid höjd beredskap

Myndigheter med ansvar för viktiga samhällsfunktionerna, beredskapsmyndigheter, delas in i tio beredskapssektorer. Även samverkan inom geografiskt avgränsade områden förtydligas genom reformen. Sex civilområden utgör en högre regional nivå, med mellan två och sju länsstyrelser i varje. För varje civilområde utses en ansvarig länsstyrelse där landshövdingen

---

36 MSB (2023), Nationell-risk-och-sårbarhetsbedömningen

37 Behöriga aktörer, framför allt beredskapsmyndigheter, behöver dock involvera övriga relevanta aktörer i arbetet med att minska dessa sårbarheter på ett sätt som uppfyller informationssäkerhetskraven.

38 Svenska bankföreningen (2023), Hotbildsbedömning för Sveriges banker

39 Försvarsberedningen (2017), Ds (2017:66)

40 Regeringens webbplats Struktur för ökad motståndskraft - Regeringen.se och Dir. 2018:79, Ansvar, ledning och samordning inom civilt försvar

41 SOU 2021:25, Struktur för ökad motståndskraft

benämns civilområdeschef. Denne ska inrikta det civila försvaret inom det geografiska området samt samarbeta med Försvarsmakten för att säkerställa en enhetlig inriktning. Ansvar och uppgifter regleras framför allt i *förordning (2022:524) om statliga myndigheters beredskap* (”beredskapsförordningen”) och *förordning (2022:525) om civilområdesansvariga länsstyrelser*.

4.1 Beredskapsförordningen (2022:524)

Beredskapsförordningen beskriver myndigheters beredskapsansvar i tre nivåer; alla statliga myndigheter, beredskapsmyndigheter och sektorsansvariga myndigheter. Alla myndigheter ska inom det egna ansvarsområdet identifiera samhällsviktig verksamhet, analysera och minska sårbarheter och bedriva kontinuitetshantering. Arbetet ska omfatta såväl fredstida krissituationer som höjd beredskap. Analysarbetet ska vartannat år redovisas i en risk- och sårbarhetsanalys (RSA). Denna ska även omfatta de åtgärder myndigheten vidtagit och planerar för att minska sårbarheten mot identifierade hot och risker samt en övergripande bedömning av vilka övriga åtgärder som bör vidtas i samma syfte. Myndigheter ska även kunna bidra med information till samlade lägesbilder och bedriva ett adekvat informationssäkerhetsarbete. Förordningen tydliggör att ansvaret för kontinuitet och beredskap inte enbart gäller den egna verksamheten, utan för ansvarsområdet i stort, med dess olika ingående aktörer. Genom särskilda regeringsbeslut ska vissa myndigheter även ha en tjänsteman i beredskap för att initiera och samordna det inledande arbetet vid fredstida krissituationer respektive ha förmåga att vid behov omgående kunna upprätta en ledningsfunktion.

Förordningens bilaga 2 pekar ut 60 myndigheter med ett utökat beredskapsansvar, beredskapsmyndigheter, då de har ansvar inom viktiga samhällsfunktioner och har verksamhet av särskild betydelse för samhällets krisberedskap och totalförsvaret. För dessa ingår att vartannat år även göra en risk- och sårbarhetsbedömning och till regeringen, MSB och till den sektorsansvariga myndigheten lämna uppgifter om förmågehöjande åtgärder, vidtagna, planerade övriga som borde vidtas. Beredskapsmyndigheterna har även ett utökat ansvar att samverka inom systemet, såväl nationellt som internationellt, liksom att identifiera behov av forskning och utveckling, att bedriva övningsverksamhet och att säkerställa tekniska behov.

I förordningens bilaga 2 beskrivs även de tio beredskapssektorerna, med respektive sektorsansvarig myndighet med ytterligare uppgifter. De ska samordna åtgärder inför och vid fredstida krissituationer och höjd beredskap, såväl inom beredskapssektorn som med andra aktörer i systemet, inklusive näringslivet. En sektorsansvarig myndighet ska vid en kris kunna lämna underlag avseende läget i sektorn till regeringen och MSB, liksom om prioriteringar och resursfördelning. För närvarande pågår analys av hur respektive aktör ska omhänderta sitt ansvar och inrikta beredskapsarbetet.

Aktörerna i finansiell sektor återfinns framför allt i två beredskapssektorer; Finansiella tjänster och Ekonomisk säkerhet. Den förstnämnda består av Finansinspektionen och Riksgälden. Sektorn samarbetar även med Riksbanken. I Ekonomisk säkerhet ingår Försäkringskassan, Arbetsförmedlingen, Pensionsmyndigheten, Riksgäldskontoret, Skatteverket och Statens servicecenter. Finansinspektionen respektive Försäkringskassan är sektorsansvarig myndighet.

4.1.1 Tolkning av sektorsansvariga myndigheters roll, ansvar och mandat

MSB har gett Försvarshögskolans Centrum för totalförsvar och samhällets säkerhet (FHS/CTSS) i uppdrag att tolka sektorsansvariga myndigheters generiska roll, ansvar och mandat enligt beredskapsförordningen, vid fredstida kriser och höjd beredskap. Under arbetet har FHS samlat in synpunkter från aktörer inom beredskapssystemet och underlaget ska inte ses som slutgiltigt.

FHS konstaterar att förordningen utgör en tvärsektoriell och gemensam grund för statliga myndigheters beredskap och samlar huvuddelen av den myndighetsgemensamma regleringen i samma förordning.[42] En utmaning bedöms vara att de sektorsansvariga myndigheterna inte har givits mandat över andra myndigheter eller näringslivets aktörer. Beredskapsmyndigheter har dock en informationsskyldighet, medan samverkan med näringslivet behöver etableras på frivillig grund och förtroendebaserat. FHS bedömer att den stora informationsmängd som sektorsansvariga myndigheter kan få tillgång till ger en bra lägesbild för sektorn, som grund för inriktning, samordning och beslutsunderlag för till exempel resurs- och åtgärdsprioriteringar. Sammantaget bedöms sektorsansvaret skapa bättre förutsättningar att nå gemensamma mål och bidra till en stärkt gemensam beredskapsförmåga.

4.2 Utveckling av beredskapsförmåga

Olika underlag för stöd i utvecklingen av förmåga till civil beredskap har utformats. I de nedan beskrivna påpekas dock att arbetet behöver utvecklas och kompletteras allt eftersom.

4.2.1 Planeringsinriktning för civil beredskap

Våren 2023 gav MSB ut en remiss av en planeringsinriktning för att ge beredskapsmyndigheterna framför allt stöd i arbetet med att skapa en större motståndskraft och förmåga att förebygga och hantera olika samhällsstörningar. Stödet utgörs främst av utvecklingssteg inom fokusområden som MSB bedömer är viktiga för att skapa grundläggande förmåga och motståndskraft, med det väpnade angreppet som det dimensionerande scenariot. Områden utgår från beredskapsförordningen, den nationella risk-och sårbarhetsbedömningen, den samlade bedömningen av det civila försvarets förmåga samt de förslag till åtgärder för att stärka det civila försvaret som MSB redovisade till regeringen 2022.[43] Fokusområdena är:

- Samhällets funktionalitet och försörjning
- Personalförsörjning
- Samverkan och ledning
- Risk- och kriskommunikation
- Psykologiskt försvar
- Informations- och cybersäkerhet
- CBRNE (farliga ämnen)

[42] *Den är subsidiär till annan författning, vilket innebär att den är underordnad avvikande bestämmelser i annan lag eller förordning.*

[43] *MSB (2022), Civilt försvar mot 2030 – ett totalförsvar i balans*

Fokusområdena är en vidareutveckling av de som finns i *"Handlingskraft - Handlingsplan för att främja och utveckla en sammanhängande planering för totalförsvaret 2021-2025"*[44], men omhändertar även fredstida krissituationer.[45]

4.2.2 Planering för civil beredskap: process och metod

En utgångspunkt för den nya strukturen är att krisberedskapen och det civila försvaret ska förstärka varandra genom gemensamma processer för samordning, planering och förberedelse. MSB har i samverkan med olika myndigheter tagit fram *Vägledning - Planering för civil beredskap: process och metod*[46]. Vägledningen är tänkt att utgöra ett stöd för gemensam förmågeutveckling på kort och medellång sikt (ca 1–10 år). Vidare tillhandahåller MSB en inriktning för planeringen och anger önskad förmåga i de olika tidsperspektiven samt ger stöd i prioriteringar av åtgärder. Planeringen omfattar fem steg;

- Analys av ingångsvärden
- Identifiering av beredskapsåtgärder
- Prioriteringar (i dialog)
- Leverans av förslag på beredskapsåtgärder
- Uppföljning och fortsatt analys

Planeringsprocessen ska genomföras på tre nivåer, beredskapsmyndighet, beredskapssektor och nationell systemnivå:[47]

- Beredskapsmyndigheter ska ha en tioårsplan för det egna ansvarsområdet, med årliga uppdateringar. Planen samt ytterligare behov av åtgärder som myndigheterna inte kan ta hand om i den egna planeringen, lyfts till beredskapssektorsnivå.
- Beredskapsmyndigheternas planer aggregeras på sektorsnivå till en gemensam tioårsplan, som ska uppdateras årligen. Planen har fokus på prioritering och samverkansbehov inom sektorn, samt ytterligare behov av åtgärder som framkommer i den gemensamma planeringsprocessen.
- Dessa planer samt åtgärder som behöver hanteras systemövergripande delas med MSB. MSB gör även en egen analys och sammanställer ett nationellt systemunderlag som delas dels till regeringen, dels till beredskapsmyndigheterna. Underlaget ger en överblick över arbetsläget i planeringen. Det första underlaget avses lämnas till regeringen våren 2024.

Samverkan i planeringsarbetet ska ske såväl inom som mellan beredskapssektorerna. MSB föreslår bildande av planeringsgrupper med representanter från de ingående myndigheterna. Till dessa kopplas samverkansgrupper med representation från kommuner, regioner, privata företag, bransch- och intresseorganisationer, för inspel, synpunkter och samråd. MSB påpekar att behov och förutsättningar kommer att se olika ut i sektorerna, men att samverkan med privata aktörer behöver vara samordnad för att undvika krockar och onödig belastning. MSB ska ta initiativ till

---

[44] *Försvarsmakten och MSB (2021)*

[45] *I oktober 2023 kom den slutgiltiga versionen, som av tidsförhållanden inte kunnat omhändertas i denna PM. MSB (2023), Planeringsinriktning för civil beredskap.*

[46] *MSB (2023), Vägledning - planering för civil beredskap: process och metod*

[47] *I denna redogörelse beskrivs inte planeringen i det geografiska områdesperspektivet.*

och driva tre mötesformer för systemövergripande avstämning och konsolidering av planerade beredskapsåtgärder; handläggarmöte, chefsmöte för civil beredskap och myndighetschefsmöte.

MSB poängterar att då beredskapsarbetet genomgår stora förändringar kommer föreslagen process behöva utvecklas.

4.2.3 Utveckling av förmåga för krisberedskap och civilt försvar

FOI har på uppdrag av MSB undersökt behoven hos aktörer som ska utveckla civil beredskap, som grund för att utvecklar lämpligt stöd. FOI presenterade 2022 en studie för att svara på:[48]

- Vilket behov av stöd till förmågeutveckling avseende civilt försvar och krisberedskap ger myndigheter i systemet uttryck för?
- Vilka lösningar skulle kunna stödja myndigheternas arbete med förmågeutveckling?

Möjlighet att bedöma förmåga anges vara förutsättningar för att utveckla både krisberedskapen och det civila försvaret. I studien identifierades olika behov av stöd som myndigheter har för att dels kunna utveckla, dels kunna bedöma förmågan. Behoven identifierades genom intervjuer med representanter för tolv bevakningsansvariga myndigheter och delades in i kategorierna inriktning, planering, genomförande, uppföljning och värdering samt övergripande behov. Avseende lösningsförslag konstateras att det inte finns en perfekt modell som svarar mot alla behov. Det krävs därför att förmågeutvecklande arbete bedrivs parallellt med att metoder och arbetssätt utvecklas.

4.3 Samhällsviktig verksamhet i finansiell sektor

En av myndigheternas grundläggande uppgifter enligt beredskapsförordningen är att identifiera vilka verksamheter inom ansvarsområdet som ä att betrakta som samhällsviktiga. I FSPOS-rapporten *Perspektiv på samhällsviktig verksamhet inom finansiell sektor* från 2022 finns resonemang kring hur processerna för identifiering av verksamhet under säkerhetsskyddslagstiftningen respektive NIS-direktivet kan bidra till identifieringen av samhällsviktig verksamhet.[49] MSB:s föreskrifter avseende NIS-direktivet pekar i kapitel 5 ut vilka betaltjänster som tillhandahålls av kreditinstitut som omfattas, medan kapitel 6 beskriver tjänster rörande finansmarknadsinfrastruktur.[50] I betänkandet *Näringslivets roll inom totalförsvaret* lyftes utöver dessa även risk- och sårbarhetsanalyser (RSA) ut som ett verktyg för identifiering.[51]

MSB uppdaterade under 2023 listan med exempel på vilka viktiga samhällsfunktioner som ingår i olika beredskapssektorer.[52] För beredskapssektorn Finansiella tjänster har betalningsförmedling, finansiell stabilitet, försäkring samt sparande, finansiering och finansiell riskhantering identifierats. För varje viktig samhällsfunktion anges exempel på samhällsviktig verksamhet som upprätthåller eller säkerställer den viktiga samhällsfunktionen. Exempel på samhällsviktig verksamhet som upprätthåller eller säkerställer den viktiga samhällsfunktionen betalningsförmedling är det centrala betalningssystemet, elektroniska betaltjänster och kontanthantering.

---

[48] *Olsén mfl (2022), Utveckling av förmåga för krisberedskap och civilt försvar, FOI-R--5287--SE*

[49] *Läs mer i FSPOS (2022), Perspektiv på samhällsviktig verksamhet inom finansiell sektor*

[50] *MSBFS (2021), Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer r av samhällsviktiga tjänster, 2021:9*

[51] *SOU 2019:51*

[52] *Se exempel (MSB2023), Identifiering av samhällsviktig verksamhet: Lista med viktiga samhällsfunktioner*

Finansinspektionen samverkar nu med Riksbanken, Riksgälden och ett urval av sektorns privata aktörer för att närmare definiera vilken verksamhet som bör vara att betrakta som samhällsviktig. Enligt Finansinspektionens uppfattning är det lämpligt att beskriva den samhällsviktiga verksamheten i termer av de produkter och tjänster som de finansiella företagen erbjuder till sina kunder, till gagn för övriga delar av det finansiella systemet och icke-finansiella företag, konsumenter och det offentliga. Arbetet utförs i form av en kartläggning av sektorns ansvarsområde som beskriver de produkter och tjänster som tillhandahålls, men utan att i detalj beskriva hur den verksamhet som bedrivs inom sektorn fungerar. Produkterna och tjänsterna kommer därefter kategoriseras utifrån de viktiga samhällsfunktionerna, betalningsförmedling, sparande, finansiering och finansiell riskhantering, försäkring samt finansiell stabilitet. Fördjupade analyser i syfte att identifiera vilka risker och sårbarheter som är förknippade med verksamheterna kommer genomföras, liksom vilka förmågehöjande åtgärder som kan vidtas.[53]

För Ekonomisk säkerhet är utbetalningar av statliga ersättningar och finansiering av offentlig verksamhet samhällsviktiga funktioner. Den första handlar bland annat socialförsäkringar, arbetslöshetsförsäkring, pensioner, pensionsrelaterade förmåner och försvarsförmåner. Funktionen omfattar hela kedjan från handläggning och utredning till beslut och utbetalning. Den andra funktionen handlar om finansieringen av offentlig verksamhet genom att fastställa och ta in skatter och avgifter. Jämfört med i sektorn Finansiella tjänster utförs mycket av den samhällsviktiga verksamheten av myndigheter. Utöver samverkan med myndigheterna inom sektorn Ekonomisk säkerhet behöver Försäkringskassan samverka med sektorsansvariga myndigheter för sektorerna Grunddata och Finansiella tjänster, det vill säga Skatteverket och Finansinspektionen. Flera åtgärder för att etablera sådan samverkan har genomförts och arbetet kommer att fortsätta.[54]

Försäkringskassan och övriga myndigheter i sektorn Ekonomisk säkerhet fokuserade under 2022 på områden som är centrala för det fortsatta arbetet; säkerhetsskydd, informationsdelning och strukturer för att ta fram och utbyta lägesbilder. [55] Tillsammans med myndigheterna i sektorn har Försäkringskassan genomfört ett antal åtgärder för att identifiera sårbarheter och stärka förmågan att upprätthålla funktionerna, bland annat genom deltagande i de övningar som Försvarsmakten och MSB arrangerade under 2023 i syfte att pröva förmågan till lägesbildsdelning och rapportering under höjd beredskap.[56]

Erfarenhetsutbyte har skett rörande hur myndigheterna i sektorn arbetar med långsiktig förmågeplanering och ett arbete med att ta fram ett gemensamt ramverk för detta är påbörjat. Vidare har myndigheterna i sektorn träffat överenskommelser med varandra rörande inriktning och former för samarbete och samverkan inom sektorn.

Ett par förändringar kommer med stor sannolikhet att påverka krisberedskapsarbetet i sektorn. Nästa år bildas Utbetalningsmyndigheten, som bland annat ska ansvara för att genomföra utbetalningar av förmåner och stöd från de anslutna statliga välfärdssystemen, samt utbetalningar från skattekontot hos Skatteverket. Ansvaret gäller även vid fredstida kriser och under höjd beredskap.[57] Utbetalningsmyndigheten kommer sannolikt att ingå i

---

[53] *Personlig kontakt med handläggare på Finansinspektionen*

[54] *Enligt korrespondens med handläggare på Försäkringskassan.*

[55] *Försäkringskassan (2022), Årsredovisning 2022*

[56] *Enligt korrespondens med handläggare på Försäkringskassan.*

[57] *Finansdepartementet (2022), kommittédirektiv 2022:8. Slutredovisning senast 31 december 2023*

beredskapssektorn Ekonomisk säkerhet. Vidare pekade coronapandemin på vikten av beredskap också i arbetslöshetsförsäkringen, då många människor plötsligt stod utan inkomst. Kommunernas system för försörjningsstöd var inte dimensionerat för den volymen människor som behövde stöd. En särskild utredare ser nu över regelverket för arbetslöshetsförsäkringen och arbetslöshetskassornas deltagande i arbetet med civil beredskap, så att arbetslöshetsförsäkringen ska fungera vid störda förhållanden, allvarlig fredstida kris, höjd beredskap och ytterst krig.[58][59]

4.4 En modell för svensk försörjningsberedskap

2021 tillsattes en utredning för att analysera och föreslå en funktion med ansvar för nationell samordning av försörjningsberedskapen. I betänkandet som kom sensommaren 2023 föreslås framtagande av försörjningsanalyser för att ge en samlad kunskap om Sveriges försörjningsförmåga i olika krissituationer.[60] Första steget skulle vara att göra behovsanalyser i fredstida krissituationer och vid höjd beredskap. Detta innefattar identifiering av försörjningsviktiga varor och tjänster, liksom av företag som bedriver samhällsviktig respektive totalförsvarsviktig verksamhet. I nästa steg måste behoven ställas mot tillgången i dessa situationer, för att kunna identifiera behov av åtgärder. Försörjningsviktigt avser sådant som är nödvändigt för att säkerställa de viktigaste samhällsfunktionerna, befolkningens överlevnad eller som bidrar till det militära försvarets förmåga.

Utredningen föreslår att uppgiften regleras i beredskapsförordningen och att de sektorsansvariga myndigheterna även blir försörjningsanalysmyndigheter. Då kunskap om de företag som producerar eller levererar dessa försörjningsviktiga varor och tjänster är central anser utredningen att beredskapsmyndigheterna ska ges uppgiften att identifiera företag som bedriver samhällsviktig verksamhet inom respektive ansvarsområde. I betänkandet föreslås att arbetet ska utgå från strukturreformens myndighetsstruktur, dock begränsad till beredskapssektorerna Elektroniska kommunikationer och post, Energiförsörjning, Finansiella tjänster, Hälsa, vård och omsorg, Livsmedelsförsörjning och dricksvatten, samt Transporter. Utgångspunkten för utpekandet av Finansiella tjänster är att en fungerande betalningsförmedling är avgörande för att säkerställa flödet av varor och tjänster som är av betydelse för att upprätthålla samhällsviktiga funktioner.

En särskild utmaning identifieras för beredskapssektorn Finansiella tjänster. Riksbanken skulle i praktiken behöva utföra stor del av arbetet, men omfattas inte av förordningen.[61] Det innebär dels att vare sig Finansinspektionen eller regeringen kan kravställa att Riksbanken utför analyserna, dels att de åtgärdsförslag som genereras inte har någon självklar mottagare, då det är riksdagen som skulle behöva besluta om åtgärder. Riksbanken arbete skulle med liggande förslag inte vara reglerat, med risken att det inte kan tillägnas tillräckligt med resurser.

---

[58] *Arbetsmarknadsdepartementet (2023), kommittédirektiv 2023:76. Uppdraget ska redovisas senast den 30 juni 2024*

[59] *Försäkringskassan svarade under 2022 på regeringsuppdraget att säkerställa utbetalningar från socialförsäkringen under krig och krigsfara (S2022/01531)*

[60] *SOU 2023:50, En modell för svensk försörjningsberedskap,*

[61] *Riksbanken ska enligt den nya riksbankslagen hålla regeringen och Riksgäldskontoret underrättade om viktigare frågor, men det gäller enbart under fredstida krissituationer och vid höjd beredskap.*

5 Beredskap avseende betalningar

Funktionen betalningar handlar om ersättning för varor och tjänster, utbetalning av löner och sociala förmåner. Att kunna genomföra betalningar är avgörande för samhällets funktionalitet och beredskap för att kunna upprätthålla betalningsekosystemet också vid störningar har ägnats uppmärksamhet de senaste åren.

5.1 Riksbankslag (2022:1568)

I januari 2023 trädde en ny riksbankslag i kraft, *lag (2022:1568) om Sveriges riksbank*. Enligt kapitel 5 ska Riksbanken planera och förbereda för att kunna upprätthålla sin verksamhet under fredstida krissituationer och vid höjd beredskap, vilket inbegriper allmänhetens möjlighet att göra betalningar. Dessutom uttrycks ansvar och befogenheter gentemot företag som bedriver verksamhet som är av särskild betydelse för genomförandet av betalningar. Riksbanken ska säkerställa att dessa företag deltar i Riksbankens planering och förberedelser samt i av Riksbanken anordnad övning och utbildning, men ska även övervaka att företagen uppfyller sina övriga skyldigheter enligt lagen. Det handlar om att de ska planera och förbereda för att kunna fortsätta verksamhet som avser betalningar under fredstida kriser och höjd beredskap och även själva tillse att arbets- och uppdragstagare får den utbildning och övning som behövs.

I kapitel 13 ges Riksbanken föreskriftsrätt att identifiera vilka företag som ska omfattas och vilken verksamhet de ska delta i. Förslag till föreskrifter har varit ute på remiss under 2023 och ska träda i kraft i början av 2024. Föreskrifterna preciserar kriterier för företag som omfattas, i termer av typ av företag och i vissa fall hur omfattande verksamheten ska vara. I förslaget ställs krav på att företagen ska planera och förbereda för att kunna upprätthålla den del av företagets verksamhet som avser betalningar under fredstida krissituationer och vid höjd beredskap. Företagen ska även bedriva utbildnings- och övningsverksamhet, liksom delta i Riksbankens arbete med civil beredskap för betalningar.[62] Bankföreningen har lämnat ett remissvar där de framhåller att de praktiska konsekvenserna inte är tillräckligt utredda och att föreskrifterna behöver förtydligas. Bankföreningen påtalar utmaningen för bankerna med många regleringar avseende säkerhet, beredskap och resiliens, såväl på EU-nivå som nationellt. Det riskerar att medföra att fokus i bankernas arbete blir uttolkning, kartläggning och rangordning av olika regelverk, snarare än praktiskt orienterad verksamhet för att stärka Sveriges beredskap.[63]

5.2 Staten och betalningarna

Betalningsutredningen lämnade våren 2023 betänkandet *Staten och betalningarna*.[64] Uppdraget var att se över och föreslå statens roll på betalningsmarknaden, sett bland annat till hur finans- och betalningsmarknaderna förändrats med den tekniska utvecklingen. Utredningen konstaterar att betalningssystem och -infrastruktur är kritiska funktioner för vilka staten behöver ta ett större ansvar.

Kapitel 11 ägnas åt civil beredskap. Utredningen redogör för tre förutsättningar som påverkar beredskapen; ansvarsfördelningen, internationaliseringen av betalningsekosystemet[65] samt det

---

[62] *I skrivande stund har Riksbanken inte beslutat om slutlig version av föreskrifterna.*

[63] *Svenska bankföreningen (2023), REMISSYTTRANDE Bankföreningens synpunkter på Riksbankens föreskrifter om civil beredskap för betalningar, 2023/06/001*

[64] *SOU 2023:16*

[65] *I betänkandet används termer för att beteckna det system som uppstår då nya sätt att betala och nya aktörer utvecklas och kopplas till varandra.*

kritiska beroendet av el och elektroniska kommunikationer. Utredningen konstaterar att det potentiellt finns svårigheter med att bedriva ett effektivt krisberedskapsarbete, när ansvaret är utspritt på flera myndigheter. Utredningen bedömer att Finansinspektionens respektive Riksbankens delvis överlappande beredskapsuppdrag kan leda till otydlighet gentemot andra aktörer, inte minst de företag som ska medverka i övning och planering. De förändringar i ansvarsförhållanden, uppgifter och befogenheter avseende beredskap på betalningsområdet som införts ger förvisso berörda myndigheter bättre förutsättningar att leda det förebyggande arbetet samt att agera snabbare och kraftfullt i kriser, men utredning anser att ytterligare tydliggörande av ansvarsförhållandena krävs. Utredningen efterfrågar också ändamålsenliga former för samverkan, särskilt när det gäller operativ krishantering. Utredningen lyfter möjligheten att Riksbanken åläggs i lag att samråda med eller informera Finansinspektionen under kriser och krig. Vidare behöver regelverk och tillsyn utformas så att en god krisberedskap kan säkerställas även då utländska aktörer tillhandahåller tjänster. Den tredje förutsättningen kräver god elberedskap, hög driftsäkerhet och cybersäkerhet.

Utredningens utgångspunkter är att krav behöver ställas på olika aktörer, staten såväl som institut och att insatser krävs på olika nivåer och i samverkan. Det ska finnas redundans avseende sätt att betala. Betalningssystem och -infrastruktur behöver vara robusta och kunna motstå störningar. Utredningen föreslår regeljusteringar för ökad tydlighet att företag kan ta emot kontant betalning utan att bryta mot lagen vid stora störningar.[66] Staten bör vidare garantera att digitala betalningar vid köp av livsnödvändiga varor kan genomföras off-line, om elektroniska kommunikationer inte fungerar i kris och krig. En sådan garanti ska avse kreditrisken för likviditetslån till näringsidkare. Utredningen föreslår därför en ny lag som reglerar förutsättningar och villkor för statliga kreditgarantier.

5.3 En ny lag om clearing och avveckling av betalningar

Finansdepartementet gav i promemorian *Ökad motståndskraft i betalningssystemet* 2022 förslag på en ny lag om clearing och avveckling av betalningar.[67] En ny lag behöver omhänderta de stora förändringarna på betalningsmarknaden med snabbt ökade digitalisering och en ökad utkontraktering av infrastrukturtjänster till leverantörer, i synnerhet sådana som inte omfattas av finansiell reglering och tillsyn. Lagstiftningen behöver även harmonisera med internationella lagändringar. Då även kortvariga störningar i betalningssystemet riskerar att få stora konsekvenser för samhället och längre avbrott dessutom kan innebära risk för störningar av den finansiella stabiliteten behöver den nya lagen ställa krav på bland annat riskhantering, beredskap och cybersäkerhet.

Lagrådsremissen kom i maj 2023 och det förslagna reglerna föreslås träda i kraft 1 januari 2024.[68] Clearingbolag ska

- identifiera, mäta, övervaka, internt rapportera och hantera risker (operativa risker och affärs-, investerings-, kredIT- och likviditetsrisker). Det ska också finnas en tillfredsställande intern styrning och kontroll och bolaget ska säkerställa driftsäkerhet,

[66] *Skatteverket föreslås få bemyndigande enligt 39 kap. 10 § skatteförfarandelagen (2011:1244)*

[67] *Finansdepartementet (2022), Ökad motståndskraft i betalningssystemet*

[68] *Regeringen (2023), Lagrådsremiss Nya regler för clearingorganisationer*

inbegripet förmågan att hantera ökande betalningsvolymer till följd av operativ eller finansiell påfrestning.

- identifiera kritisk verksamhet och säkerställa att verksamheten kan återupptas inom kort efter ett avbrott. De ska också ha beredskaps- och kontinuitetsplaner, som ska utvärderas regelbundet.
- ha strategier för informations-, IT- och cybersäkerhet för att kunna hantera risker, hot och sårbarheter. Strategierna ska utvärderas och ses över regelbundet.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter avseende ovanstående områden.

6 Natos arbete med civil beredskap

Vid denna PM:s skrivande är ett svenskt medlemskap i Nato inte klart. Sverige har dock under närmare 30 år deltagit i Natos samarbetsprogram *Partnerskap för fred* (PFF) och sedan ungefär ett decennium även i ett individuellt partnerskap, *Enhanced Opportunites Partner* (EOP). Genom detta förs politiska dialoger och fördjupat samarbete i frågor av gemensamt intresse, exempelvis kring övning, utbildning och informationsutbyte kring aktuella händelser. Ett senare initiativ är One *Partner One Plan* (OPOP), för ett effektivt partnerskap utifrån varje lands förutsättningar.

6.1 Samarbete kring civil beredskap

Inledningsvis fokuserade PFF-samarbetet på militära aspekter, men utvecklades senare till att även omfatta även civila beredskapsfrågor. Det svenska deltagandet regleras avseende inriktning och arbetsformer av regeringen i raminstruktioner, den senaste från 2021.[69] Prioriterat för svenska myndigheter som deltar är att beakta utvecklingen av civilt försvar som en del av totalförsvaret, civil beredskapsplanering i relation till det svenska värdlandsstödavtalet med Nato och att utveckla samarbete i utformning och genomförande av övningar.

Civil Emergency Planning Committee (CEPC) är Natos högsta organ för civila beredskapsfrågor. CEPC är sammanhållande inom Nato för bland annat civil beredskapsplanering, skydd av samhällsviktiga funktioner, civilt stöd vid omfattande olyckor och kriser samt Natos hantering av hybrid- och terrorhot. Under CEPC verkar sex planeringsgrupper, där relevanta svenska myndigheter är representerade. Dessa hanterar frågor avseende energi, transport, hälsa, livsmedel och jordbruk, hälsa, civila kommunikationer och civilskydd. MSB har en samordnande funktion.

Finansiella sektorns myndigheter ingår inte i någon planeringsgrupp, men de aktörer som tar emot officiella dokument har ett ansvar att på lämpligt sätt sprida dessa till övriga aktörer som bedöms relevanta.

[69] *Justitiedepartementet (2021), Raminstruktion för det svenska civila beredskapsarbetet inom ramen för Nato/PFF, Ju2021/00361*

6.2 *Baskrav för resiliens*

Nordatlantiska fördraget utgör Natos grund och i artikel 3 åtar sig parterna att, var för sig och tillsammans, genom egen beredskap och ömsesidigt bistånd, upprätthålla och utveckla sin individuella och kollektiva förmåga att stå emot väpnade angrepp. Begreppet resiliens används för att beskriva att medlemsländerna behöver vara robusta och flexibla för att kunna hantera hela spektrumet av kriser och samtidigt minska Natos sårbarhet.

Det civila beredskapsarbetet tydliggörs i sju civila förmågor, så kallade baseline requirements for national resilience, som ska bidra till att upprätthålla alliansens samlade försvarsförmåga:[70]

- säkerställande av politiskt beslutsfattande och centrala ledningsfunktioner,
- resilient energiförsörjning,
- effektiv hantering av okontrollerade stora befolkningsrörelser,
- resilienta system för livsmedels- och dricksvattenförsörjning,
- hantering av stora masskadeutfall,
- resilienta civila kommunikationssystem och
- resilienta transportsystem

Dessa förmågor är centrala också i det svenska arbetet för en stärkt civil beredskap. Även om finansiella tjänster och ekonomisk säkerhet inte explicit uttrycks är de en förutsättning för flera av de andra förmågorna, enligt vad som framhålls i kapitel 5 om betalningar.

7 IT-, informations- och cybersäkerhet

Cyberangrepp mot svenska intressen pågår ständigt, av olika aktörer, drivet av olika motiv. Det finns stora mängder information och IT-system som är av avgörande betydelse för samhällets funktionalitet och säkerhet. Störningar i funktionaliteten hos IT-system kan få allvarliga följder för samhällsviktig verksamhet, inte minst avseende finansiella tjänster som i hög grad är digitaliserade. Cybersäkerhet har således gått från att ha varit en teknisk angelägenhet till att vara av stor betydelse för fred och säkerhet.

Informations- och cybersäkerhet måste därför vara en självklar och integrerad del på alla nivåer i finansiell sektor. Då den tekniska utvecklingen sker snabbt behöver säkerhetsarbetet också utvecklas kontinuerligt. För att inrikta arbetet finns såväl stödfunktioner som lagstiftning, av vilka de mest tongivande beskrivs nedan.

7.1 *Offentliga initiativ till stöd för ökad cybersäkerhet*

7.1.1 Nationell strategi för samhällets informations- och cybersäkerhet

I den nationella strategin för samhällets informations- och cybersäkerhet från 2017 uttrycks regeringens övergripande prioriteringar och målsättningar. Strategin avsåg bidra till att skapa långsiktiga förutsättningar för samhällets aktörer, offentliga såväl som privata, att arbeta effektivt med informations- och cybersäkerhet.[71]

I Riksrevisionen granskningsrapport, *Regeringens styrning av samhällets informations- och cybersäkerhet* (RiR 2023:8) konstateras att regeringens arbete med att stärka informations- och cybersäkerheten inte är effektivt, dels beroende på brister i den nationella informations- och

[70] *Natos webbplats, NATO - Topic: Resilience, civil preparedness and Article 3, hämtad 231101*

[71] *Justitiedepartementet (2016), Nationell strategi för samhällets informations- och cybersäkerhet, Skr. 2016/17:213*

cybersäkerhetsstrategin, dels på att regeringens styrning är svag och splittrad. För att staten på bästa sätt ska kunna stödja arbetet med informations- och cybersäkerhet bör en långsiktig och holistisk inriktning tas fram, som beskriver avvägningar, prioriteringar, resurstilldelning och en handlingsplan, som involverar berörda intressenter. En förutsättning för att arbetet ska fungera effektivt är att det finns strukturer för informationsutbyte mellan aktörer. Sverige behöver även påverka arbetet i och gentemot EU, ett arbete som bedrivs i hög takt. Risken är annars att svenska intressen inte gynnas i samma utsträckning som annars hade varit möjligt.[72]

Under hösten 2023 inledde regeringen arbete med att ta fram en ny strategi. Den ska ses som en del av implementeringen av NIS2-direktivet (avsnitt 7.2.2) och ge förutsättningar för att knyta ihop satsningar nationellt, inom EU och inför ett svenskt Natomedlemskap. Stöd till, och samverkan mellan, det offentliga och det privata utgör en central fråga. I framtagandet deltar ett 50-tal aktörer, myndigheter och bransch- och intresseorganisationer.

7.1.2 Nationellt cybersäkerhetscenter (NCSC)

FRA, Försvarsmakten, MSB och Säkerhetspolisen har fått regeringens uppdrag att driva det nationella cybersäkerhetscentret. Det görs i nära samverkan med PTS, Polismyndigheten och FMV. Verksamheten ska stärka hela Sveriges förmåga att förebygga, upptäcka och hantera cyberhot. Bland annat ska NCSC arbeta med koordinering, rådgivning och erbjuda en plattform för samverkan för en bred mängd aktörer i cybersäkerhetsfrågorna. Den tänkta effekten är ökad effektivitet i arbetet att möta cyberhoten. Riksrevisionens granskningsrapport (se ovan) beskriver att NCSC tagit lång tid att bygga upp och att ansvarsfördelningen mellan flera myndigheter gör att verksamheten är svår att inrikta och följa upp. Det konstateras vidare att privat näringsliv inte inkluderats tillräckligt. Regeringen har därför tillsatt en utredning om att ge FRA ett huvudansvar för NCSC:s organisation och styrning.[73]

Hösten 2022 startades ett pilotprojekt inom NCSC som går ut på privat-offentlig samverkan med finansiell sektor i form av *NCSC Finansforum*. Under hösten 2023 avslutades pilotprojektet och övergick i permanent verksamhet. Forumet ska främja ökat informationsutbyte mellan aktörer för att stärka cybersäkerheten i sektorn. Aktörerna i forumet arbetar med att främja samverkan och informationsdelning, planering av kommunikation internt och externt samt medverkar vid FSPOS Sektorsövning 2023, med fokus på cyberhändelser i en gråzonssituation.

Under 2023 fick ansvariga myndigheter ett förtydligat uppdrag att sprida information till näringslivet om NCSC:s roll samt att etablera samverkan med energisektorn, telekomsektorn och transportsektorn. I detta arbete kommer erfarenheterna från NCSC Finansforum att tillvaratas.[74]

7.1.3 Infosäk- respektive IT-säkkollen

För att stödja näringslivet i informationssäkerhetsarbetet gav regeringen våren 2023 MSB i uppdrag att utvidga sin struktur för uppföljning av systematiskt informationssäkerhetsarbete, Infosäkkollen, till det privata näringslivet. Infosäkkollen är ett verktyg för att erbjuda en struktur för uppföljning för att förbättra aktörers förmåga att arbeta med informations- och cybersäkerhet.

---

[72] *Regeringen (2023), Regeringens skrivelse 2023/24:26 Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet*

[73] *Regeringen (2023), Regeringens skrivelse 2023/24:26 Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet*

[74] *NCSC (2023), Delredovisning av regeringsuppdrag: Uppdrag att inom ramen för Nationellt cybersäkerhetscenter stärka samverkan med näringslivet*

Därigenom ska aktörerna kunna avgörs om deras informations- och cybersäkerhet behöver förstärkas och i så fall även hur. Infosäkkollen ska kunna erbjudas främst de aktörer som omfattas av *lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänste*r och det nyligen antagna NIS2-direktivet.[75]

2023 introducerades även IT-säkkollen, en undersökning av en organisations IT-säkerhetsåtgärder. MSB beskriver att undersökningen kommer vidareutvecklas för att genomföras i full skala 2025. De svar som samlas in bidrar dels till den nationella lägesbilden, dels till regeringens nya informations- och cybersäkerhetsstrategi.[76]

7.2 Nya regelverk

Utifrån den förändrade hotbilden och de ökande behoven av att stärka motståndskraften mot cyberhot, i synnerhet i samhällsviktiga verksamheter, ses också lagstiftningen över. Kraven på aktörer att arbeta för att höja motståndskraften ökar stadigt och EU har antagit flera nya direktiv och förordningar som kommer att beröra de flesta aktörer i finansiell sektor på ett eller annat sätt.

Tre nya regleringar som är relevanta för finansiell sektor att bevaka är *Digital Operational Resilience Act* (DORA), *Critical Entities Resilience Directive* (CER) och *Directive on Security of Network and Information Systems* (NIS 2). Det övergripande syftet är att stärka resiliensen i EU i flera olika bemärkelser, så som cyberresiliens, operationell resiliens och fysisk resiliens. EU har antagit dessa som ett paket och de är tänkta att komplettera varandra. Medan NIS2 och CER är generella riktar sig DORA till specifikt mot det finansiella systemet. CER har en tillämpning även utöver cyberdomänen, men återges ändå i detta kapitel, då regleringarna behandlas som ett paket. Utkontraktering av tjänster omfattas av DORA-förordningen, men nedan beskrivs även ett par andra regelverk, även om de egentligen också har en tillämpning utöver cyberdomänen.

MSB har tagit fram en policyöversikt av pågående initiativ på EU-nivå som Sverige behöver förhålla sig till med särskilt fokus på informations- och cybersäkerhetsområdet.[77] Dokument kommer löpande att uppdateras för att följa utvecklingen av EU-initiativen och vid behov kompletteras med ytterligare regelverk. I denna tas även EU:s kommande regelverk avseende artificiell intelligens upp.

7.2.1 DORA: Digital Operational Resilience Act

Förordningen om digital operativ motståndskraft för den finansiella sektorn, den så kallade DORA-förordningen, trädde i kraft i början av 2023. Den syftar till att säkerhet i nätverk och informationssystem som stöttar affärsprocesser inom finansiell sektor upprätthålls. Aktörer verksamma inom finanssektorn, men även kritiska tredjepartsleverantörer och molntjänstleverantörer, berörs. DORA innebär högre krav på bland annat hur man detekterar, skyddar mot och förebygger angrepp, att man har kontinuitetsplaner på plats och att man har tillgång till backuper och metoder för att återställa information. Kraven på testning av digital motståndskraft ökar också.

Bolag som berörs har fram till början av 2025 att uppfylla kraven. EU:s finansiella tillsynsmyndigheter (ESA) får befogenhet att begära information, utföra inspektioner samt

---

[75] *Regeringens webbplats, Regeringen uppdrar till MSB att erbjuda effektivare informationssäkerhetsarbete till näringslivet - Regeringen.se, hämtad 231103*

[76] *MSB:s webbplats, Infosäkkollen (msb.se), hämtad 232202*

[77] *MSB (2023), Policyöversikt: Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete*

utfärda rekommendationer, administrativa sanktioner och avhjälpande åtgärder för identifierade kritiska tredjeparter. Lokala tillsynsmyndigheter kommer att utöva tillsyn över de finansiella företag som omfattas av reglerna i respektive medlemsstat.

MSB uttalar sig i policyöversikten om att regelverket kommer driva den finansiella sektorn att identifiera motståndskraft för kritiska funktioner och underliggande processer. Detta kommer att bidra till sektorns robusthet, resiliens och redundans på det digitala området - och därmed till svensk beredskap. Den nya regleringen kommer innebära en närmare samverkan inom Europa och mellan leverantörer, vilket stärker en gemensam europeisk säkerhet på marknaden. ESA bedöms behöva ta ett större ansvar, till exempel gentemot IKT tredjepartsleverantörer.[78]

7.2.2 CER och NIS2

Syftet med *Critical Entities Resilience Directive*, CER-direktivet är att öka den fysiska motståndskraften i samhällsviktig verksamhet. Direktivet går ut på att medlemsstaterna ska identifiera kritiska entiteter inom utpekade sektorer (däribland bankverksamhet och finansmarknadsinfrastruktur) som tillhandahåller samhällsviktiga tjänster. De utpekade aktörerna åläggs att stärka sin motståndskraft mot samhällsstörningar generellt, och inte bara cyberrelaterade händelser. Aktörerna ska även rapportera incidenter. Direktivet anger också att medlemsstaterna ska ta fram en nationell strategi för kritiska entiteters motståndskraft. Det ställs även krav på nationella risk- och sårbarhetsanalyser.[79]

För att ytterligare stärka skyddet av samhällsviktiga tjänster har EU också beslutat att uppdatera det tidigare NIS-direktivet. NIS2 höjer kraven på aktörer och dess leverantörskedja, incidentrapportering, skyddsåtgärder mot cyberhot i förebyggande syfte och nya krav på att utföra riskbedömningar. NIS2 innebär även en utökning av vilka sektorer som omfattas och dessa sektorer delas in i högkritiska och kritiska. Finansiella tjänster räknas som en högkritisk sektor. Bankverksamhet och finansmarknadsinfrastruktur, såsom kreditinstitut, operatörer av handelsplatser och centrala motparter omfattas, utöver leverantörer av sådana tjänster som sektorn är beroende av (exempelvis molntjänster och elektroniska kommunikationsnät). Varje aktör ska själv identifiera om det omfattas av NIS-direktivet, och i så fall anmäla detta till Finansinspektionen som är tillsynsmyndighet.[80] NIS2 möjliggör även ansvarsutkrävning för ledningsgrupper och större sanktionsavgifter i de fall organisationer inte lever upp till kraven.

Som direktiv behöver NIS2 och CER implementeras i svensk lag och utredning hur detta ska ske pågår. De lagar som berörs är lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, säkerhetsskyddslagstiftningen och lagen (2003:389) om elektronisk kommunikation. Uppdraget ska redovisas senast den 23 februari 2024 och senast 18 oktober 2024 ska de nya direktiven vara införlivade i svensk lagstiftning. Utredaren ska även bland annat föreslå hur identifieringen av och krav på entiteter som omfattas ska regleras och föreslå hur rollfördelningen mellan svenska myndigheter ska se ut. Kritiska entiteter enligt CER ska även anses vara väsentliga entiteter enligt NIS2. Vidare bör de behöriga myndigheterna enligt respektive direktiv utbyta information med varandra om hot och incidenter samt om åtgärder som myndigheterna vidtar. Mot denna bakgrund är en naturlig utgångspunkt att samma myndighet som utövar tillsyn över en viss entitet enligt NIS2-direktivet även utövar tillsyn över

---

[78] *MSB, 2023. Policyöversikt: Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete*

[79] *EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG*

[80] *FSPOS (2022), Perspektiv på samhällsviktig verksamhet inom finansiell sektor*

entiteten enligt CER-direktivet. MSB har utpekats som en lämplig nationell kontaktpunkt för CER och NIS2.

Enligt kommittédirektivet ska sektorsspecifika unionsrättsakter, som DORA, beaktas.[81] DORA är lex specialis och har därmed företräde över NIS2 som den mer specifika regleringen.[82] Bankföreningen har i en framställan till utredningen efterfrågat att det tydligt klargörs att berörda bestämmelser i NIS2-direktivet och CER-direktivet inte ska tillämpas för banker som omfattas av DORA-förordningen. [83] Bankföreningen hänvisar till *Kommissionens riktlinjer för tillämpningen av artikel 4 (1) och (2) i direktiv EU 2022/255 (NIS2-direktivet)*[84], där det framgår att medlemsstaterna inte ska tillämpa bestämmelserna i NIS 2-direktivet på finansiella entiteter som omfattas av DORA-förordningen. Liksom i remissvaret avseende riksbankslagen (avsnitt 5.1) ser Bankföreningen utmaningar för bankerna när allt fler regleringar gäller för samma område, inriktade på säkerhet, beredskap och motståndskraft. Det riskerar att tyngdpunkten i arbetet läggs på uttolkning av terminologi och rangordning av olika regelverk, snarare faktiska åtgärder för att stärka motståndskraften. Dessutom riskerar regleringen kring incidentrapportering till myndigheter att fortsatt vara komplicerad när en enskild incident kan initiera en mängd olika incidentrapporteringsprocesser, med olika mottagande myndigheter, terminologi och definitioner, tröskelvärden och mallar. Bankföreningen menar att det därmed är av vikt att liknande aktiviteter inte kommer att omfattas av flera olika regelverk.

7.2.3 Krav vid utkontraktering

Krav avseende utkontraktering är egentligen inte begränsade till att omfatta IT-, informations- eller cybersäkerhet, men bedöms ändå utgöra en så pass stor del av utmaningen att de beskrivs i detta kapitel.

Betalningsutredningen påtalar i kapitel 10 vikten av ändamålsenlig reglering och procedurer för att upptäcka och åtgärda störningar, för att undvika att utkontraktering av betalningsinfrastruktur leder till förhöjda risker, förlust av data, brister i kontinuitet med mera. Utöver den ovan beskrivna DORA-förordningen finns några andra regelverk att beakta avseende utkontraktering.

2019 trädde den Europeiska bankmyndighetens (EBA:s) Riktlinjer för utkontraktering i kraft. Riktlinjerna fokuserar på kritisk eller viktig utlagd verksamhet. Företagen behöver dock göra en riskbedömning av alla avtal med en tredje part, oavsett om det är att betrakta som utlagd verksamhet eller inte, och ett register över dessa bör föras. Bolaget behöver identifiera, värdera, övervaka och hantera alla de risker som de exponeras mot eller kan exponeras mot som ett resultat av ett avtal med en tredje part.[85] Finansinspektionens föreskrifter FFFS 2014:1 som riktar sig mot kreditinstitut innehåller i kapitel 10 regler om uppdragsavtal.

Även den nya clearinglagen som träder i kraft 2024 (avsnitt 5.3) innehåller krav vid utkontraktering av clearingverksamhet.

---

[81] *Försvarsdepartementet (2023), Kommittédirektiv 2023:30*

[82] *Skäl 16, EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011*

[83] *Svenska bankföreningen (2023), FRAMSTÄLLNING Diarienr: 2023/11/005*

[84] *EU-kommissionen (2023), Kommissionens riktlinjer för tillämpningen av artikel 4 (1) och (2) i direktiv (EU) 2022/255 (NIS2-direktivet)*

[85] *European Banking Authority (2019), EBA/GL/2019/02*

Finansinspektionen fick 2022 i regeringsuppdrag att ta fram en handlingsplan för att stärka kontrollen över de finansiella företagens utlagda verksamhet. I uppdraget ingick även att göra en analys av vilka regeländringar som behövs för att uppnå bättre kontroll över de finansiella företagens utlagda verksamhet. I rapporten som redovisades våren 2023 gjorde FI bedömningen att det krävs en ökad tydlighet och enhetlighet i reglerna för finansiella företags utkontrakterade verksamhet, då kraven idag återspeglas i flera olika regler. FI:s handlingsplan innehåller åtgärder på tre områden:[86]

- Aktivt arbete med såväl nationell som EU-rättslig regelgivning, såsom inventering och analys av regelverk som har koppling till eller påverkar arbetet med tredjepartsrisker. Ett exempel är en behovsanalys av nationella anpassningar av lagar, förordningar och föreskrifter till följd av DORA-förordningen
- Fokus på tredjepartsrisker i tillsynen
- Utveckla systemstöd, avseende främst företagens inrapportering enligt DORA-förordningen

7.2.4 Artificiell intelligens, AI

Ett område som debatteras flitigt är artificiell intelligens, AI. Utvecklingen går mycket fort och innebär nya möjligheter, men också nya hot. EU-kommissionen har under de senaste åren arbetat med nya regler och åtgärder avseende tillförlitlig artificiell intelligens. AI-förordningen riktar sig främst till tillhandahållare, tillverkare, distributörer, men i viss mån också till användare av AI-system.[87] Ramverket beskriver ett riskbaserat tillvägagångssätt med fyra olika risknivåer, oacceptabel risk, hög risk, begränsad risk och minimal risk, i syfte att skapa en strukturerad uppdelning mellan olika typer av AI-system och dess användning. De med högst risknivå är förbjudna, medan de i lägre risknivåer är tillåtna, men med restriktioner och krav i form av bland annat tillsyn och registrering hos ansvarig myndighet. Den svenska regeringen har utryckt behov av ytterligare analys, för att säkerställa att regleringen i sig inte negativt påverkar svenska myndigheters förmåga att upprätthålla nationell säkerhet eller bedriva effektiv brottsbekämpning.[88] Förhandling med EU-länderna i rådet om den slutliga utformningen av lagen inleddes sommaren 2023.

MSB gör i sin policyöversikt bedömningen av EU:s reglering på området kommer att minska den osäkerhet som råder i nuläget och bidra till säkra produkter och följaktligen säkerhet i ett vidare perspektiv.[89]

---

[86] *Finansinspektionen (2023), Handlingsplan om att stärka kontrollen över de finansiella företagens utlagda verksamhet, Dnr 22-18123*

[87] *Europaparlamentet (2021), Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING OM HARMONISERADE REGLER FÖR ARTIFICIELL INTELLIGENS (RÄTTSAKT OM ARTIFICIELL INTELLIGENS) OCH OM ÄNDRING AV VISSA UNIONSLAGSTIFTNINGSAKTER, COM/2021/206 final*

[88] *Infrastrukturdepartementet (2020), Förordning om artificiell intelligens, Fakta-pm om EU-förslag 2020/21:FPM109 : COM(2021) 206)*

[89] *MSB (2023), Policyöversikt: Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete*

7.3 Myndigheters IT-drift

I beredskapssektorn Ekonomisk säkerhet ingår flera myndigheter, med ansvar för att samhällets utbetalningar ska fungera, till exempel barnbidrag, föräldrapenning, sjukpenning och pension. IT-driften är av central betydelse för dessa funktioner, vilket innebär att villkoren för att säkerställa denna behöver vara tydliga. Myndigheternas IT-driftslösningar har dock i olika sammanhang bedömts ha brister avseende säkerhet eller kostnadseffektivitet. Nedan beskrivs några nytillkomna inriktningar som ska stödja utvecklingen mot ökad säkerhet.

7.3.1 Utkontraktering av myndigheters IT-drift

Utkontraktering av IT-drift eller IT-baserade funktioner kan vara en förutsättning för en ändamålsenlig och kostnadseffektiv verksamhet. Digitaliseringsrättsutredningen beskrev dock 2018 att flera myndigheter upplever ett oklart rättsläge när det gäller att lämna ut sekretessreglerade uppgifter till en privat tjänsteleverantör. Tjänsteleverantörens affärsmodell kan också vara svår att överblicka, med en eller flera underleverantörer. Vidare är avtalsreglerad sekretess förknippad med oklarheter avseende vilket skydd som faktiskt tillhandahålls.[90] 2021 trädde *lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter* i kraft, som syftar till att uppgifter från en myndighet som hanteras av en tjänsteleverantör ska få ett sekretesskydd som är likvärdigt med det som gäller när en annan myndighet tillhandahåller en motsvarande tjänst.[91]

IT-driftsutredningen (se följande avsnitt) fick i uppdrag att analysera säkerhetsmässiga och rättsliga förutsättningar för att utkontraktera IT-drift till privata leverantörer. I delbetänkandet *Säker och kostnadseffektiv IT-drift – rättsliga förutsättningar för utkontraktering* (SOU 2021:1) resoneras kring att myndigheters osäkerhet, framför allt avseende risk för röjande av uppgift, kan medföra att aktörer avvaktar med beslut om IT-drift, vilket i sin tur kan få negativa konsekvenser för verksamhetens utveckling, kostnader och säkerhet. Utredningens förslag ledde till införande av en sekretessbrytande bestämmelse i *Offentlighets- och sekretesslag (2009:400)*, som gäller då uppgifter lämnas ut till en aktör (myndighet eller företag) som har i uppdrag att utföra endast teknisk bearbetning eller teknisk lagring av de uppgifterna. Utlämnande ska inte ske om det intresse som sekretessen ska skydda bedöms överväga intresset av utkontraktering.[92]

7.3.2 En samordnad och säker statlig IT-drift

Försäkringskassan fick 2017 ett regeringsuppdrag att erbjuda samordnad och säker statlig IT-drift.[93] I redovisningen våren 2023 anser Försäkringskassan att staten bör stärka regleringen av digital infrastruktur. Staten bör tillhandahålla vitala digitala funktioner, för att värna samhällets fortsatta digitalisering och säkra samhällsviktiga funktioner. Under 2021 har Försäkringskassan deltagit i samverkan med ett antal områden med syfte att öka statsförvaltningens och myndighetens förmåga att erbjuda säkra, lämpliga tjänster. Programmet SITSSAM, Program 2032 och DSAM. I SITSSAM, säkra IT-tjänster i statliga samverkan, deltar Lantmäteriet, Skatteverket och Trafikverket, Transportstyrelsens deltar utifrån ett kundperspektiv. Inom ramen för Program 2023 har dessa myndigheter tillsammans med Fortifikationsverket, undersökt hur ett nationellt system med säkra, statliga samordnade datacenter, inklusive kommunikationsinfrastruktur, kan

---

[90] *SOU 2018:25, Juridik som stöd för förvaltningens digitalisering*

[91] *Regeringen (2020), Lagrådsremiss Tystnadsplikt vid teknisk bearbetning och lagring*

[92] *OSL (2009:400), 10 kap. 2a §*

[93] *Försäkringskassan (2021)*

utformas. Målsättningen är att den svenska ambitionen att vara bäst på att utnyttja digitaliseringens möjligheter ska kunna möta krav på öka robusthet i det civila försvaret. Försäkringskassan menar att uppdraget visat att statlig IT-drift behöver tillhandahållas av flera statliga myndigheter och att även stora myndigheterna behöver nyttja varandras kompetens och tekniska infrastruktur för att öka kapaciteten och stärka säkerhet och robusthet. Samverkansmyndigheterna inom SITSSAM, föreslås få i uppdrag att tillhandahålla säker IT-drift till statliga myndigheter, för att värna Sveriges säkerhet.[94]

Parallellt fick IT-driftsutredningen 2019 i uppdrag att kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv IT-drift samt säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig IT-drift. Försäkringskassans dittills dragna erfarenheter av regeringsuppdraget skulle beaktas. Säkra IT-driftslösningar ska säkerställa konfidentialitet, riktighet och tillgänglighet i statliga myndigheters information. I slutbetänkandet 2021 *Säker och kostnadseffektiv IT-drift – förslag till varaktiga former för samordnad statlig IT-drift* beskrivs syftet med samordnad statlig IT-drift vara att erbjuda myndigheter stöd och vägledning i valet av säkra och kostnadseffektiva IT-driftslösningar samt att tillhandahålla ett samordnat och ändamålsenligt statligt tjänsteutbud. Användningen av begreppet säker beskrivs på aktörsnivå vara att en offentlig aktörs IT-drift lever upp till för verksamheten tillämpliga rättsliga och säkerhetsmässiga krav, exempelvis krav på säkerhetsskydd och informationssäkerhet samt skydd för den personliga integriteten. Även förmåga att kontinuerligt bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete som omhändertar förändrade krav och risker ingår. En robust och säker IT-driftslösning på samhällsnivå tar hänsyn till olika typer av risker och hot, som kan påverka inte bara tillgänglighet utan även riktighet avseende informationen. Myndigheters informationshantering i kris och krig, vilket innefattar samhällsviktiga grunddata, liksom IT-driften behöver vara robust och redundant. En samordnad statlig IT-drift bedöms kunna bidra till ökad säkerhet, både för enskilda aktörer och för en större del av samhället. Ställning bör även tas till samordnad statlig IT-drifts roll i det civila försvaret. Förslag på en ny förordning för att reglera området ges, med Myndigheten för digital förvaltning som samordnande myndighet.[95]

8 Andra säkerhetsaspekter

8.1 Ny säkerhetsskyddslagstiftning

Säkerhetsskydd handlar om att skydda information och verksamheter som är av betydelse för Sveriges säkerhet mot spionerі, sabotage, terroristbrott och vissa andra antagonistiska hot. Förutom verksamheten i sig kan alltså uppgifter avseende exempelvis beredskapsåtgärder omfattas.[96]

Sedan några år gäller ny reglering avseende säkerhetsskydd, genom *säkerhetsskyddslagen* (2018:585) och *säkerhetsskyddsförordningen* (2021:955). Regleringen ansågs behöva moderniseras utifrån att kraven på säkerhetsskyddet förändrats beroende på utvecklingen på IT-området, ökad internationell samverkan, en ökad sårbarhet i samhällsviktiga funktioner och att säkerhetskänslig verksamhet i allt större omfattning bedrivs i av privata utövare.[97] Under 2021 utökades lagen med bestämmelser om bland annat överlåtelse av säkerhetskänslig verksamhet och

[94] *Försäkringskassan (2023), FK 2022/02371*

[95] *SOU 2021:97, Säker och kostnadseffektiv IT-drift – förslag till varaktiga former för samordnad statlig IT-drift*

[96] *Se vidare Säkerhetspolisens webbplats, Lagar, förordningar och föreskrifter - Säkerhetspolisen (sakerhetspolisen.se)*

[97] *SOU 2015:25, En ny säkerhetsskyddslag*

tillsynsmyndigheternas möjligheter till sanktionsavgifter. *Säkerhetspolisens föreskrifter om säkerhetsskydd* (PMFS 2022:1) innehåller mer detaljerade och kompletterande bestämmelser. Säpo har gett ut en rad vägledningar till stöd för arbetet. Under våren 2023 utkom flera nya versioner. Vägledningarna kommer fortsätta att revideras och kompletteras för att harmonisera med de lagändringar som genomfördes i 2021.

Regleringen omfattar fler verksamheter än tidigare och lagen innebär att både offentliga och privata verksamhetsutövare är skyldiga att utreda behovet av säkerhetsskydd i sin verksamhet, genom att genomföra en säkerhetsskyddsanalys. I en sådan görs en verksamhetsbeskrivning och en eventuell specificering av vilka delar av verksamheten (tjänster, leveranser, funktioner eller förmågor) som är säkerhetskänslig. Det kan även vara så den egna verksamhet inte bedöms som säkerhetskänslig, men att uppgifter som säkerhetsskyddsklassificerats av en annan verksamhetsutövare hanteras. Tre typer av skyddsvärden ska identifieras och bedömas; säkerhetsskyddsklassificerade uppgifter, anläggningar, objekt, system, egendom och andra tillgångar samt verksamhet som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd.

Nedbrytningen av vad som är av betydelse för Sveriges säkerhet görs i fem kategorier:

- Sveriges yttre säkerhet
- Sveriges inre säkerhet
- nationellt samhällsviktig verksamhet
- verksamhet av betydelse för Sveriges ekonomi
- verksamhet som kan generera skada på annan säkerhetskänslig verksamhet.

I vägledningen avseende säkerhetsskyddsanalys exemplifieras att nationellt samhällsviktig verksamhet ur ett säkerhetsskyddsperspektiv bland annat finns inom energiförsörjning, elektroniska kommunikationer, finansiella tjänster (centrala betalningssystem), livsmedelsförsörjning, vattenförsörjning och transporter. Verksamhet som är av betydelse för Sveriges ekonomi anges vara tjänster, leveranser, funktioner eller förmågor som är nödvändiga för den nationella betalningsförmågan, liksom förmågan att hantera, administrera, granska, styra och stödja den nationella finansiella stabiliteten. Verksamhet är av betydelse för Sveriges säkerhet om konsekvenserna av en antagonistisk handling mot verksamheten har en direkt eller uppenbart indirekt påverkan på Sveriges betalningsförmåga. Det kan exempelvis vara de system som genom sina funktioner i infrastrukturen är kopplade till det centrala betalningssystemet och har en viktig roll för upprätthållandet av betalningsflödena på nationell nivå.

Säkerhetsskyddsklassificerade uppgifter ska löpande delas in i någon av de fyra säkerhetsskyddsklasserna, utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet:

1. kvalificerat hemlig (synnerligen allvarlig skada)
2. hemlig (allvarlig skada)
3. konfidentiell (inte obetydlig skada)
4. begränsat hemlig (endast ringa skada)

Ett erforderligt säkerhetsskydd kräver åtgärder inom kategorierna personalsäkerhet, fysisk säkerhet och informationssäkerhet. Finansinspektionen är tillsynsmyndighet enligt säkerhetsskyddsförordningen.

8.2 Utländska direktinvesteringar och ägarförhållanden

I Sverige finns begränsade möjligheter att påverka eller hindra utländska direktinvesteringar som kan medföra risker för svenska säkerhetsintressen. Befintliga regelverk gäller vissa områden, för vissa verksamheter och i särskilda situationer. Enligt lagen (2004:297) om bank- och finansieringsrörelse får bankrörelse eller finansieringsrörelse drivas bara efter tillstånd, om inget annat framgår av den lagen. Bland annat görs en ägarprövning, det vill säga en prövning av dem som har ett kvalificerat innehav av aktier. Enligt EU-lagstiftning får behöriga myndigheter också bedöma förvärv och ökningar av innehav i finansinstitut. Krav på underrättelse, förfaranderegler och utvärderingskriterier för sådana bedömningar anges, med målet att säkerställa en sund och ansvarsfull ledning av finansinstitut.[98]

Europaparlamentets och rådets förordning om upprättande av en ram för granskning av utländska direktinvesteringar i unionen tillämpas sedan oktober 2020.[99] Ett grundläggande syfte är att skapa en rättslig ram för granskning med hänsyn till säkerhet eller allmän ordning. Direktinvesteringens uppdrag var att föreslå anpassningar och kompletterande bestämmelser för en svensk tillämpning. I kommittédirektiven angavs att syftet är att kontrollera uppköp och strategiska förvärv av bolag med säte i Sverige, vars verksamhet eller teknologi har betydelse för säkerhet eller allmän ordning.[100]

Enligt utredningen behöver regelverket för att hantera risker med utländska direktinvesteringar stärkas. I slutbetänkandet redovisas förslag på hur ett sådant system kan utformas.[101] Samhällsviktig tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet föreslås omfattas av systemet. *Lag (2023:560) om granskning av utländska direktinvesteringar* träder i kraft 1 december 2023 och omfattar enligt 3§ bland annat samhällsviktig verksamhet, säkerhetskänslig verksamhet enligt säkerhetsskyddslagen och behandling i stor omfattning av känsliga personuppgifter.

9 Intervjustudie med aktörer i finansiell sektor

För att undersöka vilka uppfattningar det finns kring kommande beredskapsarbete intervjuades nio aktörer i sektorn, varav ett par genomfördes som gruppintervjuer. De intervjuade arbetar hos en bredd av aktörer inom den finansiella sektorn, såsom bank, försäkring, och finansiell infrastruktur samt myndigheter. Dessutom intervjuades en person som är anställd på MSB. Urvalet gjordes för att få en bredd av aktörer, men ska ses som ett försök att fånga några tankar som kan vara intressanta att beakta i det fortsatta krisberedskapsarbetet snarare än som en representativ bild av sektorn som helhet. Intervjustudien och resultatet som presenteras i detta avsnitt är baserat på respondenternas egna åsikter och synsätt, och representerar inte nödvändigtvis synsättet hos respondenternas organisationer.

---

[98] *EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2013/36/EU om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, DIREKTIV 2009/138/EG om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II) och DIREKTIV 2014/65/EU om marknader för finansiella instrument.*

[99] *EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2019/452 av den 19 mars 2019 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen*

[100] *SOU 2020:11, Delbetänkandet Kompletterande bestämmelser till EU:s förordning om utländska direktinvesteringar. Förslagen ledde till lagen (2020:826) med kompletterande bestämmelser till EU:s förordning om utländska direktinvesteringar och förordningen (2020:827) med kompletterande bestämmelser till EU:s förordning om utländska direktinvesteringar.*

[101] *SOU 2021:87, Granskning av utländska direktinvesteringar*

Respondenterna uppmanades under intervjuerna att inte begränsa sina resonemang till krisberedskapsområdet i det fall de arbetar med perspektivet civil beredskap. De ombads också att dela tankar även om de inte ansåg sig besitta sakkunskap inom varje frågeområde. Nedan återges de synpunkter som framkommit med utgångspunkt i det de områden som beskrivits tidigare i PM:en. Synpunkterna ska inte gå att spåra till en viss respondent, vilket även gavs som ingångsvärde till respondenterna. Några synpunkter åskådliggörs med citat.

En generell reflektion är att det finns många nya förutsättningar, en hel del som är osäkert, och mycket som kommer att förändras på sikt. Olika intervjupersoner lyfter olika exempel på pågående utredningar, initiativ och arbeten som ännu inte är färdigställda eller beslutade, framför allt från myndighetsnivå och lagstiftningsnivå. Det pågår och har avslutats remissrundor av olika förslag, men tydliga besked saknas. Många intervjupersoner förmedlar en bild av att det återstår att se vart allt landar. Någon säger även att man förstått att ”något är på gång” utifrån att det inkommer olika frågeunderlag från myndighetshåll, men att det är oklart varför. Det är rimligt att det i tider av förändring finns en del osäkerhet kring hur saker ska bli och fungera, men i denna intervjustudie framträder en bild av att det finns osäkerhet på i stort sett alla områden som undersökts. Det är förståeligt om aktörer i finansiell sektor upplever stora utmaningar i att orientera bland de nya och kommande förutsättningarna för krisberedskap.

OBS! Det som framgår i nedan avsnitt är de intervjuades egna tankar och åsikter och representerar inte de organisationer de intervjuade tillhör.

9.1 Hotbild

Ett par intervjupersoner lyfter fram bevakningen av hotbild som mycket central och att de vidtagit flera åtgärder till följd av att de sett förändringar i hotbild, till exempel när det gäller skydd av verksamhet och lokaler.

> *”Vi måste omvärldsbevaka för att kunna prioritera vårt arbete. Vi analyserar utvecklingen både själva och i samverkan för att få så stor bredd på inhämtningen som möjligt.”*

Bilden som träder fram vid intervjuerna är att det skiljer sig mycket åt hur strukturerat omvärldsbevakning sker och hur organisationer följer utvecklingen av hotbilden mot enskilda aktörer, sektorn och Sverige i stort. En aktör hänvisar till resursbrist när det gäller att göra löpande hotbildsbedömning. De större bolagen har resurser och kan själva göra bedömningar och välja om de vill redogöra för dem i nätverket, men det sker inte systematiskt. Flera berättar att de håller sig informerade om omvärldsläget, bland annat genom externa rapporter eller att tjänsten köps. En respondent säger att de senaste årens händelser tydliggjort att organisationen påverkas av händelser man inte kan styra.

En respondent tar upp att man från privat sektor i slutet på 2021 såg en oroande hotutveckling och därför kontaktade Riksbanken med förslag om samverkan. Man satte då upp en särskild grupp på sektornivå som följde hotbildsutvecklingen och hade veckovisa möten under Riksbankens ledning. Konkurrensaspekter diskuterades inte, utan man tog snarare del av lägesbild, med inrapportering av egna observationer. Händelsestyrd samverkan kring hotbild, snarare än löpande och systematisk, nämns av flera.

En annan aspekt som påtalas är att vad som är relevant i en hotbild skiljer sig åt mellan olika typer av aktörer i finansiell sektor. En respondent uppfattar till exempel att banker fokuserar mycket på digitala hot mot betalningar och att det finns ett realtidsberoende, medan vissa former av bedrägerier är mer relevant för försäkringsbolag.

9.1.1 Förmågeutveckling mot den breddade hotbilden

En aktör uppger att de senaste åren inneburit stora påfrestningar, inte minst Coronapandemin, då man blev tvungna att agera snabbt för att få verksamheten att fungera. Det ställde stora krav på krisorganisationen och visade på vikten av att gå från skrivbordsövningar till simuleringsövningar för att bättre förstå vilka krav som ställs för att hantera händelser.

Övningar i stor och liten skala lyfts även av andra som viktiga förberedande aktiviteter. Här efterfrågar flera intervjupersoner tydligare förväntningar och instruktioner från myndighetshåll, vilka aktiviteter som förväntas genomföras, och vilken förmåga som ska finnas hos utpekade aktörer. En respondent påtalar att myndigheter behöver driva på de viktigaste aktörerna, så de har övat och vet hur de ska agera vid störningar.

I intervjuerna målas en bild av att många aktörer i finansiell sektor har en hög mognadsgrad och krishanteringsförmåga. Delar som kontinuitetshantering, riskhantering och krishantering är i många fall väl utvecklade, men ett par respondenter säger att det finns en del att utveckla när det gäller den interna samordningen av det sammantagna resiliensarbetet.

Däremot uttrycks att det är en stor omställning att börja planera för att kunna hantera höjd beredskap. Krigsfara och krig ställer helt andra krav på såväl individer som företag, även infrastruktur och andra resurser sektorn är beroende av kan vara otillgängliga. Flera respondenter understryker att det kommer krävas hårt arbete och god samordning för att börja planera för den typen av störningar. Myndigheternas roll som kravställare och samordnande kraft betonas.

> *”Vilken förmåga ska vi ha om tio år då? Vad ska vi göra för att landa där?”*

En respondent uttalar sig positivt om den av MSB förslagna planeringsprocessen, men den är ännu obekant för de flesta. Mycket förmågestärkande arbete behöver bedrivas långsiktigt, men myndighetsplaneringen är annars 1–3 år. För att kunna prioritera rätt bedöms att man måste sträcka ut tidsperspektivet.

9.2 Strukturreformen

9.2.1 Strukturen är under utveckling

Strukturen för civil beredskap är ny och har i nuläget framför allt påverkat myndigheter. I de flesta intervjuer lyfts att det ännu inte är klarlagt hur kraven enligt beredskapsförordningen kommer att implementeras. En respondent menar att det är svårt att förstå hur det är tänkt att fungera och att förarbetena inte ger vägledning. En respondent påtalar att alla beredskapssektorer är olika och att man måste förstå respektive sektor för att hitta vägar framåt. Man måste jobba sig igenom frågorna på ett strukturerat sätt inom respektive sektor och att det finns ingen universallösning.

"Det kanske är helt naturligt att det inte kommer vara optimalt från början utan behöver anpassning."

Myndigheterna i beredskapssektorn har intensifierat samverkan mellan varandra och även tagit initiativ till möten med privata aktörer i olika frågor. Myndigheterna har diskuterat hur samarbetet ska gå till, hur respektive myndighetsuppgift kan utföras utan att det blir dubbelt för företagen, då olika beredskapslagar påverkar finansiella sektorn med varandra.

Det flesta anser att det är tydligt att det finns mycket arbete kvar att göra, och flera intervjupersoner anser att det kanske är rimligt att förvänta att utveckling av strukturer och processer kommer att ske stegvis och anpassas efter hand som nya lärdomar dras.

Ett par intervjupersoner uttrycker besvikelse över bristen på information kring hur myndigheterna arbetar eller vilka strukturer som kommer skapas. En annan är medveten om att det pågår arbete som initierats av myndigheterna, men utan att ha fått förståelse vad det handlar om. Organisationen ombeds svara på enkäter, men kontexten framgår inte. En respondent uttrycker viss besvikelse över att det inte hänt mer.

Ett par respondenter efterfrågar mer samordning myndigheter emellan. För en del aktörer kommer frågor och enkäter från flera olika håll i otakt, vilket belastar dem som arbetar med frågorna. Myndigheters brist på samordning i informationsinhämtningen upplevs vara en belastning. Språkbruk och semantik är heller inte enhetligt, vilket kan skapa förvirring.

"Om det blir påverkan på vår bransch måste vi får vara med från start."

Från ett par håll lyfts problematiken med att en alltför snäv krets involveras i arbetet. Ett begränsat antal aktörer har involverats i olika referens- och arbetsgrupper och bjudits in till workshops. Ett par anser att kretsen behöver breddas, exempelvis kan mindre aktörer ha andra utmaningar än de större och även ha en regional betydelse. En relaterad problematik som en respondent lyfter är att arbete lagts ner på att ge remissynpunkter, som senare ändå inte omhändertagits av myndigheter.

En del aktörer i finansiell sektor skulle även kunna ingå i sektorn Ekonomisk säkerhet, där Försäkringskassan är sektorsansvarig myndighet. Ingen respondent har varit involverad i något arbete eller samverkan med Försäkringskassan. Från försäkringssidan lyfts vikten av att se funktionen som kompletterar välfärdssystemet när man analyserar samhällsviktig verksamhet. Man saknar tjänstepensionsområdet i MSB:s nya lista över samhällsviktig verksamhet, som i hög grad involverar den privata sektorn.

En respondent kallar 2024 för teståret för den nya strukturen. Under det första kvartalet ska en inriktning för sektorns beredskapsarbete beslutas mellan myndighetschefer.

9.2.2 Brist på mandat och möjlig rollkonflikt

Finansinspektionen har påbörjat arbete för att reda ut ansvar och mandat samt börjat stärka sin organisation med lämplig kompetens. På vissa sätt har strukturreformen tydliggjort ansvar för myndigheter, men andra frågor är utestående, menar flera intervjupersoner. I de flesta intervjuer lyfts att det ännu inte är klarlagt hur samverkan i finansiell sektor eller hur enskilda verksamheter kommer att påverkas.

> *"Ska man kunna styra och leda och planera så räcker inte frivillighet utan det behövs klara mandat."*

Flera respondenter vill att myndigheterna ställer krav, men efterfrågar i så fall mycket större tydlighet från myndigheterna kring förväntningar på privata aktörer. Ett par respondenter lyfter att bristen på mandat och föreskriftsrätt för Finansinspektionen som sektorsansvarig myndighet försvårar i arbetet, eftersom frivillighet inte förmodas räcka till. Samtidigt verkar engagemanget och viljan att bidra stor.

En utmaning som lyfts av flera intervjupersoner är hur Finansinspektionen ska balansera sitt tillsynsansvar och samtidigt verka för samordning av beredskapshöjande förmågeutveckling i sektorn. Privata aktörer upplever att det kan finnas intressekonflikter i att dela med sig av utmaningar och problem i det beredskapshöjande arbetet med samma myndighet som också kan besluta om sanktionsavgifter. De flesta menar att detta inte måste vara ett problem, så länge det är tydligt vilken information som kan delas i olika forum. Det behöver finnas en transparent och tydlig kommunikation om när Finansinspektionen agerar inom ramen för sitt tillsynsansvar.

> *"FI har formats utifrån tillsynsuppdraget. När man nu får nya uppgifter krävs annan kompetens och nya arbetssätt."*

En respondent framhåller dock att man inte måste problematisera för mycket när det gäller de olika rollerna, men att det troligen är en utmaning för myndigheter att utveckla ett annat mindset när man får nya uppgifter på området utöver tillsynsuppdraget. Myndigheterna måste tolka vad uppdraget innebär i dialog med berörda aktörer.

9.3 Samverkan inför och vid fredstida kriser

Vikten av att inte skapa onödiga samverkansfora lyfts fram av en respondent, utan att använda de som redan finns på ett effektivt sätt. FSPOS framhålls som ett välfungerande forum, där offentliga och privata aktörer deltar på lika villkor. Några intervjupersoner beskriver att det finns flera samverkansfora idag, framför allt i det förberedande arbetet, initierade av privata aktörer.

Kopplat till cybersäkerhetsfrågor finns operativa fora där aktörer delar information med varandra. Det finns även samverkansfora som leds av stora leverantörer av IT-tjänster till många aktörer i finansiell sektor. Under Coronapandemin initierade de tre storbankerna samverkan.

Det har identifierats ett behov av tydlighet kring vilken aktör som är ansvarig för att säkerställa samverkan och ledning i finansiella sektorn, när det gäller såväl finansiella kriser som höjd

beredskap. Att tydliggöra dessa roller och ansvar är ett pågående arbete, och något som myndigheterna arbetar med. Flera intervjupersoner lyfter den pågående utredningen som leds av Finansdepartementet om operativ krisledning.[102]

> *"Man kan inte ha visst forum som enbart tittar på händelser som har specifika orsaker i sektorn och får specifika konsekvenser för finansiell sektor".*

En farhåga är att olika system för krishantering byggs upp, beroende på huruvida en störning uppstår inom eller utanför sektorn. Finansdepartementets utredning beskrivs som ett sent svar på ett behov som funnits under en längre tid, men som i och med Finansinspektionens sektorsansvar uppfyllts. En respondent lyfter att Finansinspektionen och Riksbanken måste utreda sina respektive roller kopplat bland annat till krishantering. En faktor som kan påverka är att Riksbanken har föreskriftsrätt som är mer långtgående. Någon understryker vikten av att strukturen tar hänsyn till de forum och roller som redan finns och bygger vidare på detta.

En respondent beskriver att FSPOS-övningen 2022 väckte frågeställningen kring vem som har det huvudsakliga ansvaret för kommunikation vid större kris. Under intervjun lyfts att enskilda aktörer inte bör ha en framträdande roll i krissituationer där en bred mängd kunder påverkas och berörs. Kommunikationen bör i stället samordnas av myndigheterna. Det behöver vara tydligt vem som har det huvudsakliga ansvaret och blir en tydlig avsändare och förmedlare av kommunikativa budskap från hela eller delar av sektorn.

En poäng som lyfts i intervjuer är att vidareutvecklingen av *Gemensamma grunder för samverkan och ledning vid samhällsstörningar* pågår och leds av MSB, men involverar många aktörer inom svensk krisberedskap, i huvudsak offentliga. Begreppsvärlden i denna sfär som nu är under vidareutveckling, är viktig för aktörer inom finansiell sektor att förstå och dela. Aktörer i finansiell sektor är en del av svensk krisberedskap och det finns en god förmåga hos många aktörer att verka och samverka i kris. Perspektivet breddas dock kopplat till sektorns beroende till andra sektorer, myndigheternas samverkansformer och hur privata aktörer kan jacka in i krisberedskapssystemet i stort.

9.4 Betalningar

Den nya riksbankslagen skapar enligt flera intervjupersoner goda förutsättningar för att bygga beredskap för att betalningar alltid ska fungera. Samtidigt finns utmaningar i rollfördelningen mellan Finansinspektionen och Riksbanken, eftersom FI är sektorsansvarig myndighet för sektorn Finansiella tjänster, och Riksbanken har ett särskilt ansvar för betalningar, vilket innebär visst överlapp. För att det inte ska innebära onödig belastning på aktörer kopplat till rapportering krävs en mycket nära samverkan mellan de två myndigheterna.

Ett par intervjupersoner lyfter också vikten av att svenska samhället ska ha beredskap för att betalningar ska kunna genomföras oavsett störningar. Ansvarsbilden för detta ser komplex ut, men det är tydligt att även individer och enskilda företagare kan spela en viktig roll i förberedelserna. Däremot är det myndigheterna som behöver informera vad varje enskild person och företag kan göra för att stärka den egna beredskapen. Ju fler betalningsalternativ som erbjuds

[102] *Finansdepartementet (2023). Fi2023/01842. Utredningen ska se över hur en operativ krisledning vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur kan utformas.*

i affärer och ju fler olika betalningsmedel konsumenter kan använda sig av, desto bättre. I betalningsutredningen genomfördes en utblick över hur andra länder hanterar offline-betalningar, men intervjupersoner påpekar att det inte finns något självklart alternativ i Sverige i dagsläget.

Det är ett komplext ekosystem av aktörer och beroenden som behöver fungera. Några intervjupersoner lyfter att det är viktigt att analysera kedjor av verksamheters beroenden till varandra, och att ha en bredd i de scenarier som det planeras utifrån, eftersom det kan variera vilka verksamheter och funktioner som blir mest kritiska i olika situationer. Till exempel kan ett läge där någon enstaka region är särskilt drabbad, öka betydelsen av funktionaliteten hos regionala banker. Några intervjupersoner menar därför att de aktörer som på förslag pekats ut av Riksbanken inte är en tillräckligt bred grupp. Samtidigt menar andra intervjupersoner att det viktigaste i nuläget är att börja någonstans, och att definitioner kan omvärderas och eventuellt breddas framöver. Flera intervjupersoner lyfter att det behövs en god beredskap i hela systemet, och att alla aktörer behöver arbeta med redundans i sina system och kommunikationer.

9.5 Natos arbete med civil beredskap

Många av de intervjuade uppger att de inte analyserat vad ett svenskt medlemskap i Nato skulle innebära för finansiell sektor. Vissa framför att de utgår från att de blir informerade om nya krav när det blir aktuellt. Det är tydligt att representanterna från myndigheterna i högre utsträckning analyserat frågan. De har identifierat att finansiella tjänster eller betalningar inte uppenbart är en del av de *baseline requirements* som Sverige skulle behöva möta kopplat till Natos arbete med civil beredskap. En bedömning från några av intervjupersonerna är att det finns anledning att analysera frågan djupare.

9.6 Cybersäkerhet

Nationella cybersäkerhetscentret NCSC lyser enligt många intervjupersoner med sin frånvaro när det gäller att sprida information, bjuda in till samverkan och erbjuda stöd. De konstaterar samtidigt att det är ett arbete som är i uppstartsfasen då man fortfarande diskuterar former och hur NCSC ska fungera.

Några intervjupersoner anser att det är en för snäv krets som involverats i arbetet med *Finansforum*. De flesta tycker att det är ett bra initiativ med stor potential, eftersom behovet av samverkan i cybersäkerhetsfrågor är stort. En respondent tar upp att det finns samarbete avseende vilka krav som ska ställas på en gemensam leverantör av IT-tjänster.

Många i privat sektor uppger att de börjat förbereda för DORA, och påbörjat anpassningen. Det finns initiativ från branschföreningar att analysera gemensamt med medlemsföretagen hur man ska tolka lagstiftningen. Några lyfter att det är positivt att det finns tydlighet i DORA ned på en relativt teknisk nivå. Andra menar att det finns en risk att sådan detaljerad information snabbt blir utdaterad, och att dessa krav om några år riskerar att inte längre vara det som säkerställer en hög skyddsnivå.

"Är det anpassat till oss?"

Flera respondenter menar att deras organisationer inte kommer att omfattas av NIS2 och CER eftersom de omfattas av DORA. Någon respondent anser att varken DORA, NIS2 eller CER kommer att vara tillämpbart på den egna organisationen, men de flesta är osäkra. Ett par respondenter menar att anpassningsarbetet inte kan påbörjas förrän det är klart vilka organisationer som kommer att omfattas, det vill säga när den svenska implementeringen av EU-direktiven beslutats. Några intervjupersoner säger att om de kommer att omfattas lär det bli ett stort anpassningsarbete, och att de bevakar området löpande.

Någon påpekar att regelverk både är begränsande och hjälpsamt, det senare genom att tillhandahålla en tydlig kravbild. En farhåga med DORA som lyfts är att direktivet är sektorsövergripande, men att det är stor skillnad mellan bank och försäkring.

9.7 Säkerhetsskydd

I intervjuerna varierar det hur insatta respondenterna är i säkerhetsskyddslagen och säkerhetsskydd som begrepp, vilket delvis kan förklaras av att intervjupersonerna inte ansvarar för frågorna i sina respektive organisationer. Några bedömer att många privata aktörer har satt sig in i frågan och analyserat sin verksamhet och information utifrån lagen, men det finns ingen klar bild över hur det ser ut i sektorn. De intervjupersoner från privat sektor som har analyserat sin verksamhet har i flera fall kommit fram till att de inte berörs. Det lyfts att det läggs ett stort ansvar på privata aktörer att själva analysera sin verksamhet, och att myndigheterna eventuellt kan behöva erbjuda mer stöd här.

"Det är inget vi känner till, vi har inte gjort någon analys. Om man anser att man inte omfattas, kan man få en smäll på fingrarna då?"

Myndigheterna bedömer att de har rätt verktyg och förutsättningar att själva hantera säkerhetsskyddsklassificerad information, men en poäng som lyfts av flera är att det är viktigt att information kan delas till relevanta aktörer i hela sektorn. När det gäller viss typ av samverkan i sektorns beredskapsarbete är det möjligt att det kräver säkerhetsskyddsåtgärder. Här förväntar sig privata aktörer att myndigheterna gör den bedömningen.

10 Slutord

Svenskt beredskapsarbete är under stark utveckling, drivet av det säkerhetspolitiska omvärldsläget med Rysslands invasion av Ukraina och den snabba teknikutvecklingen som medför nya sårbarheter. Under arbetet med framtagande av denna PM, som bara pågått några månader, har det tillkommit nya inriktningar, lagar och analyser på området och det är svårt att dra en gräns. Denna PM beskriver ett nuläge inom ett antal områden under senhösten 2023. Utöver redan fastslagna inriktningar beskrivs även arbete som pågår och som inom kort kan komma att utgöra nya förutsättningar för krisberedskapen, såsom ett svenskt Nato-medlemskap och utvecklingen inom artificiell intelligens.

Genom strukturreformen utarbetades såväl en sektoriell som geografisk indelning för att öka samhällets beredskapsförmåga. Även om denna struktur är väl anpassad, kommer samhälls- och teknikutveckling och ökad kunskap att innebära att beredskapsarbetet behöver förhålla sig till nya parametrar.

10.1 Resiliens för att omhänderta det breddade perspektivet?

Både i de studerade underlagen och i intervjuer med aktörer från sektorn har det visat sig vara svårt att dra en skarp gräns mellan sektorns etablerade arbete för att säkerställa finansiell stabilitet och det arbete som ska vidtas för att minska risk för och konsekvenser av samhällsstörningar – det vill säga samhällets krisberedskap. En störning i det finansiella systemet kan leda till en finansiell kris, som i sin tur riskerar att leda till en samhällsstörning. Arbetet för att säkerställa finansiell stabilitet är en förutsättning för, men inte tillräckligt, för god krisberedskap. Målen för krisberedskapen innefattar samhällets säkerhet vilket medför behov av en vidgad syn på hot och risker. Vidare ska arbetet med krisberedskap utgöra grunden också för det civila försvaret, inramat som civil beredskap. Därmed kommer beredskapsarbetet sannolikt i vissa delar omfatta hela hotskalan, det vill säga även höjd beredskap och krig.

Med hänsyn till den breda paletten av hot och risker är det viktigt att arbetet med hot, risk och beredskap inte bedrivs i stuprör i organisationen. I intervjuerna framkommer att flera anser sig ha en väl anpassad organisation för att hantera den breda paletten - samtidigt som de också uttrycker att de har begränsad kunskap om de beredskapsrelaterade verksamheter som bedrivs i andra delar av organisationen. Begrepp som används alltmer för att beskriva förmåga att stå emot och hantera olika händelser är resiliens och motståndskraft. Det handlar om robusthet att stå emot och fungera väl under en störning, men även om förmåga att hantera effekterna av en störning, att återhämta och anpassa sig.[103] Det handlar således om förebyggande, förberedande, hanterande och återställande insatser, liksom om utvärdering och utveckling. Att samla och analysera verksamheten i dessa perspektiv kan ge en bild av hur beredskapsarbetet lämpligen ska samordnas.

10.2 Nya, omfattande och spridda krav behöver tolkas

Det finns omfattande och specifika regelverk som ska säkerställa en god hantering av risker hos finansiella aktörer. När det gäller krisberedskapsarbetet ser regleringen annorlunda ut. Beredskapsförordningen är generell och gäller över alla beredskapssektorer, vilket innebär att det i alla beredskapssektorer pågår arbete med att tolka hur uppgifter och kravställningar ska omsättas i den egna beredskapssektorn, för finansiella sektorns aktörer främst avseende Finansiella tjänster och Ekonomisk säkerhet.

EU-regleringarna, där DORA-förordningen är specifikt riktad mot finansiell sektor, kommer att bidra med kravställning, men det kommer med stor säkerhet finnas behov av att gemensamt diskutera tolkningar och hur kraven bäst tillgodoses. I intervjustudien gav en del personer uttryck för att NIS2 och CER inte är relevant för deras organisationer, men en analys behöver göras då den pågående utredningen om deras implementering slutredovisats. Det kommer endast vara ett halvår mellan att slutbetänkandet presenteras och regelverket ska implementeras och således krävs förberedelser för att kunna bidra i ett eventuellt remissförfarande.

---

[103] *I Jonsson mfl (2019) Civilt försvar i gråzon s. 20 beskrivs att motståndskraft hos den civila delen av samhället utgörs av robusthet, tålighet samt flexibilitet och anpassningsbarhet. För att motståndskraft ska vara möjlig att skapa krävs såväl vilja som förmåga, där förmåga kräver såväl resurser av olika slag som tillräcklig kunskap.*

Cybersäkerhet är oavsett kommande lagstiftning ett område där det finns samsyn mellan offentliga och privata aktörer att staten bör ta en ledande roll och stödja aktörers arbete, för en hög sammantagen cybersäkerhet.

EU:s AI-förordning kommer troligen, när den antas, påverka användningen av system inom finansiell sektor och därtill förknippat riskhantering. Att undersöka på vilket sätt AI påverkar förutsättningarna för krisberedskapen har inte rymts inom ramen för denna PM.

Någon aktör har uttryckt att regelverk bidrar med tydlighet, men att efterlevnaden kan bli en utmaning om kraven är spridda i olika regelverk. I vissa av de regelverk som nämnts (såsom säkerhetsskyddslagen), ska också aktören själv analysera om den omfattas, vilket kan bidra med osäkerhet kring eventuella påföljder och sanktioner om analysen är felaktig.

10.3 Samverkan för en god krisberedskapsförmåga

Den lagstiftning som berör krisberedskapen beskriver framför allt krav på och uppgifter för statliga myndigheter. Samverkan, såväl innan som under en kris, är dock en central aspekt inom svensk krisberedskap. För att åstadkomma aktörsgemensam och effektiv inriktning och samordning krävs förberedelser innan en kris, genom planering, övning och annan samverkan. En aspekt som skulle kunna påverka beredskapsarbetet är att privata aktörers bidrag framför allt behöver bygga på frivillighet. Till skillnad mot i totalförsvarsplaneringen finns inte lagkrav på de privata aktörernas deltagande i krisberedskapsarbetet.[104] Beredskapsförordningen ger inte heller myndigheter föreskriftsrätt. I detta avseende är krishanteringens ansvarsprincip, och den utökning avseende samverkan som formulerats, inte bindande. Engagemanget bland privata aktörer är dock stort, men man förväntar sig att offentliga aktörer bidrar med tydlig inriktning. Det finns önskemål om att myndigheterna samordnar arbetet för att minska belastningen. En tillkommande roll för FI kan bli som försörjningsanalysmyndighet och möjligheten till samordning med rollen som beredskapsmyndighet och sektorsansvarig myndigheten behöver undersökas.

En fråga är vilka som ska delta i och bidra till den sammantagna beredskapsförmågan. En av målsättningarna med krisberedskapen är att upprätthålla samhällets funktionalitet, men det är inte givet vilka verksamheter och aktörer som bidrar till detta. Beredskapsförordningen är generell och uttrycker inte specifika samhällsviktiga funktioner.[105] Det pågår arbete för att identifiera aktuella verksamheter och de aktörer som då blir berörda. Myndigheter har bjudit in vissa privata aktörer som stöd i arbetet. Större aktörer har mer resurser för att delta, men samtidigt framkommer i intervjustudien att det är viktigt att olika perspektiv lyfts fram i arbetet och att en bredd av aktörer tillsammans kan bidra till uppbyggnaden. Exempelvis kan en totalt sett liten aktör vara av stor betydelse regionalt. I implementeringen av den nya riksbankslagen har man valt att först identifiera de som definitivt kommer att beröras och sedan eventuellt utöka kretsen. Valet är gjort bland annat för att få en mer hanterbar gruppstorlek i det initiala arbetet. I intervjuerna framkommer dock en förståelse för att strukturen måste byggas undan för undan.

I intervjuerna framkommer en förhoppning om att myndigheter kan stödja i omvärldsbevakning och hotbildsanalys. Det är något som flera aktörer inte genomför systematiskt, men som skulle kunna stärka det förebyggande och förberedande arbetet. Myndigheter får bland annat genom

---

[104] *I Lag (1982:1004) om skyldighet för näringsidkare, arbetsmarknadsorganisationer m.fl. att delta i totalförsvarsplaneringen beskrivs krav på och villkor för näringslivets deltagande avseende planering för totalförsvarsförmåga.*

[105] *Däremot återfinns i den nya riksbankslagen ett uttalat ansvar för att allmänheten ska kunna göra betalningar även i kris och krig.*

nationell samverkan ta del av hotbildsbeskrivningar som inriktning för beredskapsarbetet. En utmaning för samverkan avseende hotbild, kanske framför allt då frågorna även rör väpnat angrepp och totalförsvar, är informationsdelning och de krav som ställs på informationssäkerhet och säkerhetsskydd hos deltagande aktörer.

Privata aktörer har lyft oklarheter avseende myndighetsuppgifter som ges inom ramen för olika lagrum; i beredskapsarbetet ska potentiella sårbarheter identifieras vilket befaras kunna leda till sanktionsavgifter om myndigheten även har en tillsynsroll. Detta behöver diskuteras för att inte hämma samverkan.

11 Referenslista

Arbetsmarknadsdepartementet (2023), Kommittédirektiv 2023:76 Arbetslöshetsförsäkringen vid störda förhållanden, allvarlig fredstida kris, höjd beredskap och ytterst krig

Buzan mfl (1998). Security: a new framework for analysis

Egnell (2017), Vad är mänsklig säkerhet? (manskligsakerhet.se)

EU-kommissionen (2023), Kommissionens riktlinjer för tillämpningen av artikel 4 (1) och (2) i direktiv (EU) 2022/255 (NIS2-direktivet)

Europaparlamentet (2009), Europaparlamentets och rådets direktiv 2009/138/EG om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II)

Europaparlamentet (2013), Europaparlamentets och rådets direktiv 2013/36/EU om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag

Europaparlamentet (2014), Europaparlamentets och rådets direktiv 2014/65/EU om marknader för finansiella instrument.

Europaparlamentet (2014), Europaparlamentets och rådets direktiv 2014/59/EU av den 15 maj 2014 om inrättande av en ram för återhämtning och resolution av kreditinstitut och värdepappersföretag

Europaparlamentet (2019), Europaparlamentets och rådets direktiv (EU) 2019/452 av den 19 mars 2019 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen

Europaparlamentet (2021), Förslag till Europaparlamentets och rådets direktiv om harmoniserade regler för artificiell intelligens, COM/2021/206 final

Europaparlamentet (2022), Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011

Europaparlamentet (2022), Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)

Europaparlamentet (2022), Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG

European Banking Authority (2019), EBA Guidelines on outsourcing arrangements, EBA/GL/2019/02

Finansdepartementet (2022), Kommittédirektiv 2022:8 Inrättande av utbetalningsmyndigheten

Finansdepartementet (2022), Ökad motståndskraft i betalningssystemet, Fi2022/02529

Finansdepartementet (2023), Uppdrag om operativ krisledning vid allvarliga störningar i den finansiella sektorns digitala infrastruktur, Fi2023/01842

Finansiella stabilitetsrådet (2016), Överenskommelse om samarbete avseende finansiell stabilitet och krishantering

Finansinspektionen (2014), Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:4) om hantering av operativa risker

Finansinspektionen (2014), Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:1) om styrning, riskhantering och kontroll i kreditinstitut

Finansinspektionen (2021), Finansinspektionens klimatanpassningsarbete, FI dnr 21-13007

Finansinspektionen (2023), Handlingsplan om att stärka kontrollen över de finansiella företagens utlagda verksamhet, Dnr 22-18123

FSPOS (2021), Identifiering och värdering av cyberrisker

FSPOS (2022), Perspektiv på samhällsviktig verksamhet

FSPOS (2023) Aktuella planeringsförutsättningar för finansiella sektorns arbete med civilt försvar

Försvarsberedningen (2017), Motståndskraft – inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025, Ds 2017:66

Försvarsberedningen (2023), Allvarstid. Försvarsberedningens säkerhetspolitiska rapport, Ds 2023:19

Försvarsdepartementet (2023), Kommittédirektiv 2023:30

Försvarsmakten och MSB (2021), Handlingskraft Myndigheten för samhällsskydd Handlingsplan för att främja och utveckla en sammanhängande planering för totalförsvaret 2021-2025, FM2021-l 7683:2 MSB2020-l6261-3

Försäkringskassan (2021), Delredovisning avseende Uppdrag att erbjuda samordnad och säker statlig IT-drift, FK 2020-001438

Försäkringskassan (2022), Årsredovisning 2022

Försäkringskassan (2023), FK 2022/02371

Infrastrukturdepartementet (2020), Förordning om artificiell intelligens, Fakta-pm om EU-förslag 2020/21:FPM109 : COM(2021) 206)

Jonsson (2018), Typfall 5: utdragen och eskalerande gråzonsproblematik. Komplettering av hotbildsunderlag i utvecklingen av civilt försvar, FOI Memo 6338.

Jonsson (2018) Gråzonsproblematik och hybridkrigföring – påverkan på energiförsörjning, FOI-R--4590-SE

Jonsson mfl (2019), Civilt försvar i gråzon, FOI-R--4769--SE

Jonsson mfl (2023), Gråzonslägen i krig och fred, FOI-R--5447--SE

Justitiedepartementet (2016), Nationell strategi för samhällets informations- och cybersäkerhet, Skr. 2016/17:213

Justitiedepartementet (2018), Ansvar, ledning och samordning inom civilt försvar, Dir. 2018:79

Justitiedepartementet (2021), Raminstruktion för det svenska civila beredskapsarbetet inom ramen för Nato/PFF, Ju2021/00361

MSB (2014), Övergripande inriktning för samhällsskydd och beredskap, 2014-1942

MSB (2016), MSB:s föreskrifter för statliga myndigheters risk- och sårbarhetsanalyser, MSBFS 2016:7

MSB (2017), Nationella risk- och förmågebedömningen 2017, MSB1102

MSB (2018), Gemensamma grunder för samverkan och ledning vid samhällsstörningar, MSB777

MSB (2021), Övningsinriktning för bevakningsansvariga myndigheter på nationell och regional nivå avseende samverkansövningar under 2022–2026, MSB 2021-06744

MSB (2021), Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, MSBFS 2021:9

MSB (2022), Civilt försvar mot 2030 – ett totalförsvar i balans, MSB2095

MSB (2023), Lista med viktiga samhällsfunktioner, MSB1844

MSB (2023), Nationell risk och sårbarhetsbedömning, Dnr. MSB 2022-11265-23

MSB (2023), Nya perspektiv och utmaningar för civil beredskap i ett föränderligt klimat, MSB2178

MSB (2023), Planeringsinriktning för civil beredskap

MSB (2023), Policyöversikt: Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete

MSB (2023), Vägledning - planering för civil beredskap: process och metod, MSB2167

NCSC (2023), Delredovisning av regeringsuppdrag: Uppdrag att inom ramen för Nationellt cybersäkerhetscenter stärka samverkan med näringslivet

Olsén mfl (2022), Utveckling av förmåga för krisberedskap och civilt försvar, FOI-R--5287—SE

Regeringen (2020), Regeringens proposition 2020/21:1

Regeringen (2020), Lagrådsremiss Tystnadsplikt vid teknisk bearbetning och lagring

Regeringen (2023), Lagrådsremiss Nya regler för clearingorganisationer

Regeringen (2023), Regeringens skrivelse 2023/24:26 Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet

Riksbanken (2019), Klimatrelaterade risker är en källa till finansiella risker, fördjupning i Finansiell stabilitetsrapport 2019_2

Riksbanken (2019), Ekonomisk kommentar, nr 3 2019, Bankpaketet – på väg till Sverige

Riksbanken (2023), Staff Memo Cyberrisker och finansiell stabilitet

SOU 2015:25, En ny säkerhetsskyddslag

SOU 2018:25, Juridik som stöd för förvaltningens digitalisering

SOU 2019:51, Näringslivets roll inom totalförsvaret

SOU 2020:11, Delbetänkandet Kompletterande bestämmelser till EU:s förordning om utländska direktinvesteringar

SOU 2021:25, Struktur för ökad motståndskraft

SOU 2021:87, Granskning av utländska direktinvesteringar

SOU 2021:97, Säker och kostnadseffektiv IT-drift – förslag till varaktiga former för samordnad statlig IT-drift

SOU 2023:16, Staten och betalningarna

SOU 2023:50, En modell för svensk försörjningsberedskap,

Svenska bankföreningen (2023), Hotbildsbedömning för Sveriges banker

Svenska bankföreningen (2023), REMISSYTTRANDE Bankföreningens synpunkter på Riksbankens föreskrifter om civil beredskap för betalningar, 2023/06/001

Svenska bankföreningen (2023), FRAMSTÄLLNING Diarienr: 2023/11/005

Bilaga 1: Intervjuguide

Respondentens bakgrund

- Namn och roll/ansvarsområde?
- Kunskap/erfarenhet av arbete inom krisberedskap, själv respektive i organisationen?

Hotbild

- Följer ni/tar ni del av analyser av hotbildsutvecklingen?
- Har ni vidtagit åtgärder med hänsyn till rådande hotbild?

Krisberedskap och strukturreformen

- Har synen på krisberedskap och er organisations roll i den förändrats de senaste åren?
- Har dimensionen civil beredskap beaktats i er organisation? Hur?
- Hur anser du att beredskapsarbetet inom sektorn fungerar; styrkor/brister, förslag på utveckling?
- Har strukturreformen och den nya beredskapsförordningen påverkat systemet än?
- Vad är mest angeläget att arbeta med för sektorn ska fungera?
- Vilken roll anser du att respektive typ av aktör bör ta i det nya systemet?
- Kan arbetet bedrivas i befintliga fora (FSPOS, andra) eller behövs nya, exempelvis specifika arbetsgrupper? I så fall avseende vilka teman?
- Hur kan din organisation bäst bidra?
- Bedriver din organisation eller har ni behov av samverkan avseende krisberedskap med aktörer utanför sektorn?

Cybersäkerhet

- Ser ni att det nationella cybersäkerhetscentret (NCSC) kommer att påverka ert cybersäkerhetsarbete? Kommer samverkan att förändras?
- NIS2/CER: Analyserar ni kommande krav utifrån er verksamhet? Enskilt eller i samverkan?
- DORA: ser ni utmaningar och framgångsfaktorer för att anpassa er verksamhet till DORA-kraven? Går det att integrera i annat cybersäkerhetsarbete?

Betalningar

- Vilka kriterier skulle kunna vägleda bedömningen av verksamhet som är av särskild betydelse för genomförandet av betalningar?
- Om ni skulle bli utpekade, har ni någon uppfattning vad det skulle innebära? Resursåtgång, behov av finansiering mm?
- Upplever ni ansvarsfördelningen för civil beredskap på betalningsområdet tydlig mellan FI och Riksbanken? Hur påverkas ni av den?

Säkerhetsskydd

- Bedömer ni att ni berörs av den nya säkerhetsskyddslagen?
- Hur arbetar ni i så fall med säkerhetsskydd? Internt och i samverkan?

Nato

- Bedömer ni att ett Natomedlemskap kommer att påverka er organisation/finansiell sektor? I så fall hur?

Organisationens helhetsgrepp om resiliens

- Används begreppet resiliens i er organisation? I vilken bemärkelse och hur arbetar ni med det?
- Hur arbetar er organisation med berörda områden, koordinerat eller separat?
- Är det väl anpassat för att möta kraven?
- Om du blickar framåt, hur tror du att er organisations arbete med ovan nämna områden behöver förändras, internt respektive i samverkan? Varför?

Övrigt

- Något att tillägga, något vi glömt att fråga om?