YTTRANDE
Fö2025/01133

Till Försvarsdepartementet
fo.remissvar@regeringskansliet.se
Kopia till:
fo.ech.remissvar@regeringskansliet.se

Yttrande avseende Remiss av SOU 2025:79 – Samlade förmågor för ökad cybersäkerhet

Säkerhets- och försvarsföretagen (SOFF) och Teknikföretagen tackar för möjligheten att lämna synpunkter på SOU 2025:79 – Samlade förmågor för ökad cybersäkerhet.

SOFF är en branschförening för företag inom säkerhets- och försvarsområdet med verksamhet i Sverige. SOFF har idag +350 medlemsföretag som har verksamhet inom bland annat försvar, samhällssäkerhet, cybersäkerhet.

Teknikföretagen är arbetsgivar- och branschorganisation för Sveriges teknikindustri med ca 4 500 medlemsföretag. De står för en tredjedel av landets export och utvecklar världsledande varor och tjänster som bidrar till tillväxt, välstånd och lösningar på vår tids utmaningar.

Inledning

Vi välkomnar utredningens ambition att stärka Sveriges cybersäkerhetsförmåga genom en mer samlad styrning, tydligare ansvarsfördelning och bättre samarbete mellan offentliga och privata aktörer. Nedan lyfter vi våra viktigaste synpunkter.

Vikten av tydlighet, förutsebarhet och informationsdelning

Utredningen tar ett viktigt helhetsgrepp om cybersäkerheten genom att föreslå att delar av Myndigheten för samhällsskydd och beredskaps (MSB) informations- och cybersäkerhetsverksamhet flyttas till Försvarets radioanstalt (FRA), inom ramen för det nationella cybersäkerhetscentret (NCSC). Förändringen ger FRA möjlighet att tydligare prioritera cybersäkerhet. Detta kommer också innebära att myndigheten för samhällsskydd och beredskap (MSB) får större möjlighet att fokusera sin verksamhet kring krisberedskap och civilt försvar

Vi vill understryka vikten av att roll- och ansvarsfördelningen i det föreslagna systemet blir tydlig och förutsebar. Företag måste veta vilken myndighet som är kontaktpunkt vid olika typer av incidenter och hot, särskilt i verksamhet som är känslig för försvar och säkerhet. Det måste också vara klart för företagen vilka rapporteringsvägar som de har att förhålla sig till i varje given situation.

I sammanhanget vill vi också särskilt betona vikten av hur information delas. För att arbetet ska fungera effektivt behövs en samlad struktur där incidentrapporteringen hanteras av endast en myndighet. Det gör processen enklare och mer begriplig för företagen. Det finns en utpräglad oro att krav från olika myndigheter på snarlik incdentrapportering kommer medföra dubbelarbete och dyra administrativa processer som inte bidrar till högre cybersäkerhet.

Samtidigt med behovet om informationsdelning behöver det finnas möjlighet att upprätthålla sekretess. All information om inträffade cyberincidenter kan inte alltid offentliggöras. I vissa fall kan det skada enskilda företag och få negativa ekonomiska konsekvenser. Varje situation bör därför noggrant avvägas mellan behovet av öppenhet för att stärka samhällets säkerhet och behovet av att skydda enskilda aktörers verksamhet.

Kompetensförsörjning

En framgångsrik överföring av uppgifter från MSB till FRA förutsätter att befintlig kompetens, teknik och resurser vid MSB följer med till FRA. Det är vitalt att försvarsnära kompetens bevaras och förstärks. Försvarsrelaterade säkerhetskrav ställer ofta särskilda krav på både personal och teknik. En omorganisation får inte leda till kompetensförlust, då det kan få negativ påverkan på både det civila och militära försvaret. Det är därför avgörande att organisationer som lämnar över uppgifter till FRA – särskilt MSB – försörjs med ett adekvat övergångsstöd, inklusive kompetensförsörjning, teknisk infrastruktur och processer.

Privat-offentlig samverkan

Näringslivet är en väsentlig aktör i totalförsvaret och samhällskritisk infrastruktur. Många privata företag har ansvar för att motverka, eller påverkas direkt av, attacker och hot mot cybersäkerheten. Det är därför viktigt att det finns fora där frågor kring processer och rutiner kan tas upp och diskuteras mellan berörda myndigheter och företagen likväl som det skapas sådana för samverkan och informationsutbyte om cyberhot och risker. Förslaget om uppgiftsskyldighet och regler kring informationsdelning är av stor betydelse. Föreningarna understryker i detta avseende dock vikten av att föreskrifter om sekretess och dataskydd utformas för att säkerställa skydd av företags affärshemligheter och känsliga tekniska information. Det bör finnas incitament och tydliga garantier som gör det möjligt för företag att dela information utan risk för skada eller andra negativa konsekvenser.

Försvarslogik

Eftersom FRA är en myndighet med ansvar för nationell säkerhet och försvar måste de ansvarsområden som enligt förslaget överförs från MSB hanteras med förståelse för försvarslogiken. Området för försvar och nationell säkerhet ställer bland annat särskilda krav på sekretess, specialistkompetens, skydd av teknisk infrastruktur, redundants och robusthet, samt förmåga att agera snabbt utan avkall på säkerheten i processerna.

I utredningen föreslås att viss typ av verksamhet – såsom säkra kommunikationstjänster, signalskyddssystem och ledningsmetoder – ska stanna kvar hos MSB då de är nära kopplade till området för civilt försvar. Föreningarna välkomnar det förslaget, men noterar att gränsdragningarna måste vara tydliga och utvärderas regelbundet.

Sammanfattning

Sammanfattningsvis stödjer Teknikföretagen och SOFF målsättningen att stärka Sveriges nationella cybersäkerhetsförmåga. Vi ser överföringen av centrala delar av informations- och cybersäkerhet till FRA som rimlig, under förutsättning att försvarsbehov, sekretess och skydd för nationell säkerhet

beaktas fullt ut, samt att företags- och affärsrelaterade aspekter inte åsidosätts. Det är också viktigt att säkerställa tillräckliga resurser - personella, tekniska, finansiella - inklusive för sektorer med höga krav på säkerhetsklassificering.

Vi rekommenderar att utredningen och regeringen fortsätter samverka med näringslivet, särskilt företag med försvarsanknytning, genom både dialog och pilotprojekt för att löpande pröva och utvärdera hur utredningens förslag fungerar i praktiken.

SOFF och Teknikföretagen står till förfogande för dialog, samråd och praktiskt samarbete kring implementeringen av de föreslagna förändringarna.

Stockholm den 1 oktober 2025.

För föreningarna,

Robert Limmergård
Generalsekreterare
SOFF

Maria Rosendahl
Näringspolitisk chef
Teknikföretagen

Säkerhets- och försvarsföretagen
SOFF
Box 5510
SE-114 85 Stockholm

Telefon: 08-782 0850

www.soff.se