SOFF
Säkerhets- och försvarsföretagen

Till

Statsrådsberedningen

103 33 Stockholm

**Skrivelse med anledning av pågående arbete kring ett nationellt center för informations- och cybersäkerhet**

Statsministern har i regeringsförklaringen deklarerat att ett nationellt center ska upprättas för att öka informations- och cybersäkerheten. De myndigheter som nämns för att ingå i centret är Säkerhetspolisen, Försvarets radioanstalt, Myndigheten för samhällsskydd och beredskap samt Försvarsmakten. Säkerhets- och försvarsföretagen (nedan SOFF) ser positivt på att ett nationellt center för informations- och cybersäkerheten upprättas. I detta finns det vissa frågor som föreningen vill framföra.

**Aktörer**
För det första bejakar SOFF att följande myndigheter utgör kärnan i centret; Säkerhetspolisen, Försvarets radioanstalt, Myndigheten för samhällsskydd och beredskap samt Försvarsmakten då de är de centrala aktörerna i det nationella informations- och cybersäkerhetsarbetet. I detta vill SOFF framhålla vikten av att alla myndigheter skall ha bevarad kompetens på området för den egna verksamheten. Det är viktigt att hitta en balans i att lyfta del av kompetensen till centret och behålla del vid den egna myndigheten så att inte centret blir alltför mycket av ett expertcenter som inte kan kommunicera med övriga organisationer.

Vidare så ser SOFF att det är centralt att vissa andra offentliga aktörer så som Affärsverket Svenska kraftnät samt Post- och telestyrelsen på något sätt deltar i centrets arbete då energi- och telekomfrågor är av stor betydelse för att upprätthålla informations- och cybersäkerheten i samhället. Vidare anser föreningen det viktigt att vissa nyckelföretag adjungeras för att på plats delta i centrets arbete, det bör framförallt vara de centrala aktörerna för kritisk infrastruktur som Telia och Vattenfall.

**Lokalisering**
En annan mycket viktig fråga är att centret blir på en plats, centralt belägen, dit olika aktörer kan komma för ett gemensamt arbete (samverkan) vid olika händelser. Det krävs ett visst mått av öppenhet för att ta emot aktörer vid hanteringen av incidenter som berör samhället och för att löpande förmedla information till olika aktörer för att höja säkerhetsmedvetenheten. SOFF uppfattar att detta har varit en framgångsfaktor i andra länder, exempelvis i det nationella centret för cybersäkerhet i Storbritannien.

**Delgivning**
Frågan om delgivning är en ytterligare central fråga kopplat till den fysiska placeringen för centret. Det är mycket viktigt att centret inte blir ett ”svart hål” dit information förmedlas

internt från olika aktörer och inget kommer ut till samhällets övriga aktörer. Delgivning av information till samhällets aktörer, både privata och offentliga, är av största betydelse. Att den sedan kommer att se olika ut beroende av vem som är mottagare och vilken sekretess som kan tillämpas är självklart. Det är av största betydelse att informationen som delges anpassas efter mottagarens kunskapsnivå och behov. Föreningen anser att det finns goda möjligheter att använda den nu för IT-incidentrapportering prövade sekretessgrunden för Säkerhets- eller bevakningsåtgärder, OsL 18.8 § för mer kvalificerad delgivning.

**Samverkan**
I ett helt digitaliserat samhälle där huvuddelen av den kritiska infrastrukturen drivs av privata aktörer blir samverkan mellan stat och näringsliv av avgörande betydelse. Med en effektiv privat-offentlig samverkan kan samhället hantera allvarliga IT-incidenter. Det är därför av avgörande betydelse att samverkan mellan stat och näringsliv säkerställs inom ramen för det nya centret.

**Referensgrupp**
Ytterligare en aspekt som SOFF bedömer kan skapa en bättre förståelse inom centret för samhällets behov och samtidigt utgöra en central plattform för spridandet av information är skapandet av en referensgrupp med centrala aktörer från näringslivet med flera. Exempel på sådana aktörer är; Teknikföretagen, Sveriges kommuner och landsting, Säkerhets- och försvarsföretagen, Telekomföretagen, Svenskt näringsliv och Bankföreningen.

Avslutningsvis så ser SOFF det centralt att det läggs tillräckliga resurser från regeringen och berörda myndigheter på detta center och att det sker skyndsamt. Sverige har goda förmågor, såväl inom det offentliga som inom näringslivet, när det gäller informations- och cybersäkerhet, men det krävs en helt annan samling kring dessa frågor för att full effekt ska utvecklas, här är ett nationellt center för informations- och cybersäkerhet en absolut avgörande förutsättning.

Yttrandet har beretts av medlemsgruppen för cyberförsvar.

Stockholm den 19 juni 2019.

Robert Limmergård

Generalsekreterare