Enheten för planering och uppföljning (LS-PU)
Ledningsstaben
Fredrik Magnusson
010-240 5035
Fredrik.Magnusson@msb.se

Regeringskansliet
Försvarsdepartementet
103 33 Stockholm

SOU 2025:79 Samlade förmågor för ökad cybersäkerhet

Sammanfattning

Myndigheten för samhällsskydd och beredskap (MSB) bejakar utredningens förslag om att all verksamhet inom informations- och cyberverksamhet som idag bedrivs vid MSB ska föras över till FRA. MSB anser att det är väsentligt att all verksamhet samlas hos en myndighet.[1]

MSB betonar vikten av att informations- och cybersäkerhetesfrågorna, även vid en verksamhetsövergång till FRA, fortsatt hanteras i inom ramen för beredskapssystemet och framför allt i den aktörsgemensamma hanteringen av händelser i hela hotskalan.

MSB anser att utredningen inte tillräckligt belyst hur övriga uppgifter och verksamhet som MSB bedriver påverkas när informations- och cyberverksamheten inte längre är en del av myndighetens verksamhet. Det kommer som MSB bedömer det krävas omfattande myndighetsinitierad samverkan och informationsdelning mellan MSB och FRA framöver.

Föreslagen tidpunkt för verksamhetsövergång, den 1 juli 2026, förutsätter att regeringen fattar beslut om vilken verksamhet som ska föras över från MSB till FRA senast i december 2025 så att det finns möjlighet att genomföra alla verksamhets- och personalprocesser i tid.

Avsnitt 3.3.3 samt 3.3.4 om föreskriftsrätt och tillsynssamordning

MSB tillstyrker utredarens förslag att såväl föreskriftsrätt enligt förordningen om cybersäkerhet som tillsynssamordning enligt samma förordning ska föras över till FRA. MSB anser att dessa uppgifter kräver tillgång till experter som endast FRA kommer att ha efter verksamhetsöverföringen. För att samhället ska kunna ha en tillfredsställande cybersäkerhet är det av största vikt att en aktör har det samlade ansvaret och därigenom tas ett helhetsansvar, inte bara för att det finns föreskrifter och bedrivs tillsyn.

Avsnitt 3.3.6 om att FRA ska ges föreskriftsrätt enligt beredskapsförordningen

Utredaren föreslår att FRA ska ta över föreskriftsrätten enligt 13 och 14 §§ förordningen (2022:524) om statliga myndigheters beredskap. Därmed blir det ett delat föreskriftsansvar

[1] Den 1 januari 2026 ombildas MSB till Myndigheten för civilt försvar. I yttrandet används myndighetens nuvarande namn genomgående.

i förordningen vilket ställer särskilda krav på en nära dialog mellan MSB och FRA i arbetet med nya eller förändrade föreskrifter.

För att hantera detta föreslår MSB att FRA:s föreskriftsmandat kompletteras med att MSB får yttra sig över föreskriftsförslagen.

Avsnitt 4.2 Uppgiftsskyldighet vid samverkan inom NCSC

Idag när informations- och cybersäkerhetsverksamheten är en del av MSB kan information och uppgifter vid behov delas till andra delar inom myndigheten utan att hindras eller försvåras av sekretess mellan myndigheter. När cybersäkerhetsverksamheten blir en del av FRA behöver hänsyn tas till offentlighets- och sekretesslagen (OSL) innan uppgifter delas. Detta innebär att information som kan vara till nytta för andra delar av MSB:s verksamheter tar längre tid att nå dessa verksamheter eller i vissa fall inte delas alls med hänvisning till sekretess.

Överföringen av verksamhet kan innebära att den kunskap och information som kommer från tillsynsmyndigheternas erfarenheter, inkomna incidentrapporter men även den kontaktyta med näringslivet som Cybersäkerhetslagen ger, inte kommer MSB och det civila beredskapssystemet tillgodo på samma sätt som tidigare.

Sammantaget innebär det att MSB riskerar att få mindre och mer filtrerad information rörande informations- och cybersäkerhet än idag vilket kan begränsa flera av MSB:s uppdrag: leda hantering och samordning av händelser, lämna samlad lägesbild till regeringen, Nationell risk och sårbarhetsbedömning och bedömning av det civila försvarets förmåga, rymdfrågor och särskilda uppdrag rörande hybridhot och skydd av undervattensinfrastruktur med flera.

För att MSB ska kunna lösa sina uppgifter kommer det att behövas en överenskommelse mellan myndigheterna om informationsdelning (inklusive sådana uppgifter som omfattas av sekretess). Om en sådan överenskommelse inte kommer till stånd eller blir för svag utesluter inte MSB att det kan behöva tillkomma reglering i författning istället.

Avsnitt 5.3.1 FRA är inte en del av beredskapssystemet

Det svenska samhället är i hög grad digitaliserat. Ett systematiskt arbete med informations- och cybersäkerhet har en avgörande roll för att en trovärdig totalförsvarsförmåga ska kunna uppnås. Detta gäller såväl hos staten, kommuner, regioner och näringsliv. Det handlar bland annat om att kunna hantera angrepp inom informations- och kommunikationsområdet samt upprätthålla en aktuell lägesbild över samhällets digitala miljö. Perspektivet digitalisering och cybersäkerhet är således viktigt för hela det civila försvaret, inte bara MSB.

Utredarens förslag innebär att centrala civila delar av informations- och cyberverksamheten flyttas in det militära försvarsområdet och därmed bort från det civila försvaret. FRA kommer dock att behöva ha en nära relation med det civila beredskapssystemet, till exempel genom att vara en del av det civila beredskapsrådet, utan att myndigheten formellt pekas ut som beredskapsmyndighet. MSB kommer också att ta initiativ till att adjungera in FRA i alla de övriga strukturerna för samordning och

incidenthantering som finns för arbetet med civilt försvar och krisberedskap. Det är därför mycket viktigt att FRA avsätter resurser för denna typ av deltagande i det civila beredskapssystemet.

Avsnitt 5.4 verksamhetsmässiga konsekvenser för MSB

Utredaren uttrycker att den verksamhetsmässiga konsekvensen för MSB att tappa cyber- och informationssäkerhetsverksamheten endast är att ”MSB får ett mer koncentrerat uppdrag”. Som framgår av MSB:s remissvar är konsekvenserna större än så.

Ytterligare en aspekt är att kunskap och kompetens inom cyber- och informationssäkerhet behövs inom flera delar av MSB uppdrag även efter en verksamhetsöverföring. Denna kompetens behöver byggas upp inom ramen för kvarvarande verksamheter i MSB som kompensation för att det inte längre går att hämta expertisen inom myndigheten.

MSB saknar dock resurserna inom befintligt anslag för att bygga upp sådan kompetens.

Avsnitt 5.5.3 Samordningen av NIS 2- och CER-direktiven

Ansvar för hantering av en incident

Utredningen konstaterar att det kan uppstå vissa gränsdragningsproblem om vilken myndighet som är ansvarig för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Som en konsekvens av den föreslagna fördelningen av NIS2-direktivets uppgifter enligt vilken FRA föreslås bli cyberkrishanteringsmyndighet kan FRA:s ansvar för att hantera storskaliga cybersäkerhetsincidenter och kriser komma i konflikt med MSB:s ansvar som ytterst ansvarig myndighet inom beredskapssystemet med ansvaret för samordningen av samhällets samlade insatser vid en störning i en samhällskritisk verksamhet.

Sverige behöver förhålla sig till de allt tydligare krav och förväntningar som ställs på medlemsstaterna inom EU:s struktur för cyberkrishantering, bland annat förmåga att representera hela beredskapsstrukturen vid en cyberkris som involverar flera medlemsstater. MSB har regeringens uppdrag att oavsett typ av samhällsstörning ha det sammanhållande ansvaret för samordning och hantering. Om FRA ensamt utnämns till cyberkrishanteringsmyndighet enligt NIS2-direktivets art. 9 så ska FRA ha det sammanhållande ansvaret för samordning och hantering av samhällsstörningar som orsakas av it-incidenter. Det orsakar en ineffektiv, och för utomstående aktörer svårförståelig, ordning som troligen kommer att hämma hanteringen av samhällsstörningar. Motsvarande rollfördelning har i Danmark hanterats genom att Beredskapsstyrelsen är cyberkrishanteringsmyndighet och det danska cybersäkerhetscentret tillhandahåller tekniskt operativt stöd vid storskaliga cyberincidenter och kriser.

Regeringen har enligt NIS2-direktivets art. 9 möjlighet att utse fler än en cyberkrishanteringsmyndighet. MSB rekommenderar därför att regeringen utser både FRA och MSB till cyberkrishanteringsmyndigheter och att cyberkrishanteringsuppgifterna i förordning fördelas på ett som gör att Sverige, via FRA och eventuellt med stöd av MSB, fortsatt kan fullgöra landets åtaganden inom cybersäkerhetsområdet i EU. Detta samtidigt

som MSB fortsatt, i nära samarbete med FRA och i så stor utsträckning som möjligt, kan vara den myndighet som leder samordningen av hantering av samhällsstörningar i Sverige.

Förvaltningen av NIS2 och CER direktiven kräver samordning och samarbete

Såväl regleringarna, NIS2 och CER, som berörda verksamhetsutövare är överlappande då it-incidenter är en av flera möjliga orsaker till störning i samhällsviktig verksamhet. MSB ser det därför som väsentligt att arbetet enligt respektive direktiv fortsätter att ske samordnat även efter en verksamhetsöverföring. I väntan på ny reglering har MSB använt befintliga NIS samarbetsfora för att diskutera och förbereda införande av ny reglering inom motståndskraft i samhällsviktig verksamhet. Förutom incidenthantering så är samordnad identifiering, anmälan och tröskelvärden för rapporteringspliktiga incidenter naturligt att reglera synkront i respektive författning. Det avser även informationsutbyte, utformning av information till verksamhetsutövare, tillsynssamordning etc. Det är en stor risk för otydligheter för tillsynsmyndigheter men framförallt för de aktörer som berörs av de båda regleringarna om förvaltningen av direktiven inte även fortsatt sker samordnat.

För att säkerställa att arbetet fortsätter ske samordnat kan regeringen reglera det, t ex i cybersäkerhetsförordningen och förmodat kommande ”förordning om motståndskraft hos kritiska verksamhetsutövare” eller i respektive myndighets instruktion.

Verksamhetsutövarnas perspektiv

De aktörer som tillhandahåller samhällsviktig verksamhet kommer att beröras av både NIS2 och CER. Vid en händelse är det viktigt att överföringen av verksamheten från MSB till FRA inte innebär otydligheter. Detta gäller särskilt incidentrapportering och att den aktör som har drabbats och sitter mitt i hanteringen av en störning inte ska behöva ha dubbla rapporteringsvägar.

Den samlade portal med smarta formulär för rapportering av incidenter, tillbud, sårbarheter och cyberhot under olika regelverk, primärt NIS 2- och CER-direktivet som MSB nu utvecklar syftar till att förenkla för och stödja verksamhetsutövarna. Den kommer innehålla funktionalitet för att bland annat dela incidentrapporter och annan kommunikation från verksamhetsutövarna med behöriga myndigheter enligt både NIS2 och CER samt i förlängningen utgöra ett tekniskt stöd för ledning och styrning av krisberedskap och civilt försvar. Etablerandet av en gemensam portal ligger även i linje med vad EU-kommissionen aviserat att man kommer att ställa krav på i kommande reglering.

För att undanröja otydlig ansvarsfördelning efter verksamhetsövergången välkomnar MSB att regeringen förtydligar i myndighetens instruktion att MSB även fortsättningsvis ska tillhandahålla en samlad portal för incidentrapportering enligt NIS2 och CER där övriga behöriga myndigheter har tillgång till inkomna incidentrapporter, anmälningar och annan information från verksamhetsutövarna. Det kan vidare förtydligas i cybersäkerhetsförordningen att den samlade portalen ska användas för incidentrapportering enligt cybersäkerhetslagen.

FRA bör medverka i granskningen av utländska direktinvesteringar

MSB:s cybersäkerhetsverksamhet har medverkat i arbetet med granskningar av utländska direktinvesteringar i skyddsvärd kritisk infrastruktur och samhällsviktig verksamhet. Verksamhetens cyberkompetens har möjliggjort för MSB att lämna relevanta bedömningar, av sårbarheter och risker, kopplade till enskilda direktinvesteringar i företag verksamma inom it/ot-området. Behov av granskningsstöd med specifikt cybersäkerhetskompetens kommer finnas även framgent. Då kompetensen i dessa frågor förs över till FRA bör regeringen överväga att lägga till FRA till de myndigheter som räknas upp i 6 och 7 §§ förordningen (2023:624) om granskning av utländska direktinvesteringar.

Avsnitt 5.7.1 Ekonomiska konsekvenser av förslagen om överföring av uppgifter

Överföringen kommer innebära merkostnader inte minst på kort sikt när FRA ska bygga upp ny verksamhet och viss verksamhet behöver dubbleras under en övergångstid. MSB kommer också behöva bygga upp kompetens och kapacitet som kompensation för verksamhet som övergår till FRA. Därutöver har regeringen aviserat ökade satsningar på informations- och cybersäkerhet.

Det är avgörande för den fortsatta uppbyggnaden av det civila försvaret att MSB:s anslag inte påverkas mer än motsvarande vad de direkta kostnaderna är för informations -och cyberverksamheten idag inom MSB. Satsningar på informations- och cybersäkerhet får inte ske på bekostnad av den övriga verksamhet MSB som bedriver. Regeringen har i budgetpropositionen för 2026 föreslagit att MSB anslag ska minska med 225 miljoner kronor på årsbasis och till det även en minskning med 45 miljoner avseende NCSC. MSB vill understryka att verksamheten idag inom MSB kostar 225 mnkr inklusive de medel myndigheten disponerar för NCSC. Vid en överföring av anslag från MSB till FRA måste det också beaktas att vissa av de medel MSB disponerar avseende cyber är tillfälliga satsningar från regeringens sida vilka upphör under 2026 och 2027. MSB betonar därför vikten av att anslagsbeloppet som ska föras över justeras i Vårändringsbudgeten.

Tidsförhållanden

Utredaren har föreslagit att verksamhetsövergången ska ske den 1 juli 2026.

En verksamhetsövergång den 1 juli 2026 innebär övergång mitt i ett budgetår och mitt i semesterperioden. Dessutom är tidpunkten nära det förestående valet. Samtidigt är det positivt med en snabb process ur ett bemanningsperspektiv då dagens osäkerhet om framtiden har negativ inverkan.

För att det ska vara möjligt att genomföra verksamhetsövergången den 1 juli 2026 måste regeringens beslut fattas i god tid för att bland annat de personalrelaterade processerna ska hinnas med. Det är exempelvis en utdragen process med flera formella steg för att överföra medarbetare från MSB till FRA där inte minst säkerhetsprövning är ett tidskrävande steg. Hinner inte säkerhetsprövningen blir klar i tid kommer det inte finnas personal tillgänglig när FRA tar över uppgifterna. MSB bedömer att ett beslut om vilken

verksamhet som ska vara föremål för övergång måste fattas senast i december 2025. Det är först när det finns ett beslut som många av åtgärderna kan påbörjas.

I detta ärende har generaldirektör Mikael Frisell beslutat. Fredrik Magnusson har varit föredragande. I den slutliga handläggningen har också stabschefen Anna Psaroulis, enhetschefen Göran Karlsson och avdelningschef Åke Holmgren deltagit.

Mikael Frisell

Fredrik Magnusson