Försvarsdepartementet
fo.remissvar@regeringskansliet.se
carolina.hofgren@regeringskansliet.se.

Er referens	Ert datum	Er beteckning
Christelle Bourquin	2024-04-26	Fö2024/00785

Svar på remissen Ett nytt Nationellt cybersäkerhetscenter (Fö2024/00785)

Sammanfattning

- FMV välkomnar en förstärkning av samordningen av cybersäkerhetsfrågorna och arbetet i myndighetssamverkan i Nationellt cybersäkerhetscenter (NCSC). Ytterligare analys och utredning kring en ändamålsenlig och effektiv nationell organisering av arbetet för stärkt cybersäkerhet i Sverige behöver ske.
- FMV välkomnar att det föreslås att alla sju ingående myndigheter regleras på motsvarande sätt genom myndigheternas instruktion.
- FMV menar att det är väsentligt för de ingående myndigheterna att förtydliga vad som avses med att *bidra till*, *delta i* respektive *utföra verksamhet inom ramen för* centret.
- Vid bedömningen av vilken del av de ingående myndigheternas verksamhet som ska utföras inom ramen för centret bör även ingå om sådan verksamhet är ändamålsenlig och relevant utifrån centrets reglerade uppdrag och verksamhet.
- Ändringen av uppdraget i centret till ett allriskperspektiv från att ha haft antagonistiska hot som avgränsning innebär en väsentlig förändring i uppdraget för centret. Det är viktigt att detta inte minskar möjligheten för centret att arbeta med åtgärder som görs mer förebyggande mot en bredd av cybersäkerhetshot. FMV anser att det behöver finnas en flexibilitet i uppdraget för att agera och stödja olika aktörer.
- Centrets uppdrag och verksamhet bör samordnas med utformningen och genomförandet av kommande nationell cybersäkerhetsstrategi.
- På det internationella området bör centrets verksamhet utgå från de ingående myndigheternas redan existerande internationella samarbeten och plattformar.
- FMV menar att en utvecklad myndighetssamverkan med andra relevanta myndigheter, t.ex. sektorsmyndigheter, behöver ske utan att nya myndigheter för den skull behöver tas upp som centermyndighet.
- Flera EU-regleringar på cybersäkerhetsområdet håller på att genomföras. Det är väsentligt att EU-frågor behandlas på ett adekvat sätt och hanteras även inom ramen för centrets verksamhet.

FMV:s yttrande avseende utredningens förslag

Försvarets materielverk (FMV) har av Försvarsdepartementet delgivits delbetänkandet Ett nytt Nationellt cybersäkerhetscenter – del 1 (utredningen) och ombetts inkomma med remissvar på detta (Fö2024/00785).

Inledande kommentarer

FMV välkomnar ett mer samlat grepp kring samordningen av cybersäkerhetsfrågorna i Sverige och arbetet att stärka den myndighetssamverkan som nu genomförs i det nationella cybersäkerhetscentret (NCSC). Här välkomnas även att alla myndigheter i NCSC regleras på likartat sätt genom myndigheternas instruktioner.

FMV vill inledningsvis framhålla att digitaliseringen och utvecklingen på cyberområdet, bl.a. när det gäller frågor om cybersäkerhet, förändras i mycket snabb takt mot bakgrund av omvärldsutvecklingen och teknikutveckling. Härtill kommer att det pågår ett mycket omfattande lagstiftningsarbete med krav på åtgärder för att stärka cybersäkerheten inom EU, bl.a. vad gäller inom samhällsviktiga verksamheter (NIS 2), som även kan komma att omfatta krav på ökad cybersäkerhet genom bl.a. certifiering av i IKT-produkter och IKT-tjänster i sådana verksamheter.

Genomförandet av bl.a. NIS 2-direktivet under 2025 innebär att ett stort antal offentliga och privata aktörer inom de flesta av samhällets olika verksamhetsområden kommer att omfattas av mer eller mindre långtgående krav på åtgärder som syftar till att uppnå en godtagbar cybersäkerhet i verksamheten. Vidare kommer enligt nuvarande förslag elva tillsynsmyndigheter (sektorsmyndigheter) att övervaka att den föreslagna lagstiftningen på NIS 2-området efterlevs. Det kan i detta sammanhang även noteras att många verksamheter som omfattas av NIS 2-direktivet också utgör verksamhet inom det nationella totalförsvaret.

Det kommer att ställas höga krav på ledning och kompetens på cybersäkerhet hos ett stort antal berörda verksamhetsutövare inom vitt skilda samhällsområden, såväl offentliga som privata. Samtidigt kan konstateras att ett antal offentliga utredningar och rapporter påvisat att det föreligger stora brister i cybersäkerhet hos många verksamhetsutövare och att det finns ett stort behov av kompetens och stöd till många verksamhetsutövare, såväl offentliga som privata.

Det finns flera viktiga frågor och aspekter som bör belysas till stöd för vilken lösning som är den mest optimala för att på nationell nivå uppnå en stärkt cybersäkerhet som inte behandlats eller samordnats inom utredningen, bl.a. vad gäller NIS2-direktivet och annan relevant EU-lagstiftning på cyberområdet samt med frågor som rör de ökade krav på cybersäkerhet som kan förutses på verksamheter som omfattas av säkerhetsskyddslagstiftningen. Dessa förhållanden har också bäring på styrningen, ledningen och utvecklingen av och samverkan inom den framtida verksamheten inom NCSC.

FMV menar att dessa och andra frågeställningar som rör nationell cybersäkerhet borde vara föremål för en mer samlad, omfattande och djupare analys som syftar till att åstadkomma en ändamålsenlig och effektiv nationell organisering av arbetet med att uppnå en stärkt cybersäkerhet. Även om det finns ett omedelbart behov av att åstadkomma en förändring av NCSC verksamhet bör, som Försvarsberedningen också föreslagit, frågan om en särskild nationell myndighet för cybersäkerhet utredas i särskild ordning (se nedan under Övriga synpunkter).

Synpunkter på utredningens förslag

FMV har nedan synpunkter på olika förslag som lämnas i delbetänkandet. Nedanstående synpunkter utgår från promemorians disposition (avsnitt i utredningen inom parentes).

Försvarets materielverk (avsnitt 3.3.7)

FMV:s verksamhet beskrivs översiktligt i utredningen. Inför en förstärkt samverkan i NCSC kommer myndigheten att genomföra en intern inventering med verksamhet som har relevans och koppling till NCSC.

Mål och utgångspunkter (avsnitt 5.1)

Utredningens förslag att verksamheten i NCSC ska breddas och omfatta ett allriskperspektiv innebär en väsentlig förändring av omfattning av uppdraget från den nuvarande inriktningen att fokusera på *antagonistiska cyberhot*[1]. Genom ett allriskperspektiv kommer alla typer av it-incidenter att omfattas, inklusive t.ex. olyckor och handhavandefel.[2]

Det kan vara värdefullt att hela bredden av cybersäkerhetsincidenter ingår i uppdraget men det blir ett annat fokus på den lägesbildsrapportering och annan verksamhet som centret idag bedriver. Utredningen konstaterar även att detta blir mycket brett och föreslår istället en inriktning på verksamheten till de med en viss allvarlighetsgrad (betydande it-incidenter).

FMV vill i detta sammanhang påtala vikten av ett systematisk cybersäkerhetsarbete behöver ske där åtgärder för ökad resiliens och robusthet i system och verksamhet i många fall är del av en mängd olika åtgärder som samverkar för att höja cybersäkerhetsnivån i en verksamhet. Sådana förebyggande åtgärder kommer således att vara effektiva både mot betydande it-incidenter men även incidenter av lägre allvarlighetsgrad. Begränsningen till *betydande it-incidenter* kan särskilt i det förebyggande arbetet inte alltid vara ändamålsenlig.

En förordning om Nationellt cybersäkerhetscenter (avsnitt 5.1.1)

FMV har inget att erinra om att centrets uppgifter regleras i en förordning. Genom den lösningen finns det förutsättningar att tydligare samla uppdraget för centret och för de myndigheter som ingår i centersamverkan. Samtidigt styrs varje myndighet med uppdrag och uppgifter även genom sina instruktioner och regleringsbrev.

FMV har följande preliminära kommentarer på några av de uppgifter som finns för centret i förslaget till förordning.

---

[1] Se Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter, Fö2019/01330.

[2] Här kan jämföras med hur de fyra samverkande myndigheterna avgränsade och uppfattade målsättningarna inför etableringen av NCSC i ett svar på uppdrag Fö2019/0100/SUND. ”Antagonistiska hot kan för centrets del beskrivas som företrädesvis, men inte uteslutande, statsunderstödda aktörer som drivs av nationella intressen och bedriver kvalificerade cyberoperationer mot Sverige och svenska intressen i syfte att komma över, förvanska eller förstöra information som har betydelse för Sveriges säkerhet och välstånd” (sid. 3). https://www.msb.se/contentassets/0a98ea0745994933b06ed45601472b40/svar-pa-uppdrag-infor-inrattandet-av-ett-nationellt-cybersakerhetscenter.pdf

”[…] utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot och betydande it-incidenter.”
FMV anser att en ändrad inriktning i uppdraget från *antagonistiska cyberhot* till *cyberhot och betydande it-incidenter* behöver ytterligare övervägas och analyseras. Det är väsentligt att denna formulering blir tydlig och ändamålsenlig då den kommer att vara portalparagrafen för centrets verksamhet.

FMV delar utredningens uppfattning att cyberhot ska uppfattas såsom detta begrepp definieras i EU:s cybersäkerhetsakt (2019/881). FMV delar dock inte fullt ut utredningens slutsats att en inriktning på antagonistiska cyberhot kräver attribuering till en aktör med en viss intention (sid. 36). Särskilt i det förebyggande arbetet kommer sådana avvägningar inte att vara relevanta på samma vis då antagandet är att aktörer som agerar kommer vara antagonister.

FMV kan i detta sammanhang förorda en inriktning där centrets uppdrag beskrivs på ett sätt som möjliggör ett arbete mot olika aktörer baserat på det uppdrag som centret får för att kunna höja cybersäkerhetsnivån hos dessa och i samhället. Det kan särskilt i det stödjande förebyggande arbetet bli nödvändigt för centret att inte enbart arbeta med det mest skyddsvärda eller mest allvarliga. I detta sammanhang måste det finnas en flexibilitet i uppdraget, inte minst för att kunna takta med de ansvarsområden som olika sektorsmyndigheter har på området för att kunna ge ett ändamålsenligt stöd.

Centrets uppgift bör även anknyta till visionen för Sveriges cybersäkerhet som kommer uttryckas i en kommande nationell strategi på området.

”[…] utgöra nationell plattform för privat-offentlig samverkan och vara samlad kontaktpunkt för frågor som rör informationssäkerhet och cybersäkerhet.”
FMV stöder fortsatt utvecklad verksamhet för privat-offentlig samverkan. Utifrån ett tydligt uppdrag för centret blir det en viktig plattform, även i detta fall som komplement och stöd till den samverkan som sektorsmyndigheter har.

Det är många privata verksamheter av olika slag som uppfattar att centret ska vara stöd i deras cybersäkerhetsarbete vid sidan om annan offentlig verksamhet. Det finns även specifika behov för företag verksamma inom olika sektorer och branscher. FMV har genom sin verksamhet insikt i behov som finns för bl.a. svenska försvarsindustriföretag.

FMV vill framföra att tät samverkan med privata aktörer som utför olika typer av förvaltade säkerhetstjänster, stöd och rapportering och annan hotinformation är även en absolut nödvändighet för att kunna upptäcka och hantera de it-incidenter som förutses som viktiga uppgifter för centret.

”producera samlade lägesuppfattningar avseende cyberhot och betydande it-incidenter”
Det behöver vara tydligt vilka de olika mottagarna av dessa rapporter är för att kunna utforma innehållet på ett ändamålsenligt sätt.

Begreppet *lägesuppfattning* kan ha flera betydelser och i vissa sammanhang används istället begreppet *lägesbild*, vilket också är fallet för centret nuvarande produktion utifrån de särskilda regeringsuppdrag som finns för detta. Hänvisningen till att begreppet lägesuppfattning används av utredningen av genomförandet av NIS 2-direktivet kan bygga på en missuppfattning då lägesuppfattning som verksamhet eller tillstånd baserar sig på, och innebär bl.a. att ta fram, just

lägesbilder[3]. FMV kan även framföra att centret även skulle kunna ha uppdrag att ta fram andra typer av analyser och rapporter inom ramen för detta arbete.

”övergripande koordinera och delta i internationella samarbeten kopplade till centrets verksamhet”

FMV betonar vikten av att centrets internationella samverkan till stor del kommer behöva utgå från och förhålla sig till myndigheternas uppbyggda relationer och samarbeten. Det är naturligt att plattformar för internationell samverkan som myndigheter byggt upp och som faller inom centrets uppdragsområden även kan komma centret till del i det internationella utbytet, inte minst med liknande center utomlands. Det kommer att finnas överlappning mellan myndigheternas internationella samarbeten och centrets dito som myndigheterna behöver förhålla sig till. Det kan övervägas om centret i detta sammanhang istället för att ha rollen att koordinera sådana samarbeten används som plattform för myndigheterna att samordna eller facilitera vissa internationella kontakter.

Ledning och styrning av NCSC (avsnitt 5.2)

I detta avsnitt anger utredningen att centret blir en del av Försvarets radioanstalt (FRA) som får huvudansvaret. Samtidigt anges i förslag till förordning att övriga myndigheter *deltar* i centret (4 §) och ska *bidra* till verksamheten (6 §) och slutligen att myndigheternas verksamhet ska utföras *inom ramen för centret*.

FMV påtalar att det kommer att behövas ytterligare förtydliganden kring vad som avses utgöra centerverksamhet och hur dessa olika begrepp rörande deltagande i och bidrag till centret och dess verksamhet konkret ska tolkas och tillämpas av myndigheterna, särskilt i förhållande till myndigheternas övriga uppgifter och uppdrag som styrs genom instruktion och regleringsbrev. Se även nedan kommentarer under avsnitt 5.3.

Beslutsfattande i NCSC (avsnitt 5.2.2)

De deltagande myndigheternas ansvar och beslutsmandat behöver upprätthållas så det är tydligt vilken myndighet som agerar och är ansvariga för uppdrag, även när en aktivitet sker tillsammans med en centerprofilering.

Utredningen resonerar kring förvaltningslagen och begreppet faktiskt handlande vilket bl.a. centrets uppdrag att ge råd och stöd i stort kan falla in under. Dock kan det finnas områden, särskilt för deltagande myndigheter med tillsynsroller – såsom bl.a. Post- och telestyrelsen (PTS), FMV och Säkerhetspolisen – att del av rådgivningen hör ihop med den myndighetens utpekade tillsynsroll. Sådan verksamhet kan dock fortfarande även betraktas som verksamhet som kan och därmed ska utföras inom ramen för centret. FMV anser att det här aktualiseras frågor kopplade till gränsdragningen mellan tillsyn och rådgivning samt vikten av att det tydligt framgår vilken myndighet som agerar med centerprofilering.

[3] Se SOU 2024:18 sid. 306.

Övriga centermyndigheternas medverkan och bidrag (avsnitt 5.3)

FMV välkomnar att de två olika nivåer av samverkan som hittills funnits, dvs. *fördjupad samverkan* och *medverkan*, nu i allt väsentligt tas bort. Att alla myndigheter har samma styrning rörande centret i instruktionen, förutom FRA som huvudansvarig för centret, kommer att förenkla samordning mellan myndigheternas deltagande.

Samtidigt anser FMV att de formuleringar för deltagandet som föreslås i den styrande förordningstexten behöver förtydligas. Detta gäller särskilt formuleringen i 6 § *inom ramen för centret*. Det behöver tydligare framgå vilken typ av deltagande och bidrag som detta avser med utgångspunkt i de olika verksamhetsområden som de deltagande myndigheterna idag har inom cybersäkerhetsområdet. Det rör sig alltifrån ren myndighetsutövning, tillsynsverksamhet, särskilda roller enligt EU-lagstiftning som myndigheten utpekats av regeringen att ha, mm.

Nedan är exempel på typer av bidrag som kan komma ifråga för centersamverkan baserat på myndigheternas nuvarande verksamheter samt bidrag till centret.

- Bidrag av personella resurser i form av expertis – både centerinternt gentemot andra centermyndigheter/kansliet och externt inriktat mot andra aktörer *(kan redovisas i tid)*
- Bidrag av personella resurser i form av samordningsuppdraget för centermedverkan – centerinternt gentemot andra centermyndigheter/kansliet *(kan redovisas i tid)*
- Bidrag med information som underlag syftande till intern eller extern leverabel *(kan redovisas som lämnad information)*
- Bidrag med operativa tekniska förmågor *(kan redovisas i tid eller antal användningar av teknisk plattform el. dyl.)*
- Bidrag med inspel till andra plattformar som myndigheten förfogar över (t.ex. inspel till deltagande i EU-arbetsgrupp) *(kan redovisas som lämnad information)*

Samtliga dessa typer av bidrag kan komma att behöva hanteras eller utföras ”inom ramen för centret”. När det rör sig om personella resurser så kommer dessa, utöver FRA:s egen personal, att inte direkt förfogas eller arbetsledas av FRA resursmässigt. Ett sådant asymmetriskt styrningsförhållande kommer behöva hanteras mellan de ingående myndigheterna. Till det kommer även att det kan finnas viss verksamhet som idag utförs av centret och dess kansli som inte direkt hänför sig till någon myndighets direkta uppdrag.

De ingående myndigheterna behöver även kunna komma överens om på vilket sätt de kan agera under centerflagg, ev. tillsammans med sin egen myndighetsprofilering. En eller bara några av de ingående myndigheterna kan behöva kunna agera i centrets namn. FMV menar att det inte bör vara avsikten att alla myndigheter måste vara med i alla delar av centrets verksamhet. Hela vitsen med centersamverkan är att olika myndigheter tar med sig olika kompetenser och expertis till samverkan. Utredningen är samtidigt tydlig med att alla myndigheters olika verksamheter inom ramen för cybersäkerhetsområdet ska utföras inom ramen för centret.

FMV instämmer i stort i ansatsen att så mycket som möjligt av relevant verksamhet på cybersäkerhetsområdet som utföras av de ingående myndigheterna ska så lång möjligt kopplas till centret. Utredningens förslag att den verksamhet som centermyndigheterna bedriver som kan utföras inom ramen för NCSC ska utföras inom ramen för centret behöver dock tydliggöras. FMV anser att det även behöver finnas en bedömning av om det är ändamålsenligt i förhållande till centrets uppdrag och andra omständigheter.

Skyldighet att medverka och bidra (avsnitt 5.3.1)

FMV hänvisar i denna del till resonemangen ovan rörande behov av tydighet kring vad som avses med bidrag. FMV har ingen synpunkt på att uppdraget att bidra och medverka i centret regleras i myndighetens instruktion. Det är rimligt och skapar tydlighet även i förhållande till myndighetens egen uppföljning, redovisning och myndighetsdialog med Regeringskansliet.

Myndigheternas författningsreglerade uppgifter vid attacker och incidenter (avsnitt 5.3.2)

FMV är idag utsett av regeringen att vara nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt.[4] Denna roll innebär att, när EU:s ramverk för cybersäkerhetscertifiering är i full drift, ta emot sårbarhetsrapporter från certifieringsorgan rörande upptäckta sårbarheter i certifierade IKT[5]-produkter eller -tjänster (t.ex. en certifierad molntjänst eller router). Det kan i det sammanhanget vara aktuellt att sådana sårbarheter även kopplas till en eventuell och betydande it-incident av den art som centret också ska hantera. Således kan även relevant information för hantering av en sådan incident finnas hos andra myndigheter än den som, i det fallet inom ramen för centret, hanterar incidenten.

Produkter och tjänster som är certifierade enligt det europeiska ramverket, där sårbarhetsinformation kopplade till dessa rapporteras till FMV, kan även användas av olika aktörer som omfattas av NIS 2.

Andra myndigheter med tangerande uppdrag (avsnitt 5.3.4)

FMV vill erinra om att cybersäkerhet är en del av många myndigheters olika uppdrag och verksamhet. Utredningen nämner myndigheterna Totalförsvarets forskningsinstitut (FOI), Myndigheten för digital förvaltning (DIGG) och Myndigheten för psykologiskt försvar (MPF). Det finns fler som är relevanta att nämna i detta sammanhang, t.ex. Integritetsskyddsmyndigheten (IMY) eller andra sektorsmyndigheter.

Det är helt avgörande att centret har en tydlig organisation för att möjliggöra stöd till och samverkan med andra myndigheter än de som deltar i centersamverkan enligt den föreslagna förordningen, här ingår t.ex. alla sektorsmyndigheter. Det gäller särskilt för myndigheter som kan bidra till centrets uppdrag på något sätt. Här delar FMV utredningens förslag om att centret ska upparbeta nära samarbeten med relevanta myndigheter.

Även om gränsområdet mellan påverkansoperationer och rena cybersäkerhetsrelaterade hot kan vara diffust så förfaller den verksamhet som MPF arbetar med vara mer inriktat på innehåll (påverkande desinformation mm.) än hantering av konkreta cyberattacker i sig. Samtidigt kan myndigheten i flera fall säkerligen ha relevant teknisk och annan information som kan vara relevant vid hantering av en it-incident kopplat till olika typer av påverkanskampanjer (t.ex. om det kombinerats med överbelastningsattacker mm.). Men det innebär inte nödvändigtvis att det ska ses som att MPF i sig har ett nationellt uppdrag på cybersäkerhetsområdet och därmed ska delta som centermyndighet. Däremot är ett nära samarbete med centret mycket relevant.

[4] Se 3 § förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.
[5] Informations- och kommunikationsteknologi.

Det bör också övervägas om en myndighet som DIGG, vars verksamhet helt präglas av en utbyggd digitalisering, är mer relevant att inlemma och integrera i det cybersäkerhetsarbetet som bedrivs i centret. Även IMY och kopplingen till efterlevnad till vissa nivåer av cybersäkerhet inom ramen för dataskyddet kan vara relevant för olika typer av samverkan med och bidrag till centret. FOI besitter på samma vis en mängd relevant expertis på området. Inte minst inom övningsverksamheten kan FOI ha stor relevans och även med bidrag till de olika analyser och rapporter som centret utarbetar givet att FOI även är en försvarsunderrättelsemyndighet.

Här kan även nämnas alla sektorsmyndigheter som finns enligt nuvarande och kommande uppdateringen av NIS-ramverket som är relevanta för cybersäkerhetsarbetet inom sina respektive sektorer.

Samverkan inom NCSC (avsnitt 5.4)

FMV påtalar vikten av att det mellan de ingående myndigheterna uppfattar en tydlig och ensad bild av uppdraget i centret genom den styrning som de får och hur detta ska utföras. Sådan tydlighet skulle kunna skapas genom att myndigheterna åläggs att deklarera vilka av sina verksamheter var och en av myndigheterna avser bidra med eller utföra inom ramen för centret utifrån uppdraget.

FMV vill även framför att centrets uppdrag och mål ska vara synkade med den nationella cybersäkerhetsstrategin som håller på att utarbetas, bl.a. i enlighet med kraven som finns i NIS 2-direktivet[6].

Bland centrets mer konkreta verksamhet, utöver incidenthantering, så är t.ex. utformningen av och arbetet med Nationell modell för systematisk cybersäkerhetsarbete viktig. Även frågor om cybersäkerhetscertifiering kan komma att spela en större roll framöver och kan därmed användas mer strategiskt i arbetet att stötta företag etc. NIS 2-direktivet kommer även vara en utgångspunkt för många aktörers konkreta cybersäkerhetsarbete framöver och kommer således även spela en roll för hur centret utformar sin verksamhet och stöd.

Samverkan på strategisk nivå (avsnitt 5.4.1)

FMV har inget att erinra om en reglering i förordning av ett strategiskt samverkansråd för centret, som består av de ingående myndigheternas generaldirektörer eller chefer på motsvarande nivå. Här vill FMV särskilt betona vikten av det som utredningen lyfter fram om detta råds roll i att överbrygga olikheter i myndighetskultur och olika utgångspunkter.

Samverkan på operativ nivå (avsnitt 5.4.2)

FMV instämmer att den operativa samverkan i centret inte ska regleras i förordning. Det ställer dock krav på att centermyndigheterna finner en operativ samverkansmodell som tar hänsyn till de olika typer av verksamhet som myndigheterna utför inom ramen för centret, se resonemanget ovan under avsnitt 5.3.

[6] Se artikel 7, NIS 2-direktivet (2022/2555).

Deconfliction (avsnitt 5.4.3)

Eftersom flera centermyndigheter även har olika former av underrättelseuppdrag kommer frågan om den typ av avvägningar som utredningen beskriver i detta avsnitt att uppstå. Samtidigt är det tydligt att centret inte har ett underrättelseuppdrag per se. De nationella säkerhetsintressen som finns behöver hanteras, men oaktat detta ska centret ha fokus på sin mer breda roll som stöd för olika aktörer och företag.

Näringslivet, offentliga aktörer och andra intressenter (avsnitt 5.5)

På samma sätt som för olika internationella samarbeten som de medverkande myndigheterna kan ha på cybersäkerhetsområdet behöver centersamverkan förhålla sig till alla de olika samverkansnätverk och annan informationsinhämtning som myndigheter har inom ramen för deras respektive verksamheter och uppdrag och som identifierats som möjliga att utföra inom ramen för centret.

FMV stödjer utredningens ansats att ta inspiration från andra verksamheter när det gäller hur samverkan med privata aktörer utformas. Det finns behov av att finna nya sätt att ta in samverkan från näringslivet och där är idén med placering av personal från företag sekunderade till centret särskilt intressant.

Internationella samarbeten (avsnitt 5.6)

Utöver vad som ovan anförts rörande avsnitt 5.1.1 behöver det även tydliggöras hur centret ska förhålla sig till de mer formella internationella samarbetsplattformar och beslutsfora som de deltagande centermyndigheterna är med i inom ramen för t.ex. EU (exempelvis de samverkansgrupper som upprättas av olika EU-rättsakter) och Nato. Flera myndigheter i centret deltar även i utveckling av harmoniserade standarder i internationella standardsorgan med verksamhet inom centrets område.

NCSC:s fortsatta utveckling (avsnitt 5.7)

FMV instämmer i det utredningen lyfter fram i avsnittet att även aspekter såsom frågor om cybersäkerhetscertifiering är verksamhet som i större utsträckning kan beröras inom ramen för centret, på så sätt att sådana verktyg kan ingå i en mer strategisk ansats från svensk sida. Det bör hänga samman med den strategiska inriktningen som antas i den nationella strategin samt de behov som olika sektorsmyndigheter kan se.[7]

Konsekvenser och kostnader för övriga centermyndigheter (avsnitt 6.4)

För de tre myndigheter som hittills inte haft ett regeringsuppdrag rörande centersamverkan (PTS, Polismyndigheten, FMV) innebär den föreslagna förändringen en ny styrning och uppföljning av myndigheternas verksamhet.

[7] Jfr. artikel 7.2.b NIS 2-direktivet som anger att ”[r]iktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod” ska antas som en del av strategin.

Kostnadsfrågan hänger ihop med resonemanget om hur olika typer av bidrag till centrets uttrycks, där vissa helt klart utförs inom ramen för myndighetens existerande verksamhet. Det är däremot tydligt att centersamverkan innebär ett ökat behov av samordning även internt inom myndigheterna för den verksamhet som utförs inom ramen för centret. Till viss del kommer detta vara dimensionerande för myndigheternas resurstillsättning.

Ikraftträdande (avsnitt 7)

Det är inte sannolikt att alla samordningsprinciper och liknande vägledning och överenskommelser som behövs mellan de medverkande myndigheterna för det nya upplägget för centret kommer vara på plats till september 2024 då utredningen föreslår att den nya förordningen ska träda ikraft. Däremot ser inte FMV att det i sig skulle utgöra ett hinder för att de övergripande ramarna för samverkan i centret antas i förordning vid den tidpunkten.

Övriga synpunkter

EU-frågorna

Förändringen av Nationellt cybersäkerhetscenter kommer under en tid med ökad diskussion om styrningen av cybersäkerhetsområdet i Sverige. FMV vill särskilt uppmärksamma att det finns ett antal EU-rättsakter på cybersäkerhetsområdet som antingen är antagna och trätt ikraft eller färdigförhandlats mellan rådet och parlamentet. Det gäller bl.a. det redan omnämnda NIS 2-direktivet, cyberresiliensakten, AI-akten, eIDAS-förordningen, cybersolidaritetsakten och en uppdatering av cybersäkerhetsakten. Tillsammans skapar detta en omfattande regelmassa att implementera i Sverige och innebär att en stor mängd olika krav ställs på aktörer och företag som dessa ska leva upp till.

Genomförande och tillsyn kommer utföras av både myndigheter som ingår i centret och ett antal andra sektorsmyndigheter. Dessa EU-regelverk kan komma att spela en roll t.ex. i arbetet som ett antal centermyndigheter har med att utforma en Nationell modell för systematisk cybersäkerhetsarbete. Med FRA som ny huvudman för centret är det viktigt att EU-frågorna får fortsatt och i relevanta perspektiv ökad belysning inom ramen för centrets verksamhet.

Andra organisationsformer

I olika sammanhang har förslaget om att skapa en ny cybersäkerhetsmyndighet i Sverige framförts eller antytts. Senaste togs det upp av Försvarsberedningen i delbetänkandet Kraftsamling (Ds 2023:34) som ansåg att det kan övervägas att ansvaret för cyber- och informationssäkerhet som idag finns på MSB organiseras som ny myndighet. FMV kan i detta sammanhang hänvisa till sitt svar på regeringsuppdraget att bedöma genomförbarheten av förslagen i Kraftsamling där myndigheten förordar en sådan lösning på sikt, men att fler funktioner och uppgifter än de som idag finns hos MSB skulle behöva tillföras inom ramen för en ny myndighets ansvar.[8]

[8] Se svar på Uppdrag om åtgärdsförslag inom det civila försvaret inför nästa försvarspolitiska inriktningsproposition, 23FMV6250-2, sid. 9.

Nationella behov vid framtagandet av certifieringsordningar enligt EU:s cybersäkerhetsakt

I detta sammanhang hänvisar FMV även till myndighetens rapport som i april 2024 skickades som svar på regeringsuppdraget med förslag på hur nationella behov ifråga om cybersäkerhet kan identifieras och omsättas till säkerhetskrav som Sverige bör framhålla i arbete med att utveckla certifieringsordningar inom EU:s cybersäkerhetsakt.[9]

I FMV:s rapport anges att det är en stor utmaning för både den stora gruppen sektorsmyndigheter och verksamhetsutövare att var och en etablera och upprätthålla nödvändig kompetens inom informations- och kommunikationsteknik, cybersäkerhet, risker för sårbarheter och attacker, effektiva säkerhetsåtgärder, effektiva kontrollmetoder och certifiering, samt förmåga att påverka relevanta standarder och certifieringsordningar. Därmed föreslås i rapporten att en samlad nationell kompetens- och stödfunktion bör etableras. Rapporten fortsätter:

> Denna [stödfunktion] ska ha en stark nationell förmåga för analys, samordning, proaktiv och tidig påverkan på utvecklingen av standarder och certifieringsordningar, samt ska kunna stödja sektorsmyndigheter och verksamhetsutövare inom cybersäkerhetsområdet. [– – –]
>
> Stödfunktionen ska i samråd med sektorsmyndigheter utarbeta rekommenderade lösningar för säkerhetsbehov som finns inom en eller flera sektorer, samt i övrigt utgöra ett expertstöd till sektorsmyndigheter och verksamhetsutövare angående effektiva, genomförbara och kostnadseffektiva lösningar som kan adressera respektive sektors behov, avseende bl.a. produkter, arkitektur, drift, tjänster, underhåll, övervakning och kontrollmetoder (inkl. certifiering) samt därtill relaterade standarder. Stödfunktionen ska samverka med sektorsmyndigheterna och tillsammans med dessa bevaka eller proaktivt delta i eller påverka utvecklingen i relevanta standardiseringsorgan och certifieringsordningar. [– – –]
>
> Försvarets materielverk förordar att stödfunktionen organiseras inom en redan existerande myndighet, eller inom en ny myndighet för cybersäkerhet, om en sådan etableras i enlighet med Försvarsberedningens förslag. De närmare formerna för stödfunktionens ansvar och uppgifter i relation till sektorsmyndigheterna bör närmare utredas. [– – –][10]

Dessa förslag kan även bidra till diskussionerna om NCSC kommande utformning och uppdrag.

– – –

I den slutliga handläggningen har avdelningschef John Billow, informationssäkerhetschef Thomas Palfelt, rådgivare Thomas Wallander och verksamhetsutvecklare Linda Bjärnebro deltagit. John Billow har varit föredragande.

Försvarets materielverk

Anders Sjöborg
Chefsjurist, Juridik- och säkerhetsstaben

---

[9] Nationella behov vid framtagandet av certifieringsordningar enligt EU:s cybersäkerhetsakt, 26 april 2024 (23FMV2840-8).
[10] Ibid. sid. 10f.

Sändlista
Försvarsdepartementet

Kopia till
Arkiv
FMV Lednings- och ekonomistaben
FMV Juridik- och säkerhetsstaben