

Kommittédirektiv

Uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet

Beslut vid regeringssammanträde den 14 november 2024

Sammanfattning

I Försvarsberedningens rapport Kraftsamling – Inriktningen av totalförsvaret och utformningen av det civila försvaret (Ds 2023:34) ifrågasätts om dagens myndighetsstruktur är ändamålsenlig för att uppnå en samlad och samordnad styrning av samhällets informations- och cybersäkerhetsarbete. Mot denna bakgrund ges en särskild utredare i uppdrag att utreda hur en överföring av arbetsuppgifter inom informations- och cybersäkerhet från Myndigheten för samhällsskydd och beredskap (MSB) till Försvarets radioanstalt (FRA) kan genomföras.

Utredaren ska bl.a.

- utreda och redovisa förutsättningarna för och konsekvenserna av en överföring av arbetsuppgifterna,
- analysera och bedöma hur överföring av uppgifter och ansvar för dessa påverkar samhällets motståndskraft på informations- och cybersäkerhetsområdet,
- analysera och föreslå vilka av MSB:s uppgifter inom informations- och cybersäkerhet som bör föras över till FRA, och
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 1 juli 2025.

Behovet av att se över ansvaret för vissa delar av samhällets informations- och cybersäkerhet

Det svenska samhället har i mycket snabb takt digitaliserats och näringslivet och samhällsviktiga tjänster är i dag beroende av digitala lösningar. Det har inneburit nya sårbarheter eftersom automatisering och digitalisering av alltifrån betalfunktioner till vatten- och avloppssystem gjort oss mer utsatta för t.ex. systemfel i den digitala miljön och cyberattacker. Med hänsyn till det allvarliga säkerhetsläget behöver en förändring ske snabbt. Arbetet med att ständigt effektivisera den samhällsviktiga infrastrukturen måste i största möjliga utsträckning anpassas efter vilka säkra digitala lösningar som finns tillgängliga.

I takt med samhällets ökande digitalisering är det viktigt att inte tappa fart i arbetet med att förebygga, upptäcka, stå emot och hantera problem som uppkommer när informations- och cybersäkerheten brister. Regeringen bedömer att dagens befintliga myndighetsstruktur när det gäller informations- och cybersäkerhet inte är ändamålsenlig utan behöver ses över för att bli mer samlad och funktionell.

Uppdraget att föreslå en ny struktur för en samlad styrning av vissa delar av informations- och cybersäkerhet

Informations- och cybersäkerhet är en grundläggande del av samhällets funktionalitet och har stor inverkan på näringslivet och medborgarnas vardag som helhet. För att stärka samarbetet mellan myndigheter och näringsliv och förbättra kunskapen om hur samhället på bästa sätt kan värnas vid cyberangrepp, samt för att skydda samhället vid andra större störningar, krävs att det finns såväl förmåga som adekvat stöd för att motstå, hantera och snabbt agera på händelser i cybermiljön. Detta är särskilt viktigt när cyberangrepp sker vid en kris, höjd beredskap eller i krig.

MSB och FRA har båda omfattande uppgifter inom informations- och cybersäkerhet. Enligt sin instruktion ska FRA ha hög teknisk kompetens inom informationssäkerhetsområdet och får efter begäran stödja andra myndigheter och enskilda verksamhetsutövare på området, bl.a. genom att ge tekniskt stöd. MSB har i uppgift att stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och

regioner samt till företag och organisationer. Båda myndigheterna arbetar således med att stärka samhällets motståndskraft på cybersäkerhetsområdet.

År 2020 gav regeringen FRA, Försvarmakten, MSB och Säkerhetspolisen i uppdrag att fördjupa samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter (NCSC) (beslut den 10 december 2020, Fö nr 8). Regeringen angav att dessa myndigheter skulle ha en nära samverkan med Försvarets materielverk, Polismyndigheten och Post- och telestyrelsen. Syftet med uppdraget var att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot. En utredare har biträtt Försvarsdepartementet med att lämna förslag på hur en ändamålsenlig och effektiv ledning, organisering och styrning av NCSC kan utformas och föreslår bl.a. att FRA ska få ett huvudmannaskap för NCSC (Fö2024/00785). Förslagen har remitterats. FRA har efter en ändring av myndighetens instruktion, som beslutades den 19 september 2024, huvudmannaskap för NCSC från och med den 1 november 2024. Övriga förslag bereds inom Regeringskansliet.

Det finns skäl att i större uträkning än i dag – och med en bredare ansats än den tidigare utredningen hade i uppgift att föreslå – samla uppdrag och arbetsuppgifter rörande informations- och cybersäkerhet hos en och samma myndighet i syfte att uppnå ett mer ändamålsenligt informations- och cybersäkerhetsarbete. För att åstadkomma detta ska centrala delar av de arbetsuppgifter inom informations- och cybersäkerhet som MSB har i dag föras över till FRA. Utredaren ska därför undersöka och lämna förslag på vilka av MSB:s uppgifter rörande informations- och cybersäkerhet som bör överföras till FRA. En utgångspunkt för utredaren ska vara att en organisatorisk åtskillnad mellan stödjande verksamhet och tillsynsverksamhet inom cybersäkerhetsområdet ska upprätthållas. Utredaren ska säkerställa en tydlig ansvarsfördelning, utan överlapp eller dubblering av uppgifter och ansvar, och att verksamheten kan bedrivas effektivt utifrån de behov som finns att samla informations- och cybersäkerhetsfrågorna.

Samhällets behov av snabb och säker information om pågående it-incidenter är omfattande och ökar i takt med digitaliseringen. FRA behöver därför vid en överföring av uppgifter ha möjlighet att förmedla råd och stöd avseende hot, sårbarheter och risker. Vid en överföring av uppgifter behöver dessa behov tillgodoses och utredaren ska därför utreda vilka förutsättningar FRA

behöver för att kunna genomföra denna uppgift, i fråga om t.ex. personalresurser och lokaler.

MSB är Sveriges nationella CSIRT (computer incident response team) vilket innebär att myndigheten bl.a. har i uppgift att ta emot och hantera incidentrapporter från leverantörer enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen). Eftersom verksamheten som CSIRT-enhet regleras av Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet) omfattas den av tillsyn från Europeiska unionens revisionsrätt i enlighet med artikel 287 i fördraget om Europeiska unionens funktionssätt. Det finns även möjlighet för MSB att ta emot finansiering från EU för denna verksamhet.

EU har enligt artikel 4.2 i fördraget om Europeiska unionen som huvudregel inte kompetens inom områden som rör medlemsstaternas nationella säkerhet eller försvar. Den största delen av FRA:s verksamhet, signalspaning i försvarsunderrättelseverksamhet, är sådan verksamhet som inte omfattas av EU:s kompetens. Det är viktigt att denna verksamhet även fortsatt kan bedrivas utan krav på ytterligare reglering eller insyn från EU. De övriga uppgifter hos MSB som omfattas av EU-lagstiftning granskas också av Europeiska unionens revisionsrätt. Revisionsrätten kan ta del av granskningar av verksamheten som ansvarig tillsynsmyndighet har genomfört. Det gäller i synnerhet om verksamheten utvecklas med stöd av EU-finansiering. Dessa förhållanden kvarstår även om verksamheten flyttas till annan myndighet.

Det är viktigt att överföringen av uppgifter genomförs på ett sätt som möjliggör att de delar av FRA:s verksamhet som rör nationell säkerhet och försvar inte omfattas av krav på insyn från EU.

Både MSB och FRA, var för sig och inom ramen för NCSC, spelar en viktig roll för svensk utrikes- och säkerhetspolitik på cyberområdet. Bland annat utgör MSB svensk teknisk kontaktpunkt i cyberarbetet inom Organisationen för säkerhet och samarbete i Europa (OSSE). Utredaren bör beakta hur en överföring av arbetsuppgifter kan bidra till ett mer samlat internationellt företrädeskap i cyberfrågor på myndighetsnivå.

Utredaren behöver även analysera om informationshantering som krävs med anledning av överföringen av arbetsuppgifter till FRA och NCSC medför något behov av ändringar i offentlighet- och sekretesslagstiftningen eller av regelverket som gäller för personuppgiftsbehandling. Utredaren behöver bl.a. ta ställning till om det finns förutsättningar för nödvändigt utbyte av information mellan MSB och FRA i samband med och efter överföringen av arbetsuppgifter. Utredaren behöver även analysera om det finns förutsättningar för att genomföra nödvändigt informationsutbyte mellan FRA och privata aktörer. I uppdraget ingår därmed bland annat att ta ställning till om nu gällande regelverk innebär ett tillräckligt skydd för uppgifter som kommer att utbytas.

Utredaren ska därför

- analysera och föreslå vilka uppgifter på informations- och cybersäkerhetsområdet hos MSB som bör föras över till FRA eller NCSC vid FRA, och när en sådan överföring kan och bör genomföras,
- analysera och föreslå hur överföringen från MSB till FRA av aktuella uppgifter kan genomföras,
- analysera och lämna förslag på hur FRA efter en överföring av uppgifter kan tillgodose regeringens och samhällets behov av snabb och säker information om cyberincidenter,
- analysera och föreslå hur rapportering och uppföljning av informations- och cybersäkerhetsverksamheten vid en överföring av uppgifter kan struktureras så att verksamheten blir möjlig för regeringen att följa upp över tid,
- analysera och lämna förslag på hur en överföring av uppgifter kan ske utan att Sveriges möjligheter att uppfylla sina EU-rättsliga förpliktelser eller få del av EU-rättsligt stöd påverkas,
- analysera om det finns behov av ändringar i offentlighets- och sekretesslagstiftningen och regelverket som gäller för personuppgiftsbehandling,
- analysera vilka följder en överföring av uppgifter får när det gäller FRA:s behov av personalresurser och lokaler,
- vid behov föreslå åtgärder för en fördjupad samverkan inom ramen för NCSC, och
- lämna nödvändiga författningsförslag.

Utredaren ska i analys och förslag säkerställa att en överföring av uppgifter inte inverkar negativt på de delar av FRA:s verksamhet som rör nationell säkerhet och försvar.

Konsekvensbeskrivningar

Utredaren ska i enlighet med kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar ange kostnadsberäkningar och andra konsekvensbeskrivningar för sina förslag.

Utredaren ska

- i sina överväganden och förslag särskilt beakta de konsekvenser för MSB respektive FRA som en överföring av uppgifter får för respektive myndighets övriga uppdrag,
- klargöra vad en överföring av uppgifter medför för konsekvenser när det kommer till hanteringen av säkerhetskyddsfrågor inom verksamheten,
- analysera vilka rättsliga konsekvenser, både nationella och EU-rättsliga, som en överföring av arbetsuppgifterna innebär,
- särskilt beakta konsekvenserna i förhållande till genomförandet av Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet), samt
- analysera och redovisa de verksamhetsmässiga och personella konsekvenserna av förslagen som lämnas.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och kommittéväsendet. Utredaren ska särskilt beakta arbetet med att ta hand om förslagen i promemoriorna Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning och Ett nytt Nationellt cybersäkerhetscenter, Förutsättningar för en effektiv verksamhet (Fö2024/00785). Utredaren ska också beakta arbetet med att ta om hand förslagen i betänkandena Nya regler om cybersäkerhet (SOU 2024:18) och Motståndskraft i samhällsviktiga tjänster (SOU 2024:64).

Utredaren ska ha en nära dialog med MSB och FRA och kontakter bör även tas med andra myndigheter och organisationer som på olika sätt berörs av de

frågeställningar som uppdraget omfattar, bl.a. de myndigheter som är tillsynsmyndigheter enligt NIS-direktivet. Utredaren ska ha en nära dialog med Arbetsgivarverket i arbetsrättsliga frågor. Utredaren ska fortlöpande hålla Regeringskansliet (Försvarsdepartementet) informerat om det löpande arbetet.

Utredaren får även ta upp och lämna förslag i andra frågor än de som nämns i dessa direktiv om frågorna har samband med uppdraget och det ändå kan redovisas i tid.

Uppdraget ska redovisas senast den 1 juli 2025.

(Försvarsdepartementet)