Kontaktperson RISE
Johan Rosell
Centrum för cybersäkerhet, RISE
+46 10 228 49 56
johan.rosell@ri.se

Datum
25-09-30

Beteckning
Fö2025/01133

Försvarsdepartementet
fo.remissvar@regeringskansliet.se
fo.ech.remissvar@regeringskansliet.se

Yttrande över betänkandet Samlade förmågor för ökad cybersäkerhet (SOU 2025:79)

RISE Research Institutes of Sweden AB (RISE) har beretts tillfälle att yttra sig över betänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79). Efter en genomgång av utredningens förslag, utförd av våra experter inom cybersäkerhet, innovation och digitalisering, lämnar vi härmed följande yttrande.

I beredningen av detta ärende har Hanifeh Khayyeri, Andreas Aurelius, Carl Heath, Johanna Parikka Altenstedt och Johan Rosell deltagit.

1. Sammanfattande ställningstagande

RISE tillstyrker i allt väsentligt utredningens förslag att överföra Myndigheten för samhällsskydd och beredskaps (MSB) centrala cybersäkerhetsuppdrag till Försvarets radioanstalt (FRA) och att organisera verksamheten inom det nationella cybersäkerhetscentret, NCSC. Utredningen visar på ett tydligt och väl underbyggt behov av en samlad kontaktpunkt. Dagens delade ansvar har skapat en osäkerhet hos både offentliga och privata aktörer kring ansvarsfördelning och kontaktvägar, vilket RISE i vår breda samverkan med svenskt näringsliv och offentlig sektor kan bekräfta. En konsolidering av de centrala funktionerna stärker Sveriges förmåga att på ett sammanhållet sätt tillämpa EU:s cybersäkerhetsramverk som innehåller bl a de viktiga regelverken NIS 2-direktivet, DORA, AI Act, Cybersäkerhetsförordningen och CRA, och agera som en tydlig part i internationella samarbeten.

Samtidigt vill RISE understryka att reformens framgång är beroende av att den nya strukturen förmår att upprätthålla och utveckla transparens, tillit och civil innovationskraft. För att Sverige ska kunna bygga en långsiktig och dynamisk motståndskraft krävs att NCSC i den mån det är möjligt bedriver sin verksamhet öppet gentemot näringsliv, akademi och civilsamhälle. Detta är en förutsättning för att attrahera EU-medel och ingå i de forsknings- och innovationskonsortier som driver utvecklingen framåt inom cybersäkerhet.

RISE är, i egenskap av Sveriges forskningsinstitut och innovationspartner, redo att erbjuda konkret och strategiskt stöd i den förestående övergången. Detta innefattar bland annat tillgång till vår nationella test- och övningsmiljö Cyber Range, våra etablerade europeiska forskningsnätverk och vår kompetens inom standardisering och ekosystembyggande.

Därtill ligger European Cybersecurity Competence Centre and Networks, ECCC:s, svenska verksamhet med kompetensgemenskapen Cybernode placerad på RISE. Cybernode samlar näringslivet, myndigheter, kommuner, regioner, science parks och branschorganisationer kring aktuella och brännande cybersäkerhetsfrågor, informerar om EU:s utlysningar samt faciliterar

innovation särskilt inom produkt- och tjänsteutvecklingen som företas bland SME:er. Detta är en EU-reglerad funktion tillsammans med NCC-SE hos MSB och styrs direkt av unionens ECCC -myndighet. Den svenska Cybernoden är idag den största inom EU. Därmed behöver man notera att Cybernode inte är en myndighet och begrunda hur man bäst bibehåller kvaliteten och öppenheten i denna verksamhet, som kan vara värdefull för NCSC genom den direkta kopplingen till en kritisk massa av aktörer.

2. Övergripande synpunkter och rekommendationer

2.1 NCSC:s roll som öppet nav och behovet av balanserad styrning

2.1.1 En ändamålsenlig samordning

Utredningens förslag att låta FRA axla rollerna som CSIRT-enhet, gemensam kontaktpunkt och cyberkrishanteringsmyndighet är välgrundat och står i linje med regeringens nationella strategi för cybersäkerhet. En samlad huvudman skapar den klarhet och det entydiga ansvar som är nödvändigt. Den avgörande utmaningen blir dock att i praktiken balansera FRA:s sekretesspräglade underrättelsekultur med den öppenhet, tillgänglighet och serviceorientering som NCSC:s uppdrag som ett nav för hela samhället kräver. Förtroendet från näringslivet vinns inte enbart genom juridiskt skydd, utan genom en upplevd neutralitet och en kultur av samarbete.

2.1.2 Förslag om rådgivande flerpartsorgan

För att aktivt stödja och institutionalisera denna nödvändiga öppenhet föreslår RISE att regeringen överväger att inrätta ett rådgivande flerpartsorgan, en *strategisk samverkansgrupp*, knuten till NCSC. Ett sådant organ, med representation från industri, forskningsinstitut, akademi och relevanta delar av civilsamhället, skulle kunna fungera som en viktig mekanism för att säkerställa att NCSC:s verksamhet är relevant för mottagarna, ge externa perspektiv på prioriteringar samt bidra till en transparent och gemensam planering för forskning, utveckling och innovation (FoI).

2.2 Överföring av NCC-SE och säkrad innovationsförmåga

2.2.1 Riskscenarier och kontinuitet

RISE stödjer den strategiska logiken i att samlokalisera Nationella samordningscentret (NCC-SE) med NCSC. Vi ser dock, i likhet med utredningen, en betydande risk i att ansvaret för civil förvaltningskompetens kring EU-bidrag och innovationsstöd överförs till en myndighet utan tidigare erfarenhet av detta. En utdragen startsträcka eller initiala administrativa flaskhalsar hos FRA riskerar att hämma svenska aktörers förmåga att söka och erhålla finansiering från program som Horisont Europa och DIGITAL, vilket skulle skada Sveriges innovationskraft inom ett kritiskt teknikområde. Som det konstaterats ovan är den svenska Cybernoden kontraktuellt kopplad till NCC-SE och utgör dess kompetensgemenskap inom cybersäkerhet och innovation. Beslut som berör NCC-SE kommer att påverka även Cybernoden och det behöver beaktas i sammanhanget.

2.2.2 Förslag om strategiskt partnerskap

För att hantera denna risk och säkerställa kontinuitet föreslår RISE att regeringen ger FRA ett tydligt mandat att teckna ett **strategiskt och flerårigt samarbetsavtal** med RISE. Genom ett sådant partnerskap kan FRA omedelbart dra nytta av RISE befintliga kompetens och processer för hantering av komplexa, EU-finansierade FoI-projekt. Detta skulle säkerställa att stödfunktioner och samordning inom ramen för bland annat Cybernoden kan fortgå utan

avbrott under övergångsperioden, och att FRA snabbt kan bygga upp sin egen långsiktiga förmåga.

En annan fråga som RISE skulle kunna bidra med genom sin breda och gedigna samhällsforskning är den stora ”elefanten i rummet” inom cybersäkerhet, nämligen kompetensbristen. Den svenska cybersäkerheten kommer framöver hänga lika mycket på att få fram adekvata utbildningar snabbt såväl för noviser som för personer redan aktiva inom arbetslivet om vi ska kunna nå våra mål med cybersäkerhet i tid. För detta krävs projekt, samarbeten och samverkan med olika myndigheter och utbildningsleverantörer. RISE kan bli kunskapsnoden på olika sätt för att bistå FRA med den här delen av viktig samhällsutveckling.

2.3 Implementering, resurser och tidsplan

2.3.1 Dimensionering av resurser och kompetens

Utredningen uppskattar att 85–100 medarbetare överförs till FRA. RISE bedömer att detta är en adekvat initial nivå för att hantera de direkta uppgifterna från MSB. Däremot kommer arbetsvolymen att öka betydligt när NIS 2-, CER- och DORA-förordningarna får fullt genomslag, tillsammans med nya krav från exempelvis Cyberresiliensakten och AI-akten. Regeringen bör därför budgetera för en **stegvis och flexibel resursdimensionering** fram till 2029. Denna personalförsörjning måste kompletteras med en nationell satsning på avancerad övning och validering. RISE test- och demonstrationsmiljöer, i synnerhet vår Cyber Range, utgör en befintlig nationell resurs som står till förfogande för att snabbt och effektivt höja NCSC:s och andra aktörers operativa kapacitet.

2.3.2 Finansiering och ikraftträdande

RISE instämmer i behovet av en anslagsomfördelning från MSB och noterar utredningens kostnadsuppskattning. För att säkerställa långsiktig hållbarhet och möta EU:s revisionskrav är det, som utredningen påpekar, av yttersta vikt att en modell för **särredovisning av civila och militära kostnader** inom FRA etableras.

Gällande tidsplanen bedömer vi att ett ikraftträdande den 1 juli 2026 är mycket ambitiöst. Med hänsyn till komplexiteten i systemmigrering, säkerhetsprövning, kulturbyggande och regelharmonisering förordar RISE en **etappvis implementering**. En sådan modell skulle kunna innebära en formell överföring under 2026, med målet att nå grundläggande operativ beredskap senast början av 2027 och full regelefterlevnad för de mest komplexa delarna under 2028.

3. Övriga synpunkter

RISE vill lyfta frågan om att på sikt även utreda möjligheten att utse FRA till nationell myndighet för cybersäkerhetscertifiering och föra över ansvaret för Sveriges certifieringsorgan för IT-säkerhet (CSEC) och Inspektionen för cybersäkerhetscertifiering (ICC) från FMV till NCSC på FRA. En sådan konsolidering skulle ytterligare bidra till en minskad fragmentisering och ökad effektivisering av frågor kopplade till cybersäkerhet i Sverige. För att beakta de krav på oberoende som EU:s cybersäkerhetsakt ställer på verksamhet som utfärdar cybersäkerhetscertifikat och verksamhet som innefattar tillsyn skulle en sådan förflyttning behöva utredas vidare och separeras från övrig verksamhet på NCSC.

Vi vet idag att de olika nordiska länderna har valt att bedriva cybersäkerhetsförvaltningen på olika sätt; Danmark har segmenterat uppgifterna och ansvaret branschvis, medan i Finland är ansvaret centralt medan uppgifterna decentraliserade till regioner. Genom RISE samarbete med sina motsvarigheter inom den övriga Norden kan viktig gränsöverskridande kunskap inom fältet genereras.

4. Avslutande bedömning

RISE välkomnar reformens övergripande mål att skapa ett sammanhållet och mer slagkraftigt nationellt cybersäkerhetscentrum. För att reformen ska lyckas och nå sin fulla potential krävs dock att den förstärkta statliga kontrollen och förmågan balanseras med ett medvetet arbete för att garantera och främja öppenhet, civil innovationsförmåga och ett starkt integritetsskydd.

Genom våra testmiljöer, vår tillämpade forskning och vår breda samverkan med näringsliv och myndigheter är RISE berett att bidra både operativt och strategiskt för att stödja FRA och NCSC under hela övergångsperioden och i det fortsatta arbetet för ett säkrare digitalt Sverige.

RISE ber regeringen att beakta de synpunkter och rekommendationer som redovisats ovan och står till förfogande för fortsatt dialog i dessa viktiga frågor.

Med vänlig hälsning,

Paul Halle Zahl Pedersen

Divisionschef, Digitala System

RISE Research Institutes of Sweden AB