Ett nytt Nationellt cybersäkerhetcenter

Förutsättningar för en effektiv verksamhet

Del 2

Förord

Statsrådet Carl-Oskar Bohlin beslutade den 4 oktober 2023 att en utredare skulle biträda Regeringskansliet med att lämna förslag på hur en ändamålsenlig och effektiv ledning, organisering och styrning av Nationellt cybersäkerhetscenter ska utföras (Fö2023/01606).

Samma dag förordnades generaldirektören Per Bergling att fullgöra uppdraget. Kammarrättsassessorn och verksjuristen Ninni Bohman Olin anställdes samma dag att arbeta som sekreterare inom ramen för uppdraget. Tf. kammarrättsassessorn Anna Wennberg anställdes den 5 februari 2024 att arbeta som sekreterare i uppdraget.

Härmed överlämnas utredningens andra delbetänkande *Ett nytt Nationellt cybersäkerhetscenter – Förutsättningar för en effektiv verksamhet*.

Med detta är uppdraget slutfört.

Umeå i juni 2024

Per Bergling

/Ninni Bohman Olin
Anna Wennberg

Innehåll

Sammanfattning

Personal, arbetsledning och arbetsgivaransvar

Utredningens bedömning är att det kommer att krävas olika kategorier av personal i centret. Majoriteten av personalen kommer att vara anställd av Försvarets radioanstalt. Utredningen ser också ett behov av att övriga centermyndigheter är kontinuerligt representerade i verksamheten, dels i form av en grundbemanning, dels sådan personal som arbetar i centret under begränsad tid inom ramen för särskilda uppgifter eller projekt.

Utredningen föreslår att det i förordningen (2024:000) om Nationellt cybersäkerhetscenter ska föras in en bestämmelse där det framgår att personal ska placeras i centrets verksamhet efter överenskommelse mellan Försvarets radioanstalt och den centermyndighet där personalen är anställd. Genom överenskommelser mellan centermyndigheterna kan chefen för centret också ges mandat att arbetsleda all personal oavsett vilken myndighet personalen är anställd vid.

Möjligheten att genomföra personallån till Försvarets radioanstalt, både från de övriga centermyndigheterna och från andra myndigheter, bör också utnyttjas när behov uppstår. Det går även att köpa konsulttjänster av privata aktörer.

Det övergripande arbetsmiljöansvaret har respektive arbetsgivare. För personal som inte är anställda av Försvarets radioanstalt ansvarar Försvarets radioanstalt och personalens arbetsgivare för olika delar av arbetsmiljön. Försvarets radioanstalt får dock ett rådighets- och samordningsansvar för arbetsmiljön.

Informationsdelning

Den interna informationsdelningen kommer ske med stöd av bestämmelser i offentlighets- och sekretesslagen (2009:400), OSL. Det finns möjligheter att dela information med nuvarande reglering men utredningen anser att det bör utredas om en uppgiftsskyldighet eller sekretessbrytande bestämmelser som effektiviserar informationsutbytet kan införas.

Vad gäller den externa informationsdelningen är ingiven information om exempelvis incidenter sådan att den kommer skyddas av sekretess enligt OSL. Dock saknas sekretess till skydd för uppgifter om affärs- och driftsförhållanden hos de privata aktörer som lämnar information. Det bör därför enligt utredningen övervägas om sekretessbestämmelser med sådant skydd ska införas.

Personuppgiftsbehandling

Utredningen bedömer inte att det krävs några förändringar av personuppgiftsbehandlingsregleringen för centrets verksamhet. Myndigheterna deltar i centret inom ramen för sina egna verksamhetsområden. Någon ny grund för behandling av personuppgifter har därför inte tillkommit. Personuppgiftsbehandlingen kommer i mycket större utsträckning än tidigare styras av Försvarets radioanstalts personuppgiftsreglering. Personuppgiftsansvaret kommer dock i varje myndighets interna system

styras av myndighetens personuppgiftsreglering även om myndighetens personal arbetar i centret. Utökade möjligheter för Försvarets radioanstalt att dela personuppgifter elektroniskt med andra än statliga myndigheter kan effektivisera arbetet. Det bör övervägas om regleringen av detta ska ändras. Det kan också övervägas om utökad direktåtkomst mellan centermyndigheterna vore ändamålsenligt. I nuläget kan enbart vissa myndigheter medge direktåtkomst för centerverksamheten.

Säkerhetsskydd

Utredningen bedömer att ansvaret för centrets säkerhetsskydd huvudsakligen kommer ligga hos Försvarets radioanstalt. Myndighetens generaldirektör blir ytterst ansvarig för säkerhetsskyddet och säkerhetsskyddschefen vid Försvarets radioanstalt blir säkerhetsskyddschef även för centret.

Det kommer däremot vara den myndighet där personalen är anställd som ansvarar för säkerhetsprövning av den personal som deltar i verksamheten. Detta följer av att det är myndigheten som är arbetsgivare som beslutar om vilken personal som ska medverka i centerverksamheten. Varje centermyndighet kommer också att ha ansvar för säkerhetsskyddet för sitt eget tekniska system.

Förkortningar

I denna promemoria används bland annat följande förkortningar.

BDL	Brottsdatalagen (2018:1177)
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
FRA-PuL	Lagen (2021:1172) om personuppgifts-behandling vid Försvarets radioanstalt
FRA-PuF	Förordningen (2021:1208) om behandling av personuppgifter vid Försvarets radioanstalt
FM-PuL	Lagen (2021:1171) om behandling av personuppgifter vid Försvarsmakten
FM-PuF	Förordningen (2021:1207) om behandling av personuppgifter vid Försvarsmakten
FL	Förvaltningslagen (2017:900)
GDPR	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)
MSB	Myndigheten för samhällsskydd och bered-skap
Must	Militära underrättelse- och säkerhetstjänsten
NCSC	Nationellt cybersäkerhetscenter
NCT	Nationellt centrum för terrorhotsbedömning
OSF	Offentlighets- och sekretessförordningen (2009:641)
OSL	Offentlighets- och sekretesslagen (2009:400)
TF	Tryckfrihetsförordningen

1 Författningsförslag

1.1 Förslag till förordning med ändring i förordning (2024:000) om Nationellt cybersäkerhetscenter

Härigenom föreskrivs i fråga om förordningen (2024:000) om Nationellt cybersäkerhetscenter att det ska införas en ny paragraf, 8 §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	8 §
	Personal från de deltagande myndigheterna ska placeras i det Nationella cybersäkerhetscentret.
	Placering av personal i centret ska ske efter överenskommelse mellan Försvarets radioanstalt och den myndighet där personalen är anställd.

Denna förordning träder i kraft den 1 september 2024.

2 Utredningens uppdrag och arbete

2.1 Uppdraget

I sin första del har utredningen analyserat och lämnat förslag på hur Försvarets radioanstalt ska leda samordning, utveckling och genomförande av centrets verksamhet. Utredningen har också föreslagit lednings- och ansvarsförhållanden för verksamheten, former för samverkan mellan de olika myndigheterna och hur samverkan ska regleras. I den första delen analyserades även om myndigheterna var i behov av förtydligade uppgifter och befogenheter för att tillsammans utföra centrets uppgifter.[1]

I detta delbetänkande analyserar och föreslår utredningen hur personal-, arbetsgivar-, budget- och säkerhetsskyddsfrågor ska regleras. Utredningen analyserar och föreslår också hur informationsutbyte ska ske inom centret och med de aktuella myndigheterna samt mellan centret och andra offentliga och privata aktörer. Utredningen ser även över hanteringen av personuppgifter i centrets verksamhet.

Uppdragsbeskrivningen i sin helhet finns i bilaga 1.

2.2 Samråd och dialog

Under utredningens arbete med det andra delbetänkandet har utredningen haft möten och kontakt med Försvarets radioanstalt, Försvarsmakten, Säkerhetspolisen, Arbetsmiljöverket, Arbetsgivarverket och cybersäkerhetscentrets kansli. Utredningen har även haft möten med utredningen med uppdrag att granska hur it-incidenten hos bolaget Tietoevry den 20 januari 2024 hanterades och följdes upp hos de myndigheter som ingår i Nationellt cybersäkerhetscenter (Fö2024/00754).

[1] Se *Ett nytt Nationellt cybersäkerhetscenter - Ändamålsenliga och effektiva former för ledning, organisering och styrning* (Fö2024/00785).

3 Bakgrund

3.1 Utredningens första delbetänkande

Utredningen har i sitt första delbetänkande föreslagit att Nationellt cybersäkerhetscenter (NCSC) ska bli en del av Försvarets radioanstalt. Genom utredningens förslag får Försvarets radioanstalt ansvar för samordning, utveckling och genomförande av centrets verksamhet. Det innebär att verksamheten i NCSC är en del av Försvarets radioanstalt och att det är Försvarets radioanstalt som beslutar om verksamhetens inriktning och innehåll utifrån de uppgifter som anges i den föreslagna förordningen om Nationellt cybersäkerhetscenter. Utredningen föreslår också att verksamheten ska präglas av ett allriskperspektiv.

De sju myndigheter som redan ingår i cybersäkerhetscentrets verksamhet ska fortsätta att göra detta och ska bidra till verksamheten inom ramen för sina verksamhetsområden. Detta ska framgå av myndigheternas instruktioner. Utredningen föreslår att det i förordningen om Nationellt cybersäkerhetscenter ska anges att den verksamhet som centermyndigheterna kan utföra inom ramen för cybersäkerhetscentret ska utföras inom ramen för centret för att tydliggöra att centrets verksamhet förutsätter samverkan och samarbete.

Försvarets radioanstalt har inte rättslig möjlighet att besluta om de andra myndigheternas bidrag till verksamheten. Det behövs därför dialog mellan centermyndigheternas ledningar om vilka resurser som ska tillföras verksamheten. Denna dialog ska ske i ett strategiskt samverkansråd där centermyndigheterna företräds av myndighetschefen eller chef på motsvarande nivå. Samverkansrådet ska också ge råd till generaldirektören för Försvarets radioanstalt om verksamheten i cybersäkerhetscentret, till exempel i strategiska ledningsfrågor, och bistå och ge råd vid beredning av bland annat budgetunderlag, verksamhetsplanering, årsrapporter och annan rapportering och redovisning till regeringen.[2]

Utredningen föreslog vidare att den operativa verksamhetens organisation inte ska regleras i förordning utan ska byggas upp utifrån verksamhetens behov.

Utredningen bedömde också att centrets uppgifter förutsätter att verksamheten i den nationella CSIRT:en (Computer Emergency Response Team) förs över från Myndigheten för samhällsskydd och beredskap (MSB) till Försvarets radioanstalt och NCSC. De närmare förutsättningarna för denna verksamhetsöverföring bör utredas i ett annat sammanhang. Utredningens förslag och slutsatser i detta delbetänkande bör läsas tillsammans med de förslag och slutsatser som presenterats i utredningens första delbetänkande.

[2] Se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 5.4.1.

4 Personal, arbetsgivaransvar och arbetsledning

4.1 Utgångspunkter

Det finns inte någon gemensam rutin för hur och i vilken omfattning personal från centermyndigheterna ska verka inom centret, eller någon gemensam uppfattning om vem som arbetsleder personalen. Det har varit oklart vilket ansvar och vilket mandat som centerchefen har att leda och fördela arbetet. Det är därför nödvändigt att uppmärksamma frågor om personal och arbetsledning. Att centrets behov styr tillsättning av personal måste också bli tydligare.[3]

4.2 Personal i NCSC

4.2.1 Grundbemanning

Utredningens förslag: Det ska framgå av förordningen om Nationellt cybersäkerhetscenter att personal från de deltagande myndigheterna ska placeras i centret. Placering av personal i verksamheten ska ske efter överenskommelse mellan Försvarets radioanstalt och den myndighet där personalen är anställd.
Utredningens bedömning: Centermyndigheterna bör få i uppdrag att årligen återrapportera vilka personalresurser de har bidragit med och vilket arbete som har utförts i centret.

Ett stabilt och effektivt center kräver en viss grundbemanning. Den största delen av personalen kommer vara anställd av Försvarets radioanstalt eftersom centret blir en del av myndigheten. Men det kommer även behövas kontinuerlig bemanning från övriga centermyndigheter för att få tillgång till myndigheternas perspektiv, kompetenser och befogenheter. En sådan närvaro är också en nödvändighet för en effektiv delning av information. I vilken utsträckning och på vilket sätt personalen ska ingå i grundbemanningen ska respektive myndighet och Försvarets radioanstalt komma överens om. Antalet personer kommer rimligen variera beroende på myndighetens kompetens och verksamhetsområde. Efterfrågan kan även variera över tid beroende på hur centrets uppgifter och behov utvecklas. Det väsentliga är att samtliga centermyndigheter finns kontinuerligt representerade så att förtroendefulla samverkansformer kan

[3] Se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 3.5 och 5.2.1.

byggas upp. En grundbemanning är även en förutsättning för att kunna hantera akuta händelser.[4]

För att säkerställa att centret har tillgång till den personal som verksamheten kräver ska det framgå av förordningen om Nationellt cybersäkerhetscenter att centermyndigheterna ska placera personal i centret.

Generaldirektören för Försvarets radioanstalt bör ha en nära dialog med centerchefen och efterfråga vilken personal centret behöver. Denna information bör förmedlas vidare i det strategiska samverkansrådet[5]. Försvarets radioanstalt kommer dock ha det övergripande ansvaret att se till att centret har den personal som verksamheten kräver.

För att säkerställa att centermyndigheterna bidrar med relevanta personalresurser bör myndigheterna få i uppdrag att årligen återrapportera till regeringen vilka resurser de har bidragit med och vilket arbete som har utförts i centret.

4.2.2 Flexibel bemanning

Tillfällig personal från centermyndigheterna

Centret kan också ha behov av personal med viss kompetens för att utföra specifika uppgifter eller för att delta i särskilda projekt. Genom Försvarets radioanstalts möjlighet att framföra önskemål om placering av personal i verksamheten, och att personalen placeras i centret efter överenskommelse med berörd centermyndighet, kan det säkerställas att centret har tillgång till den kompetens och andra resurser som en effektiv verksamhet förutsätter.

Denna personal kommer fortfarande vara anställd av en annan centermyndighet, men tjänstgöra i NCSC på uppdrag av sin ordinarie arbetsgivare under en viss period.

Personallån

Även personallån[6] kan tillgodose kortsiktiga behov av särskild kompetens i verksamheten.

Personallån omfattas inte av det upphandlingsrättsliga regelverket.[7] Utredningen bedömer att personallån framför allt är till nytta när centret är i behov av kompetens från en myndighet som inte deltar i cybersäkerhetscentrets verksamhet. Personal från centermyndigheterna kan placeras kort- och långsiktigt inom centret i och med det författnings-

[4] Se vidare *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 5.4.2.

[5] Se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, 5.4.1.

[6] Myndigheters deltagande vid personallån kan utgöra ett sådant samarbete som regleras i 6 § andra stycket myndighetsförordningen (2017:515). Där framgår att myndigheterna ska verka för att genom samarbete med andra myndigheter tillvarata de fördelar som kan finnas för enskilda samt för staten som helhet. Personallån kan även ses som ett stöd enligt 9 § förordningen (2022:524) om statliga myndigheters beredskap. Av denna bestämmelse följer att myndigheter ska samverka och stödja varandra vid en fredstida krissituation.

[7] Det upphandlingsrättsliga regelverket är inte tillämpligt på anskaffningar mellan statliga myndigheter under regeringen, jfr. Högsta förvaltningsdomstolens avgörande HFD 2021 ref. 35 och EU-domstolens avgörande C-26/03, *Stadt Halle*, p. 48.

reglerade samarbetet som utredningen föreslår och behöver därför inte bli föremål för personallån för att deras kompetens ska kunna nyttjas av NCSC.

För att kunna hantera personallån på ett snabbt och effektivt sätt kan Försvarets radioanstalt som huvudansvarig ingå samarbetsöverenskommelser med relevanta myndigheter. Av en sådan överenskommelse bör förutsättningarna för framtida personallån framgå.[8]

NCSC bör också förbereda sig för att kunna hantera en lånesituation, bland annat genom att analysera vilken eller vilka myndigheter centret kan tänkas behöva hjälp av och upparbeta samarbeten med dessa myndigheter.

Det finns dock vissa faktorer som innebär begränsningar i hur personallån kan nyttjas. Ett lån får i praktiken inte innebära en ny anställning eftersom det finns ett omfattande regelverk som måste beaktas vid tillsättning av en statlig tjänst. Arbetsgivarverket har som rekommendation angett att en period om tre till sex månader för lån av personal borde vara tillåten.[9]

Utredningen ser dock inte att detta innebär något problem för centrets verksamhet eftersom personal som blir föremål för lån är avsedd att täcka tillfälliga behov av kompetens. Mer långvariga behov tillgodoses genom Försvarets radioanstalts anställda eller andra centermyndigheters personal som tjänstgör i centret.

En ytterligare faktor att beakta är att inlånad personal måste genomgå en säkerhetsprövning om personen ska delta i säkerhetskänslig verksamhet.[10]

Även om personalen från övriga centermyndigheter i första hand inte kommer bli föremål för personallån, kan det finnas tillfällen där även personallån från centermyndigheter är ändamålsenliga. Personallån från centermyndigheterna innebär enklare hantering av bland annat säkerhetsskyddsfrågor och sekretessbelagd information eftersom inlånad personal får en ställning som liknar den som anställda hos den inlånande myndigheten har.[11]

Inköp av konsulttjänster

NCSC har möjlighet att utan upphandling köpa in konsulttjänster och andra resurser av andra statliga myndigheter. Om NCSC däremot köper in tjänster från en aktör som inte är en statlig myndighet behöver NCSC tillämpa aktuellt upphandlingsrättsligt regelverk.

4.3 Slutsatser om personal

Personalen i centret kommer till största delen bestå av personal som är anställd av Försvarets radioanstalt.

Men det finns också behov av kontinuerlig närvaro och medverkan av övriga centermyndigheter i verksamheten för att bygga upp välfungerande

[8] Jfr. Ds 2022:26, *En hjälpande hand – ökade möjligheter till in- och utlån av personal mellan myndigheter*, s. 129–131.
[9] Jfr. 12 kap. 5 § regeringsformen och 4 § lagen (1994:260) om offentlig anställning och Arbetsgivarverket, *Promemoria avseende kompetensbehov hos vissa statliga myndigheter med anledning av flyktingsituationen*, daterad 2015-10-21, reviderad 2016-02-17.
[10] Jfr. Ds 2022:26, s. 85.
[11] Ds 2022:26 s. 83, 94–96.

samverkan mellan centermyndigheterna, vilket är en förutsättning för att exempelvis informationsdelningen och erfarenhetsutbytet ska fungera effektivt. Den osäkerhet som idag finns om vilken information som kan delas internt innebär en utmaning för verksamheten som delvis kan underlättas av att personalen från de olika myndigheterna i centret lär känna varandra och upparbetar ett ömsesidigt förtroende, se vidare avsnitt 5.3.

Utredningen har ovan redovisat olika möjligheter att tillgodose personalbehovet. Bibehåller personalen sin anställning hos sin ordinarie arbetsgivare innebär det att personalen representerar arbetsgivaren, dess mandat och verksamhetsområde. Det är viktigt för att personalen ska kunna bidra till ett utökat informationsutbyte eller utöva en specifik myndighets mandat och representera en specifik myndighets verksamhetsområde. Är det i stället så att en viss personalgrupp främst är av intresse för att de har en specifik kompetens och behovet enbart avser en begränsad tid är personallån ett bättre alternativ av exempelvis sekretesskäl och säkerhetsskyddsskäl.

Utredningens slutsats är att det kommer finnas behov av olika personalkategorier med olika former av anställning för att tillgodose personalbehovet i centrets verksamhet. För att säkerställa att rätt personal från myndigheterna tjänstgör i NCSC ska placeringen av personalen ske efter överenskommelse med Försvarets radioanstalt. Utredningen anser att bemanningen i cybersäkerhetscentret ska vara efterfrågestyrd. Med detta menas att det är centrets behov som ska vara ledande för vilken personal de olika centermyndigheterna tillgängliggör för arbete i centret.[12]

[12] Se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning* avsnitt 5.1 och 5.3.1.

4.4 Arbetsgivaransvar

Försvarets radioanstalt övertar inte arbetsgivaransvaret för den personal som arbetar inom centret om personalen är anställd vid en annan myndighet. Personalens arbetsgivare har fortfarande arbetsgivaransvaret. Avgörande för vem som är arbetsgivare, och som därigenom har arbetsgivaransvar, är vilket rättssubjekt som har slutit avtalet om anställning.[13]

4.4.1 Arbetsledning och arbetsskyldighet

Utredningens bedömning: För en effektiv verksamhet krävs det att centerchefen har möjlighet att arbetsleda personal som arbetar i centret. Centermyndigheterna kan med stöd av överenskommelser med Försvarets radioanstalt placera personal i centrets verksamhet under centerchefens arbetsledning. Denna möjlighet tydliggörs av att deltagandet i centrets verksamhet regleras i centermyndigheternas instruktioner och placeringen av personal i centret regleras i förordningen om Nationellt cybersäkerhetscenter.

Arbetsgivaren har arbetsledningsrätt, vilket innebär att arbetsgivaren ensidigt kan bestämma vilka arbetsuppgifter arbetstagaren ska utföra samt var och när arbetet ska utföras inom arbetstagarens arbetsskyldighet. Arbetsledningsrätten kan däremot begränsas av lag, kollektivavtal eller det individuella anställningsavtalet.[14]

Om annat inte följer av lag eller avtal anses arbetstagaren i princip vara skyldig att följa en av arbetsgivaren såsom arbetsledningsåtgärd vidtagen omplacering eller förändring av arbetsuppgifterna om förutsättningarna enligt den s.k. 29/29-principen[15] är uppfyllda. Principen anger tre gränslinjer för arbetstagarens arbetsskyldighet:

- Arbetet ska ha naturligt samband med arbetsgivarens verksamhet.
- Arbetet ska utföras för arbetsgivarens räkning.
- Arbetet ska falla inom arbetstagarens allmänna yrkeskvalifikationer.

Inom den offentliga sektorn gäller därutöver som en allmän princip att en arbetstagare inte är skyldig att underkasta sig sådana ändringar av sina arbetsuppgifter att anställningen ändras i grunden.[16]

Detta hindrar dock inte att en arbetstagare kan vara skyldig att i enlighet med arbetsgivarens instruktion utöva arbete under annans ledning, om detta sker i arbetsgivarens intresse.[17]

[13] Se till exempel AD 2019 nr 17.
[14] Malmström, Ramberg, *Malmströms Civilrätt*, 2022, s. 316–317.
[15] AD 1929 nr 29.
[16] Se till exempel AD 2021 nr 37 och AD 1998 nr 39.
[17] Se till exempel AD 1983 nr 156, AD 1996 nr 113, AD 2021 nr 37, AD 2021 nr 57 och Ds 2022:26, s. 71–72.

Att en arbetstagare förflyttas organisatoriskt men behåller sina arbetsuppgifter innebär som huvudregel att det sker inom arbetsskyldigheten, så länge det inte är alltför långt geografiskt avstånd. Arbetstagaren är skyldig att såväl tillfälligt som permanent godta att placeras på annan arbetsplats på samma ort eller på en ort som ligger nära.[18]

Utredningen bedömer att detta innebär att arbetstagare som kommer från centermyndigheter kan utföra arbetsuppgifter inom centret under centerchefens ledning. Centermyndigheterna får med förslaget en skyldighet att medverka i och bidra till centrets verksamhet inom ramen för sina verksamhetsområden. Arbetstagarna kommer vidare utföra uppgifter i centret som motsvarar eller är närliggande till de uppgifter de utför hos sin arbetsgivare i normala fall.

Att arbetstagaren placeras på ett annat ställe är inte heller i sig ett hinder för arbetsskyldigheten så länge förflyttningen inte är allt för lång. Utredningens bedömning är alltså att det finns förutsättningar för centermyndigheterna att placera sin personal i centret.

Det finns andra exempel på samarbeten där personal från myndigheter ställs under en annan myndighets arbetsledning. Ett sådant exempel är Nationellt centrum för terrorhotbedömning (NCT) som består av en permanent arbetsgrupp med personal från Försvarets radioanstalt, Militära underrättelse- och säkerhetstjänsten (Must) och Säkerhetspolisen. Arbetet leds av chefen för NCT efter inriktning från en styrgrupp bestående av chefer från respektive myndighet. Samarbetet inom NCT är formaliserat genom en överenskommelse mellan myndigheterna. Överenskommelsen reglerar bland annat myndighetsansvar, ledning och styrning.[19]

Med stor sannolikhet kommer det finnas behov av liknande överenskommelser rörande NCSC för att klargöra olika aspekter av ansvar och arbetsledning. I en sådan överenskommelse bör framgå att arbetet inom centret utförs under arbetsledning av centerchefen.

Vad gäller inlånad personal är även här möjligheterna goda att den inlånade personalen arbetar under arbetsledning av centerchefen under förutsättning att det är inom ramen för arbetsskyldigheten. Som ovan nämnts är det av betydelse att förutsättningar fastställs i överenskommelser även avseende inlånad personal.[20]

[18] Se till exempel AD 1995 nr 133 och AD 2017 nr 59.
[19] Ds 2016:31, *Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning*, s. 43–47.
[20] Ds 2022:26, s. 65–67, 126 och 129–131.

4.4.2 Arbetsmiljöansvar

Utredningens bedömning: Arbetsgivaren har det övergripande ansvaret för arbetsmiljön. Försvarets radioanstalt är rådighetsansvarig och samordningsansvarig för arbetsmiljön i centrets verksamhet.

För personal som inte är anställda av Försvarets radioanstalt ansvarar Försvarets radioanstalt och personalens arbetsgivare för olika delar av arbetsmiljön.

Rådighetsansvar

Utgångspunkten är att arbetsgivaren har en skyldighet att se till att arbetsmiljön på arbetsplatsen är så god som möjligt. Det är därmed personalens arbetsgivare som har det övergripande ansvaret för arbetsmiljön. Av 2 kap. 1 § arbetsmiljölagen (1977:1160) följer att arbetsmiljön ska vara tillfredsställande med hänsyn till arbetets natur och den sociala och tekniska utvecklingen i samhället.[21]

Av 3 kap. 12 § första stycket arbetsmiljölagen framgår att den som råder över ett arbetsställe ska se till att det på arbetsstället finns sådana fasta anordningar att den som arbetar där utan att vara arbetstagare i förhållande till den som råder över arbetsstället inte utsätts för risk för ohälsa och olycksfall. Denna bestämmelse avser sådana anläggningar som bara den som råder över arbetsstället disponerar. Bestämmelsen riktar sig uttryckligen till den som råder över ett visst arbetsställe. Avsikten är att fastlägga ett ansvar för arbetsgivare eller egenföretagare, som disponerar över ett arbetsställe, men inte att reglera ansvaret för ägare eller nyttjanderättshavare till en fastighet.[22]

Det framgår vidare av andra stycket samma bestämmelse att den som anlitar inhyrd arbetskraft att utföra arbete i sin verksamhet är skyldig att vidta de skyddsåtgärder som behövs i det arbetet. Inhyrd arbetskraft är inordnad i verksamheten och står under arbetsledning på ett sätt som gör att de är att jämställa med arbetstagare i denna verksamhet. Ansvaret är dock begränsat till det aktuella arbetet på arbetsplatsen. De långsiktiga arbetsmiljökraven ligger fortfarande kvar på arbetsgivaren, det vill säga den som hyr ut arbetskraften. När det gäller arbetsmiljöåtgärder som behövs i arbetet ska en rimlig fördelning göras mellan den arbetsgivare som hyrt in arbetskraften och den arbetsgivare som hyrt ut arbetskraften utifrån omständigheterna i det enskilda fallet. Uthyrare och inhyrare bör precisera hur skyddsansvaret mellan dem ska fördelas.[23]

Försvarets radioanstalt kommer vara ansvarig för lokaler och personalens arbetsställe. Utredningen bedömer att Försvarets radioanstalt kommer att vara rådighetsansvarig och är därmed ansvarig för anordningar på arbetsstället, även i den tillfälliga lokalen. Ansvaret för åtgärder avseende fasta anordningar kan dock vara delat mellan Försvarets radioanstalt och den som upplåter lokalen.[24]

[21] Jfr. 3 kap. 2 § och 3 kap. 2 a § arbetsmiljölagen.
[22] Prop. 1973:130, *Kungl. Maj:ts proposition angående ändringar i arbetarskyddslagstiftningen och andra åtgärder för en bättre arbetsmiljö*, s. 209 och prop. 1993/94:186, *Ändringar i arbetsmiljölagen*, s. 31 och 67.
[23] Prop. 1993/94:186, s. 34–35 och 68.
[24] Jfr. 7 kap. 8 § arbetsmiljölagen och prop. 1993/94:186, s. 36–37.

När personal från centermyndigheter placeras i centrets verksamhet omfattas de av Försvarets radioanstalts rådighetsansvar vad gäller anordningar. Det finns dock andra arbetsmiljöfaktorer såsom organisatoriska och sociala som är av betydelse för centrets verksamhet. Dessa omfattas inte enligt nuvarande reglering av Försvarets radioanstalts ansvar för arbetsmiljön. Ansvaret för arbetsmiljön är därför avseende andra arbetsmiljöaspekter kvar hos arbetsgivaren trots arbetsgivarens begränsade möjlighet att faktiskt påverka arbetsmiljöförhållandena.[25]

En utredning, SOU 2022:45, har lämnat förslag på ändringar som innebär att den som anlitar en fysisk person för att utföra arbete i sin verksamhet utan att anställa eller hyra in den som utför arbetet, och har det huvudsakliga inflytandet över arbetsmiljön, ska vidta de skyddsåtgärder som behövs i detta arbete.[26]

Denna föreslagna bestämmelse kan eventuellt påverka arbetsmiljöansvaret i centret. Det ska framhållas att SOU 2022:45 som innehåller de föreslagna ändringarna inte är färdigbehandlad och att någon proposition ännu inte finns. Därmed innebär den nu gällande regleringen att Försvarets radioanstalt endast har ett rådighetsansvar för anordningar trots arbetsgivarens begränsade möjlighet att påverka arbetsmiljön i centret.

Personalen som lånas in till centrets verksamhet kommer rimligen omfattas av 3 kap. 12 § andra stycket arbetsmiljölagen. Arbetsmiljöansvaret bör då vara uppdelat mellan Försvarets radioanstalt och den utlånande myndigheten och inte avgränsas till Försvarets radioanstalts rådighetsansvar för anordningar. För det arbetet som utförs i centrets verksamhet får Försvarets radioanstalt ett ansvar som i stort motsvarar arbetsgivarens ansvar och ska därför vidta skyddsåtgärder som myndigheten skulle ha vidtagit för anställd personal. Den utlånande myndigheten behåller huvudansvaret för arbetsmiljön och även ansvar för åtgärder som rehabilitering. Arbetsmiljöansvaret bör tydliggöras genom överenskommelser mellan berörda myndigheter.[27]

Samordningsansvar

I sammanhanget ska även lyftas fram 3 kap. 7 d § arbetsmiljölagen som bland annat anger att om ett fast driftställe är gemensamt arbetsställe för flera verksamheter, är den som råder över arbetsstället ansvarig för samordningen av arbetsmiljöfrågor. Detta ansvar kan överlåtas till någon som bedriver verksamhet på arbetsstället. Enligt 3 kap. 7 e § punkt 1 samma lag ska den som är ansvarig för samordningen se till att arbetet med att förebygga risker för ohälsa och olycksfall samordnas på det gemensamma arbetsstället. Den samordningsansvarige har ett ansvar att samordna frågor om arbetsmiljön mellan olika arbetsgivare.[28]

Ansvaret gäller de gemensamma arbetsmiljörisker som uppkommer på grund av att flera verksamheter bedrivs på en arbetsplats och är ett ansvar

[25] Jfr. SOU 2022:45, *Steg framåt, med arbetsmiljön i fokus*, s. 62–63.
[26] SOU 2022:45, s. 21 och 153–154.
[27] Se 3 kap. 2 a § tredje stycket arbetsmiljölagen vad gäller rehabilitering. Jfr. Ds 2022:26, s. 106–109.
[28] Prop. 1993/94:186, s. 29.

som tillkommer utöver det som är varje enskilds arbetsgivares skyldighet.[29]

Försvarets radioanstalt blir enligt utredningens bedömning även samordningsansvarig i och med sitt rådighetsansvar. Detta innebär ett ansvar för myndigheten att samordna frågor om arbetsmiljön mellan centermyndigheterna. I arbetet med att förebygga risker för ohälsa borde även frågor om bland annat den psykosociala arbetsmiljön inkluderas. Det kan därför vara nödvändigt att inom centret ta fram policyer och andra styrdokument för arbetsmiljöfrågor.

4.5 Slutsatser om arbetsgivaransvar m.m.

Som redogjorts för ovan finns det flera olika personalkategorier som kan bli aktuella för tjänstgöring i centrets verksamhet. En stor del av personalen kommer vara anställda av Försvarets radioanstalt, vilket innebär ökad tydlighet i fråga om arbetsgivaransvar, rätten att arbetsleda och ansvar för arbetsmiljö. Även för personal som blir föremål för personallån blir ansvarsfördelningen tydlig, men överenskommelser där de närmare förutsättningarna för exempelvis arbetsledning och arbetsmiljö behöver ingås.

En effektiv verksamhet förutsätter att centerchefen har möjlighet att arbetsleda all personal, alltså även personal från de andra centermyndigheterna. Personalens arbetsgivare kan genom att ingå överenskommelser med Försvarets radioanstalt lämna arbetsledningsansvaret för personalen som placeras i NCSC till centerchefen, vilket möjliggör en effektiv organisation där centerchefens mandat och möjlighet att driva verksamheten blir tydligare och starkare.[30]

Personalens arbetsgivare har det övergripande arbetsmiljöansvaret. Arbetsmiljöansvaret blir däremot i viss mån uppdelat. För de som är anställda hos Försvarets radioanstalt har myndigheten hela arbetsmiljöansvaret. För inlånad personal ansvarar Försvarets radioanstalt i stort sett på samma sätt som om myndigheten är arbetsgivare och ska vida skyddsåtgärder som myndigheten skulle ha vidtagit för anställd personal. Däremot ligger delar av arbetsmiljöansvaret kvar på hemmamyndigheten. För personalen som är anställd av övriga centermyndigheter kommer arbetsmiljöansvaret vara uppdelat. Försvarets radioanstalt har rådighetsansvar och ansvarar därigenom för fasta anordningar på arbetsstället. Myndigheten får också samordningsansvar för andra arbetsmiljöaspekter.

[29] Iseskog, *Arbetsmiljöansvar*, Nordstedts Juridik, (2020 JUNO) under rubriken 10.4 Samordningsskyldighet/-ansvar i övriga fall.
[30] Se vidare om centerchefens roll, *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 5.2.1.

5 Informationsdelning

5.1 Informationsdelningen idag

Cybersäkerhetscentrets verksamhet bygger på ett ömsesidigt informationsutbyte, både internt och externt. Informationsutbytet ska ske både mellan centermyndigheterna och mellan NCSC samt näringslivet och andra aktörer. Som redan återgetts i utredningens första delbetänkande har inte informationsdelningen inom NCSC fungerat fullt ut, varken internt eller externt. Problemen har varit juridiska, kulturella och kommit sig av bristande systemstöd.[31]

Riksrevisionen lyfter särskilt fram att Försvarets radioanstalt, Försvarsmakten och Säkerhetspolisen är underrättelsemyndigheter[32] med både legala och kulturella hinder för informationsdelning. Sekretess och överenskommelser med andra aktörer kan utgöra hinder för underrättelsemyndigheterna att dela information.[33]

Vid de möten utredningen haft har vidare framkommit att informationsdelning begränsats av att den personal från de deltagande myndigheterna som arbetar i centret inte i tillräckligt stor omfattning har kunskap om de sekretessregler som finns. Det medför att de inte delar information med de övriga myndigheterna i den utsträckning som egentligen är möjlig enligt gällande lagstiftning.

När det gäller informationsdelningen med näringslivet uppges det också finnas brister och problem. Näringslivsföreträdare anser att myndigheterna saknar intresse för samarbete och förståelse för vad näringslivet kan bidra med. Det saknas också standardisering eller tydliga riktlinjer för vilken information som är aktuell att dela mellan myndigheterna och näringslivet. Riksrevisionen bedömer att avsaknaden av standardisering har gjort informationsdelning svårare både internt och externt.[34]

[31] Se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 3.5. och *Regeringens styrning av samhällets informations- och cybersäkerhet − både brådskande och viktig* (RiR 2023:8), s. 44.
[32] Säkerhetspolisen och Försvarsmakten är inte underrättelsemyndigheter per definition. Säkerhetspolisen är en säkerhetstjänst och hos Försvarsmakten är det bara den delen av myndigheten som utgörs av Must som kan benämnas som en ”underrättelsemyndighet”. Delar av Säkerhetspolisens verksamhet och den delen av Försvarsmakten som utgörs av Must fungerar dock i praktiken som underrättelsemyndigheter.
[33] RiR 2023:8, s. 45.
[34] RiR 2023:8, s. 46–47.

5.2 Intern informationsdelning

5.2.1 Rättsliga utgångspunkter

Handlingsoffentlighet och sekretess

Möjligheten att dela information internt mellan myndigheterna i NCSC styrs av olika regelverk, bland annat regelverket om allmänna handlingar i tryckfrihetsförordningen (TF). Enligt TF har varje svensk medborgare rätt att ta del av allmänna handlingar. En handling är allmän om den förvaras hos en myndighet och anses inkommen till myndigheten eller upprättad där.[35]

Handlingsoffentligheten gäller främst i det allmännas verksamhet och i viss utsträckning i vissa privaträttsliga organ. Rätten att ta del av allmänna handlingar begränsas endast om det krävs med hänsyn till vissa angivna intressen, till exempel skyddet för enskilds personliga eller ekonomiska förhållanden eller intresset att förebygga eller beivra brott. En sådan begränsning ska anges i en bestämmelse i OSL eller, om det i visst fall är lämpligare, i en annan lag.[36]

Sekretess innebär att det finns ett förbud att röja en uppgift. Sekretess kan gälla såväl mot enskilda som andra myndigheter och även i vissa fall mellan olika verksamhetsgrenar.

Det saknas särskilda sekretessregleringar som reglerar delning av information mellan samtliga centermyndigheter. Det finns dock generella bestämmelser som ger möjlighet att dela både offentlig och sekretessreglerad information.[37]

Myndigheter ska enligt förvaltningslagen (2017:900), FL, samverka med varandra, även avseende informationsdelning. Myndigheter har både uppgifter som är offentliga och som omfattas av sekretess. Enligt OSL ska en uppgift som är offentlig och som en myndighet förfogar över på begäran av en annan myndighet lämnas ut om den inte är sekretessbelagd och utlämnandet hindrar arbetets behöriga gång.[38]

Uppgifter som omfattas av sekretess får inte lämnas ut varken till andra myndigheter eller enskilda om det inte finns stöd för det i OSL eller annan författning. Sekretess i detta avseende gäller också mellan självständiga verksamhetsgrenar inom en och samma myndighet. Om en sekretessbestämmelse är primär, dvs. att den gäller både hos den utlämnande och den mottagande myndigheten hindrar den dock inte att det sker ett utbyte av uppgifter mellan myndigheter. Primära sekretessbestämmelser innebär att sekretessen följer med oavsett till vilken myndighet en uppgift lämnas vilket underlättar den sekretessprövning som ska göras innan en uppgift

[35] 2 kap. 1 och 2 kap. 3–4 §§ TF.
[36] Jfr. 2 kap. 2 § TF.
[37] 3 kap. 1 § OSL och 8 kap. 1 och 2 §§ OSL.
[38] Jfr. 8 § FL och 6 kap. 5 § OSL. Bestämmelsen i FL om samverkan innebär ingen uppgiftsskyldighet för myndigheterna att dela sekretessreglerade information med varandra, jfr prop. 2016/17:180, *En modern och rättssäker förvaltning – ny förvaltningslag*, s. 70–71.

kan lämnas ut. Om en uppgift genomsnittligt sett måste betraktas som harmlös ska den normalt anses falla utanför sekretessen.[39]

Sekretess kan brytas genom sekretessbrytande bestämmelser, vilket innebär att en sekretessbelagd uppgift får lämnas ut under vissa förutsättningar. Sådana bestämmelser kan också innebära att myndigheter eller andra organ har en uppgiftsskyldighet gentemot varandra. Med uppgiftsskyldighet avses att det av en särskild lag eller av förordning följer att en uppgift ska lämnas till en annan myndighet. Sekretessbrytande bestämmelser finns både i OSL och andra författningar.[40]

Annan reglering och förutsättningar som påverkar möjligheten till informationsdelning

Det finns även andra regleringar som kan påverka möjligheten att utbyta information mellan centermyndigheterna. Exempelvis lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott som förbjuder användandet av information från Försvarets radioanstalts underrättelseverksamhet för utredning av brott.

Utöver författning kan också centermyndigheternas överenskommelser med uppdragsgivare eller andra samarbetspartners inskränka möjligheterna att dela information med de övriga deltagande myndigheterna. Interna myndighetsregleringar kan också innebära begräsningar i hur information kan delas.

Vissa uppgifter som finns hos centermyndigheterna är säkerhetsskyddsklassificerade. Även om en större del av informationen som kommer hanteras inom centret troligen inte kommer vara av sådan art finns bestämmelser i säkerhetskyddslagstiftningen som påverkar möjligheten att dela sådan information, se avsnitt 7.2.1.

Försvarets radioanstalt, Försvarsmakten genom Must och Säkerhetspolisen har särskilda förutsättningar för informationsdelning. Dels har myndigheterna en utökad möjlighet att dela viss information med varandra, dels kan deras möjlighet till informationsdelning med andra myndigheter och med näringslivet begränsas av till exempel överenskommelser med samarbetspartners om hur information får användas. Dessutom måste informationsdelningen ske på ett sådant sätt att inhämtningsmetoder eller källor inte röjs.[41]

Utöver regleringar som särskilt behandlar sekretess påverkar också regleringar om behandling av personuppgifter möjligheterna att dela uppgifter, se avsnitt 6.[42]

5.2.2 Aktuella sekretessbestämmelser

De uppgifter som kommer hanteras inom NCSC omfattas av flera olika sekretessbestämmelser. Mest relevanta är 15 kap. 1–2 § OSL och 18 kap.

[39] Jfr. HFD 2021 not. 58, p. 11–15, 8 kap. 1–2 §§ OSL, prop.1979/80:2 Del A, *Regeringens proposition med förslag till ny sekretesslag*, s. 80 och prop. 2023/24:60, *En telesamverkansgrupp för fredstida kriser och höjd beredskap*, s. 24.
[40] Prop. 1979/80:2 del A s. 322. Jfr. till exempel lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet.
[41] RiR 2023:8, s. 45.
[42] Jfr. även 21 kap. 7 § OSL, sekretess gäller för personuppgifter om dessa efter ett utlämnande kan antas komma att behandlas i strid med GDPR.

8 § OSL. Andra bestämmelser kan bli relevanta beroende på hur verksamheten i centret utvecklas.[43]

De sekretessbestämmelser som aktualiseras är sådana som är till skydd för det allmänna och som är tillämpliga i alla myndigheter och organ som ska tillämpa OSL.

Sekretess enligt 15 kap. 1 § OSL

Av 15 kap. 1 § OSL följer att sekretess gäller för uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs.

Paragrafen reglerar utrikessekretessen. Bestämmelsen är primär och kan tillämpas av alla myndigheter och organisationer som ska tillämpa OSL.[44]

Föremålet för sekretessen är i första hand uppgifter som rör Sveriges förbindelser med annan stat. Detta ska förstås bredare än bara utrikespolitiska förbindelser. Även handelsförbindelser och kulturella förbindelser med mera innefattas i begreppet. Uttrycket *Sveriges förbindelser* innebär att det måste röra sig om förbindelser på nationell nivå. Om en svensk myndighet har kontakt med en främmande stat och om förbindelserna avser myndighetens egna angelägenheter så omfattas det inte av paragrafen. Företräder däremot en myndighet Sverige som nation rör det sig om Sveriges förbindelser i den mening som avses i bestämmelsen.[45]

Sekretessen omfattar också uppgifter som i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös. Denna del av bestämmelsen kräver inte att det ska röra sig om uppgifter med direkt anknytning till Sveriges förbindelser. Uppgifter om en utländsk myndighets kontakter med en svensk myndighet kan därmed falla inom paragrafens tillämpningsområde.

Bestämmelsen har ett rakt skaderekvisit. Möjligheten att sekretessbelägga uppgifter enligt 15 kap. 1 § OSL begränsas av kravet på skada för Sverige.[46]

Sekretess enligt 15 kap. 2 § OSL

15 kap. 2 § OSL reglerar sekretess för uppgifter som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs. Bestämmelsen är en primär sekretessbestämmelse vars räckvidd inte har begränsats utan den kan tillämpas av alla myndigheter och organ som ska tillämpa OSL.

[43] Jfr. till exempel 18 kap. 13 § OSL om sekretess för myndighets verksamhet som består i risk- och sårbarhetsanalyser avseende fredstida krissituationer, planering och förberedelser inför sådana situationer eller hantering av sådana situationer.
[44] Lenberg, Tansjö och Geijer, *Offentlighets- och sekretesslagen*, (2023-11-22, JUNO) kommentaren till 15 kap. 1 §.
[45] Prop. 1979/80:2 Del A, s. 130 och Lenberg, Tansjö och Geijer, *Offentlighets- och sekretesslagen*, (2023-11-22, JUNO) kommentaren till 15 kap. 1 §.
[46] Lenberg, Tansjö och Geijer, *Offentlighets- och sekretesslagen*, (2023-11-22, JUNO) kommentaren till 15 kap. 1 §.

Den har störst betydelse för Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk och andra myndigheter med verksamhet som berör försvaret. Det finns även andra myndigheter, till exempel MSB, som har skäl att tillämpa bestämmelsen. Bestämmelsen avser främst det militära försvaret men i förarbetena till motsvarande bestämmelse i 2 kap. 2 § i den tidigare sekretesslagen (1980:100) framgår att området som skyddas av försvarssekretess omfattar alla de olika verksamheter som är av betydelse för landets försvar, alltså inte bara rent militära företeelser utan också exempelvis den ekonomiska försvarsberedskapen, folkförsörjningen och det psykologiska försvaret.

Bestämmelsen har ett rakt skaderekvisit vilket innebär att sekretess gäller om det kan antas att ett röjande av en uppgift skadar Sveriges försvar eller på annat sätt innebär fara för rikets säkerhet.[47]

Sekretess enligt 18 kap. 8 § OSL

Av 18 kap. 8 § OSL följer att sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser bland annat telekommunikation eller system för automatiserad behandling av information eller behörighet att få tillgång till upptagning för automatiserad behandling eller annan handling. Bestämmelsen kan tillämpas av alla myndigheter och organ som ska tillämpa OSL.[48]

Bestämmelsen möjliggör sekretess för olika brottsförebyggande åtgärder som huvudsakligen hänför sig till annan verksamhet än polisens. Sådant som kan omfattas av sekretess enligt 18 kap. 8 § OSL är exempelvis incidentrapportering som Sveriges nationella CSIRT, CERT-SE, tar emot. Exempel på sådant som kan skyddas av sekretess är olika tekniska funktioner för användning av lösenord, loggning och kryptering, installation av brandväggar och antivirusprogram samt administrativa rutiner för till exempel utdelning av lösenord eller bevakning av loggar och larm. Som exempel på uppgifter som kan bidra till att lämna upplysningar om säkerhets- eller bevakningsåtgärder om till exempel ett operativsystem är uppgift om vilken typ och version av operativsystem som används. Sådana uppgifter kan hemlighållas om till exempel en viss version av ett operativsystem har visat sig ha svagheter som gör att det är lätt att olovligen ta sig in i systemet trots de vidtagna skyddsmekanismerna. En uppgift om vilket operativsystem som används skulle i ett sådant fall indirekt innebära en anvisning för den med rätt typ av kunskap om hur man kringgår de vidtagna skyddsåtgärderna.[49]

Bestämmelsen har ett rakt skaderekvisit vilket innebär att sekretess gäller om det kan antas att syftet med skyddsåtgärden motverkas om den aktuella uppgiften röjs.[50]

[47] Prop. 1979/80:2 Del A, s. 132–133 och Lenberg, Tansjö och Geijer, *Offentlighets- och sekretesslagen*, (2023-11-22, JUNO) kommentaren till 15 kap. 2 §.
[48] 18 kap. 8 § OSL avser även åtgärder avseende andra områden, bland annat byggnader eller andra anläggningar, lokaler och inventarier samt civil luftfart och sjöfart, hamnskydd och transporter på land av farligt gods.
[49] Prop. 1979/80:2 del A, s. 141–143 och prop. 2003/04:93, s. 79–82.
[50] Lenberg, Tansjö och Geijer, *Offentlighets- och sekretesslagen*, (2023-11-22, JUNO) kommentaren till 18 kap. 8 § samt Kammarrätten i Göteborgs dom den 29 juni 2021 i mål nr 2144-21.

5.2.3 Sekretess mellan verksamhetsgrenar inom Försvarets radioanstalt

Utredningens bedömning: Det uppstår inte någon sekretessgräns mellan Försvarets radioanstalts övriga verksamhet och cybersäkerhetscentret.

En myndighet med flera olika verksamhetsgrenar kan också ha interna sekretessgränser. Det innebär att olika delar av en myndighets verksamhet omfattas av sekretess gentemot övriga delar av myndigheten.[51]

När det gäller cybersäkerhetscentrets förhållande till övriga delar av Försvarets radioanstalts verksamhet kommer centret att ha en profil som avviker från den Försvarets radioanstalt har i övrigt och kommer även bedriva en mer utåtriktad verksamhet. Utredningen gör dock bedömningen att NCSC inte är en självständig verksamhetsgren i den mening som avses i 2 kap. 11 § TF och 8 kap. 2 § OSL.

Av 2 kap. 11 § TF följer att om ett organ som ingår i eller är knutet till en myndighet lämnat över en handling till något annat organ inom samma myndighet, anses handlingen som inkommen eller upprättad därigenom endast om organen uppträder som självständiga i förhållande till varandra. I förarbetena till TF framgår att enheter inom samma myndighet kan anses vara självständiga om de fattar överklagbara beslut i eget namn eller lämnar ett självständigt yttrande där organet definitivt skiljer sig från frågan. Omständigheter som också kan vara av betydelse är att ett organ självständigt förvaltar viss egendom, har viss handlingsfrihet inom en angiven ekonomisk ram eller i övrigt kan vidta vissa faktiska åtgärder självständigt och på eget ansvar.[52]

Cybersäkerhetscentret kommer i regel inte att självständigt fatta några överklagbara beslut i eget namn. Centret kan inte heller vidta åtgärder på eget ansvar utan lyder under generaldirektören och ledningen för Försvarets radioanstalt, precis som övriga avdelningar på myndigheten. Centerchefen är direkt underställd generaldirektören för Försvarets radioanstalt och rapporterar till generaldirektören. Centerchefens ansvar för verksamheten följer bland annat av förordningen om NCSC och delegation från generaldirektören för Försvarets radioanstalt. Att centrets verksamhet regleras särskilt i Försvarets radioanstalts regleringsbrev innebär inte att centret är självständigt från övriga delar av myndigheten eftersom centret är en del av Försvarets radioanstalt och dess chef är underställd generaldirektören vid Försvarets radioanstalt.[53]

Av 8 kap. 2 § OSL följer att en uppgift för vilken sekretess gäller inte får röjas mellan olika verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra om inte annat anges i OSL eller i annan lag eller förordning. Om olika delar av en myndighets verksamhet ska tillämpa olika sekretessbestämmelser kan de anses utgöra

[51] Ett exempel på detta är Kriminalvårdens verksamhet som består av dels kriminalvårdsverksamhet, dels sjukvårdsverksamhet. Sekretess gäller mellan dessa båda verksamhetsgrenar.
[52] Prop. 1975/76:160, *Regeringens proposition om nya grundlagsbestämmelser angående allmänna handlingars offentlighet*, s. 152.
[53] Se *Ett nytt Nationellt cybersäkerhetscenter - Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 5.2 och 5.2.1 samt jfr. HFD 2013 ref. 40.

olika verksamhetsgrenar i sekretesshänseende. Att olika delar av en myndighet tillämpar olika sekretessbestämmelser inom samma verksamhetsområde innebär dock inte att det finns olika verksamhetsgrenar i sekretesshänseende. Att en myndighet tillämpar olika sekretessbestämmelser innebär alltså inte automatiskt att det finns olika verksamhetsgrenar inom myndigheten enligt OSL. Först om det finns olika delar av en myndighets verksamhet som har att tillämpa sinsemellan helt olika set av sekretessbestämmelser är det fråga om olika verksamhetsgrenar i sekretesslagens mening. Om verksamheterna bedöms utgöra olika verksamhetsgrenar i sekretesslagens respektive offentlighets- och sekretesslagens mening måste det därefter göras en bedömning av om de också har organiserats på ett sådant sätt att de förhåller sig självständiga till varandra. Det är bara om *båda* dessa kriterier är uppfyllda som det uppstår en sekretessgräns inom en myndighet.[54]

Försvarets radioanstalt tillämpar i sin övriga verksamhet främst bestämmelser om försvarssekretess enligt 15 kap. 2 § OSL samt sekretess för säkerhets- och bevakningsåtgärd enligt 18 kap. 8 § OSL. Även sekretess enligt 15 kap. 1 § OSL kan aktualiseras. Bestämmelserna i 15 kap. 1–2 § och 18 kap. 8 § OSL kommer också att tillämpas i centrets verksamhet. Samma bestämmelser tillämpas även av övriga centermyndigheter. Utredningen gör därmed bedömningen att centret kommer att tillämpa samma sekretessbestämmelser som gäller för Försvarets radioanstalts övriga verksamhet och inte vara särskild från myndighetens andra verksamhetsområden på ett sådant sätt att det uppstår sekretesshinder mellan NCSC och övriga delar av Försvarets radioanstalt.

Det kan i vissa fall finnas ett intresse av att en verksamhetsgren inom en myndighet har sekretessgränser gentemot den övriga verksamheten vid myndigheten. I sådana fall krävs som ovan angetts dels att verksamheten är självständig i förhållande till övriga delar av myndigheter, dels att andra sekretessbestämmelser tillämpas av verksamhetsgrenen är de som tillämpas av övriga delar av myndigheten.[55]

5.2.4 Sekretessbrytande bestämmelser

I 10 kap. OSL finns sekretessbrytande bestämmelser som är tillämpliga på sekretess enligt alla eller ett stort antal sekretessbestämmelser i lagen.

10 kap. 2 § OSL

Det följer av 10 kap. 2 § OSL att sekretess inte hindrar att en uppgift lämnas till en enskild eller en myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Möjligheten att lämna ut uppgifter med stöd av 10 kap. 2 § OSL är dock begränsad och bestämmelsen är avsedd att tillämpas restriktivt. Tillämpning av bestämmelsen blir aktuell när den utlämnande myndighetens verksamhet hindras av att uppgiften inte lämnas ut. Det är alltså den utlämnande

[54] Prop. 2008/09:150, *Offentlighets- och sekretesslag*, s. 357–360.
[55] Jfr. till exempel prop. 2011/12:4, *Utredningar avseende vissa dödsfall*, s. 50–51 där det införs en sekretessgräns för en del av Socialstyrelsens utredningsverksamhet. Dels införs en ny bestämmelse i OSL om sekretess för utredningsverksamheten under en egen rubrik, dels uppmanas Socialstyrelsen att organisera verksamheten så att en sekretessgräns uppstår.

myndighetens intresse av att lämna ut uppgiften som är avgörande och inte den mottagande myndighetens intresse att få del av uppgiften. Enbart att den utlämnande myndigheten skulle kunna utföra sina uppgifter mer effektivt är inte tillräckligt för att lämna ut uppgifter med stöd av bestämmelsen.[56]

Generalklausulen i 10 kap. 27 § OSL

Av generalklausulen i 10 kap. 27 § OSL framgår att en sekretessbelagd uppgift får lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.[57]

Syftet med generalklausulen är att den ska utgöra en ventil för det fall ett utbyte av uppgifter uppenbart behöver ske och situationen inte har kunnat förutses i lagstiftningen. Bestämmelsen kan enbart tillämpas av myndigheter och tillkom för att göra det möjligt för myndigheter att utväxla uppgifter i situationer där intresset av att uppgifterna lämnas ut bör ha företräde framför det intresse som sekretessen avser skydda.[58]

Generalklausulen är subsidiär till annan lagstiftning. Finns det andra sekretessbrytande bestämmelser som är tillämpliga ska de bestämmelserna och inte generalklausulen tillämpas.

Generalklausulen kan tillämpas för att myndigheter på eget initiativ ska kunna lämna information till andra myndigheter. Det innebär att någon uttrycklig begäran från den mottagande myndigheten inte är ett krav för att bestämmelsen ska kunna tillämpas av den utlämnande myndigheten.

Prövningen av om en uppgift kan lämnas ut görs av den myndigheten där uppgiften finns. Av betydelse för bedömningen om uppgiften kan lämnas ut är bland annat om och i vilken utsträckning uppgiften är skyddad hos den myndighet som är avsedd att ta emot den. Är uppgiften skyddad hos den mottagande myndigheten är utrymmet för att lämna ut den större.[59]

I förarbetena anges att det inte finns något hinder mot att använda generalklausulen vid ett rutinmässigt informationsutbyte mellan olika myndigheter och mellan en myndighets självständiga verksamhetsgrenar. Det anges dock att sådant utbyte i regel ska vara författningsreglerat. I de undantagsfall då uppgiftslämnandet inte är författningsreglerat men ändå anses vara tillräckligt motiverat måste den intresseavvägning som ska ske vid ett utlämnande enligt generalklausulen ske på förhand. Den måste dock inte göras i varje enskilt fall utan bedömningen kan göras på ett liknande sätt som vid massuttag. Av förarbetena följer att då bör kunskap om beställarens identitet och avsikt med uppgifterna i kombination med bedömning av den skaderisk som typiskt sett finns med en viss typ av uppgifter vara tillräckligt för att bedöma om uppgifterna kan lämnas ut eller inte.[60]

[56] Jfr. prop. 1979/80:2 del A, s. 122 och Lenberg, Tansjö och Geijer, *Offentlighets- och sekretesslagen*, (2023-11-22, JUNO) kommentaren till 10 kap. 2 §.
[57] Bestämmelsen gäller dock inte sekretess i 24 kap. 2 a och 8 §§, 25 kap. 1–8 §§, 26 kap. 1–6 §§, 29 kap. 1 och 2 §§, 31 kap. 1 § första stycket, 2 och 12 §§, 33 kap. 2 och 4 a §§, 36 kap. 3 § samt 40 kap. 2 och 5 §§ och inte heller om utlämnande strider mot lag eller förordning.
[58] Prop. 1979/80:2 Del A, s. 326–327.
[59] Jfr. Prop. 1979/80:2 Del A, s. 77.
[60] Prop. 1979/80:2 Del A, s. 327 och 81–82.

10 kap. 28 § OSL

Av 10 kap. 28 § första stycket OSL följer att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Bestämmelsen gäller både mellan myndigheter och mellan en myndighets olika verksamhetsgrenar om de är självständiga i förhållande till varandra i den mening som avses i 8 kap. 2 § OSL.

Enligt bestämmelsen får uppgifter lämnas utan hinder av sekretess när det följer av annan lag än OSL eller av förordning att uppgiften ska lämnas till en annan myndighet eller verksamhetsgren. 10 kap 28 § OSL är en generell reglering om att en bestämmelse i en lag eller förordning om uppgiftsskyldighet ska tillämpas också när de uppgifter som ingår i skyldigheten att lämna uppgifter omfattas av sekretess. Det är inte nödvändigt att bestämmelsen som medför en uppgiftsskyldighet har utformats med tanke på att uppgifterna kan vara hemliga. Däremot krävs att bestämmelsen uppfyller vissa krav på konkretion. Den kan avse utlämnande av uppgifter av ett speciellt slag, avse en viss myndighets rätt att få del av uppgifter i allmänhet eller avse en skyldighet för en viss myndighet att lämna andra myndigheter information.[61]

En bestämmelse som mer generellt föreskriver att myndigheter ska samarbeta innebär inte att det finns en uppgiftsskyldighet. Det innebär till exempel att 6 § FL och 6 kap. 5 § OSL inte innebär att det finns någon uppgiftsskyldighet myndigheter emellan. Det måste också göras skillnad på uppgifter som *får* lämnas och uppgifter som *ska* lämnas till andra myndigheter. Att en myndighet får lämna uppgifter till en annan innebär inte att den har en uppgiftsskyldighet. Ett sådant utlämnande sker i stället med stöd av till exempel 10 kap. 27 § OSL, se ovan.[62]

5.3 Slutsatser om intern informationsdelning

Utredningens bedömning: Det finns juridiska förutsättningar för viss informationsdelning mellan centermyndigheterna. Myndigheterna behöver säkerställa att den personal som deltar i centrets verksamhet har tillräcklig kunskap för att avgöra vilken information som kan delas med övriga centermyndigheter. Rutiner för informationsdelning bör tas fram.

Det bör utredas om det ska införas en ny lag eller bestämmelse som utökar och förenklar möjligheterna till informationsdelning inom centret.

Det finns juridiska förutsättningar för viss informationsdelning

Utredningen är av uppfattningen att den reglering av sekretess och den möjlighet att dela information som finns idag är tillräcklig för att

[61] Prop. 1979/80:2 Del A, s. 322–323 samt Lenberg, Tansjö och Geijer, *Offentlighets- och sekretesslagen*, (2023-11-22, JUNO) kommentaren till 10 kap. 28 §.
[62] Lenberg, Tansjö och Geijer, *Offentlighets- och sekretesslagen*, (2023-11-22, JUNO) kommentaren till 10 kap. 28 §.

möjliggöra viss intern informationsdelning. De sekretessbestämmelser som generellt bör komma att användas i centrets verksamhet är sådana att de gäller i alla myndigheter. Sekretessen följer med oavsett till vilken myndighet en uppgift lämnas vilket bör underlätta den sekretessprövning som ska göras. Att sekretessprövningar behöver genomföras vid informationsdelning innebär att det kan bli tidskrävande och hindra full effektivitet och en snabb och sömlös informationsdelning inom centret.[63]

Även om informationsdelningen internt i NCSC i stor utsträckning bör ske till samtliga myndigheter kommer det finnas ett större utrymme för myndigheterna som bedriver underrättelse- och säkerhetstjänst att sinsemellan dela viss information än att dela information med samtliga myndigheter i centret. Möjligheter finns dock för de myndigheter som arbetar med känslig information att anpassa eller avidentifiera information så att den kan delas med övriga centermyndigheter när det behövs.

Det krävs att personalen har kunskap om regelverket

Det är av vikt att den personal som tjänstgör i centret är medveten om i vilken utsträckning det är möjligt att dela information med de andra centermyndigheternas personal. De legala förutsättningarna för en mer omfattande informationsdelning än den som görs i nuläget finns, men det krävs att kunskapsmässiga och kulturella hinder undanröjs för att centrets verksamhet ska effektiviseras och ett utökat informationsutbyte ska kunna ske. Det är därför viktigt att den personal som tjänstgör i centret får rätt förutsättningar att göra korrekta bedömningar av vilken information som kan delas med de övriga centermyndigheterna. För det krävs både kunskap hos den som ska dela information och att förtroende finns mellan den personal från de olika myndigheterna som ska dela information med varandra. Det är därför viktigt att det finns en kontinuitet i den omfattning det är möjligt beträffande den personal som ska tjänstgöra i NCSC från de olika myndigheterna, se avsnitt 4.2.1.

Utöver kontinuitet i personalgruppen och utökad kunskap om regelverket bör riktlinjer och rutiner utarbetas inom centret för att förenkla informationsdelningen.

Det bör utredas om informationsdelningen i NCSC kan förenklas

Utredningen har övervägt om det går att föreslå en ny bestämmelse som innebär enklare regler för informationsdelning inom centret. I 10 kap. 28 § OSL anges att sekretess inte hindrar att en uppgift lämnas till en annan myndighet om uppgiftsskyldighet följer av lag eller förordning. Det finns exempel på lagstiftning som reglerar uppgiftsskyldighet inom ramen för olika typer av myndighetssamverkan. Inom det myndighetsgemensamma arbetet mot organiserad brottslighet finns exempelvis lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet. Lagen möjliggör för myndigheter inom särskilt beslutad samverkan vid arbetet mot organiserad brottslighet att dela sekretessbelagd information med andra myndigheter om det behövs för att de andra myndigheterna ska kunna delta i samverkan. Vilka myndigheter som ingår i samverkan

[63] Jfr. HFD 2021 not. 58, p. 12–15.

regleras särskilt i en förordning, lagstiftningen är alltså flexibel för att sammansättningen av myndigheter i samarbetet kan förändras över tid.[64]

Utredningen bedömer att en liknande lagstiftning för verksamheten i NCSC väsentligt skulle kunna underlätta informationsdelningen och göra det möjligt för nya myndigheter att delta i centerverksamheten.

Utredningen förordar att förutsättningarna för att införa en sådan ordning utreds. Det måste bland annat utredas hur uppgiftsskyldigheten bör avgränsas och hur det påverkar personuppgiftsbehandlingen inom centrets verksamhet. Även hur uppgiftsskyldigheten ska förhålla sig till att några av centermyndigheterna är tillsynsmyndigheter och brottsbekämpande myndigheter och att informationsdelning till dem kan hämma viljan från privata aktörer att lämna känslig information till cybersäkerhetscentret bör utredas i det sammanhanget, se avsnitt 5.4.1 nedan.

5.4 Extern informationsdelning

5.4.1 Informationsdelning med privata aktörer

Utredningens bedömning: Den information som näringslivet delar med NCSC om incidenter, risker och sårbarheter är i regel skyddad av sekretess. Det saknas dock uttryckligt sekretesskydd för uppgifter om näringslivets affärs- och driftsförhållanden hos samtliga centermyndigheter. Det bör införas sekretesskydd för uppgifter om affärs- och driftsförhållanden som lämnas till NCSC**.**

Centret bör utarbeta tydliga rutiner och riktlinjer för extern informationsdelning.

De privata aktörernas vilja att dela information påverkas i hög grad av möjligheten att få information och stöd tillbaka. Informationsdelningen måste därför vara förtroendebaserad och till ömsesidig nytta. Det är viktigt att information delas med privata aktörer i lämplig omfattning. Information kan därför behöva avidentifieras och anpassas innan den delas med externa parter. Centret bör utarbeta tydliga rutiner och riktlinjer för informationsdelning.[65]

Informationsdelningen mellan NCSC och externa aktörer är beroende av samma sekretessbestämmelser i OSL som den informationsdelning som sker internt. Uppgifter i till exempel ingivna incidentrapporter omfattas i regel av sekretess enligt 18 kap. 8 § OSL. Även de regelverk som styr till exempel säkerhetsskyddsklassificerade uppgifter och personuppgiftsbehandling inverkar också på möjligheterna att dela viss typ av information, såväl internt som externt i centrets verksamhet, se avsnitt 6 och 7.2.1.[66]

[64] Jfr. 2 § lagen om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet samt 2 § förordningen (2016:775) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet.

[65] Jfr. *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning* avsnitt 5.4.3 och RiR 2023:8, s. 45.

[66] Jfr. Kammarrätten i Göteborgs dom den 29 juni 2021 i mål nr 2144-21.

Möjligheten att uppställa förbehåll

Vid den externa informationsdelningen måste beaktas att de uppgifter som lämnas vidare från centermyndigheterna till privata aktörer inte längre är skyddade av sekretess eftersom sekretessen inte överförs mellan myndigheter och privata verksamheter på det sätt som görs mellan myndigheter.

Det går dock att under vissa förutsättningar lämna ut uppgifter med förbehåll enligt 10 kap. 14 § OSL. Med stöd av 10 kap. 14 § OSL har en myndighet möjlighet att lämna ut uppgifter till en enskild som är sekretessbelagda enligt en sekretessbestämmelse som har ett skaderekvisit. Utlämnande kan ske om risken för skada, men eller annan olägenhet som hindrar att uppgifterna lämnas till den enskilde, kan undanröjas genom att ett förbehåll uppställs när uppgifterna lämnas ut. Syftet med bestämmelsen är att möjliggöra att informationsbehov tillgodoses i sådana fall där det är angeläget att informationen kan lämnas ut trots att den omfattas av sekretess.[67]

Ett förbehåll får bara ställas upp om det behövs för att undanröja skaderisken som hindrar ett utlämnande av uppgifter. Innehållet i ett förbehåll måste vara tillräckligt preciserat och ska inte ge alltför mycket tolkningsutrymme för den som förbehåller riktar sig mot. Ett förbehåll innebär att ett formellt beslut om förbehåll måste fattas. Ett avtal eller en utfästelse om att inte lämna vidare uppgifterna är inte tillräckligt. I och med att man lämnar ut uppgifter med förbehåll så följer tystnadsplikt. Om den som förbehållet riktar sig mot inte följer villkoren kan ansvar för brott mot tystnadsplikt enligt 20 kap. 3 § brottsbalken aktualiseras.[68]

Sekretesskydd för incidenter, risker och sårbarheter

Den information som näringslivet delar med centret kopplat till incidenter, risker och sårbarheter kommer i regel att omfattas av sekretess med stöd av 18 kap. 8 § OSL. Sekretessen som följer av den bestämmelsen är inte absolut men bedömningen av skada bör som utgångspunkt innebära att uppgifter som lämnas av privata aktörer om incidenter innebär risk för skada om dessa lämnas ut. Uppgifter om sårbarheter, risker och intrång i tekniska system kan utnyttjas om dessa offentliggörs. Även uppgifter om vilken organisation som drabbats bör kunna omfattas av sekretess eftersom uppgift om vilken organisation som drabbats kan lämna upplysningar om säkerhetsarbetet och eventuella brister i detta. Sekretessbestämmelsen för uppgift om inträffade incidenter bör därmed vara tillräcklig för att tillgodose näringslivet behov av skydd för uppgifterna i det avseendet.[69]

Sekretesskydd för uppgift om affärs- driftsförhållanden

Utöver det kan behov av sekretesskydd uppstå för uppgift om affärs- och driftsförhållanden hos en verksamhetsutövare. Sådant sekretesskydd finns till exempel i MSB:s verksamhet. Samtliga centermyndigheter saknar dock möjlighet att tillämpa sekretesskydd för affärs- och driftsförhållanden hos näringslivsaktörer som lämnar uppgifter till

[67] Prop. 1979/80:2 del A, s. 349.
[68] JO 1994/95, s. 574 och JO 1984/85, s. 274.
[69] Se till exempel Kammarrätten i Göteborgs domar den 31 januari 2017 i mål nr 5032-16 och den 29 juni 2021 i mål nr 2144-21.

myndigheterna. I 30 kap. 23 § OSL och 9 § offentlighets- och sekretessförordningen (2009:641), OSF, finns reglering av sekretess kring bland annat affärs- och driftsförhållanden om det kan antas att den enskilde lider skada om uppgiften röjs. Av bestämmelsen följer också att sekretess gäller för uppgift om andra personliga eller ekonomiska förhållanden för den som trätt i affärsförbindelse eller liknande med den som är föremål för myndighetens verksamhet.

Att det finns sekretesskydd för affärs- och driftsförhållanden kan ha betydelse för viljan att dela information med centret och centermyndigheterna. För att informationsutbytet ska bli så omfattande som möjligt måste det därför säkerställas att den information som lämnas av näringslivet till centret inte innebär en risk för skada för den verksamhet som uppgiften rör. En bestämmelse om sekretess till skydd för affärs- och driftsförhållanden hos de privata aktörer som lämnar information till cybersäkerhetscentret bör därför införas. En möjlighet är att i bilagan till OSF ange att sekretessen i 30 kap. 23 § OSL och 9 § OSF också ska omfatta centrets verksamhet.

5.4.2 Informationsdelning med andra offentligrättsliga aktörer

Informationsdelningen med offentligrättsliga aktörer, till exempel andra statliga myndigheter, kommuner och regioner, innebär inte lika stora utmaningar ur sekretessynpunkt. Om sekretessbelagd information från NCSC delas med andra myndigheter gäller sekretessen fortfarande i den mottagande myndighetens verksamhet så länge det är primära sekretessbestämmelser som gäller i alla myndigheter som tillämpas. Som redogjorts för ovan är både 15 kap. 2 § OSL och 18 kap. 8 § OSL sekretessbestämmelser som gäller i alla myndigheter. Informationsdelning med offentliga aktörer borde därför innebära en enklare sekretessavvägning än vad som behöver göras i förhållande till privata aktörer.[70]

5.5 Slutsatser om extern informationsdelning

Informationsdelningen i förhållande till näringslivet kompliceras av att information som lämnas till näringslivet inte längre är skyddad av sekretess om inte förbehåll uppställs i samband med utlämnandet av uppgifter. Det är dock möjligt att lämna uppgifter med förbehåll för att undvika att känsliga uppgifter inte längre skulle omfattas av sekretess.

Andra begränsningar kan följa av bland annat regleringar kring personuppgiftsbehandling och säkerhetsskyddsklassificerade uppgifter.

Med anpassning av innehåll och avidentifiering information kan viss information delas med näringslivet. Med det krävs att rutiner och riktlinjer utarbetas för hur informationsdelningen ska ske för att säkerställa kontinuitet och förtroende mellan NCSC och externa aktörer. Målet är att informationsutbytet ska vara ömsesidigt – utöver legala förutsättningar

[70] Heuman, *Tryckfrihetsförordningen*, 2 kap. 4 § 2023-08-01, (Lexino).

krävs därför också att förtroende byggs upp i de samarbetsforum som NCSC medverkar i. Precis som i den interna informationsdelningen förutsätter en välfungerande extern informationsdelning både legala förutsättningar och förtroende parterna emellan.

Incidentrapporter samt uppgifter om sårbarheter och risker bör i regel omfattas av sekretess enligt 18 kap. 8 § OSL. Sådan information skyddas således redan med nuvarande reglering. Däremot saknas reglering till skydd för näringslivets affärs- och driftsförhållanden. Utredningen anser att sådan reglering bör införas för att säkerställa en effektiv och förtroendefull informationsdelningen mellan NCSC och näringslivet.

Vad gäller informationsdelning med offentliga aktörer omfattas de av OSL. Det innebär att de primära sekretessbestämmelser som tillämpas av NCSC även tillämpas av dem, vilket precis som vid den interna informationsdelningen underlättar den sekretessprövning som ska göras vid ett utlämnande. Informationen kommer fortsatt vara skyddad hos den mottagande parten så länge den omfattas av bestämmelserna i OSL.

6 Personuppgiftsbehandling

6.1 Utgångspunkter

NCSC blir med utredningens förslag en del av Försvarets radioanstalt. Eftersom centrets verksamhet fortfarande bygger på samarbete mellan de sju centermyndigheterna måste det finnas förutsättningar för att personuppgiftsbehandlingen sker på ett korrekt sätt.[71]

Det finns andra myndighetsöverskridande samarbeten, exempelvis NCT, där förutsättningarna för personuppgiftsbehandling liknar de som kommer råda för NCSC. Inom NCT utbyts information mellan myndigheterna och man arbetar också gemensamt med att ta fram rapporter. Handläggarna i NCT arbetar på samma arbetsplats hos Säkerhetspolisen och har tillgång till sina egna myndigheters it-system men delar också tillgång till vissa gemensamma mappar så det är möjligt att sammanställa information och arbeta med utkast till rapporter.[72]

Den för centermyndigheterna relevanta regleringen av personuppgiftsbehandling finns i olika registerförfattningar, brottsdatalagen (2018:1177), BDL, och GDPR[73]. I nuläget arbetar NCSC med överenskommelser om behandlingen av personuppgifter inom centret. Överenskommelserna avser de fyra myndigheterna (Försvarets radioanstalt, Försvarsmakten, MSB och Säkerhetspolisen) som har fått regeringsuppdraget att bedriva fördjupad samverkan inom NCSC.

Att Försvarets radioanstalt får ett huvudansvar för verksamheten och att NCSC blir en del av myndigheten medför att personuppgiftsbehandlingen kommer att följa av den reglering som styr Försvarets radioanstalts personuppgiftsbehandling i störst utsträckning. Försvarets radioanstalt kommer därmed i hög grad bestämma ändamål och medel för personuppgiftsbehandlingen.

6.2 Tillåten behandling av personuppgifter

För att centermyndigheterna ska kunna utbyta information inom NCSC krävs att aktuella registerförfattningar och GDPR ger stöd för det utbytet. Ett utlämnande av personuppgifter innebär att det sker en behandling av personuppgifter. Möjligheten att lämna ut personuppgifter följer av de ändamålsbestämmelser som styr myndigheternas personuppgiftsbehandling, se mer om dessa i avsnitten nedan.

[71] Se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 5.2 och 5.3.
[72] Prop. 2017/18:36, s. 13.
[73] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Samtliga myndigheters personuppgiftsbehandling står under tillsyn. Tillsynsmyndighet är i huvudsak Integritetsskyddsmyndigheten.[74]

6.2.1 Försvarets radioanstalt

Försvarets radioanstalt ska enligt sin instruktion samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet. [75]

När Försvarets radioanstalt är personuppgiftsansvarig sker behandlingen med stöd av lagen (2021:1172) om personuppgiftsbehandling vid Försvarets radioanstalt (FRA-PuL). Den gäller när det är Försvarets radioanstalt som behandlar personuppgifter men inte när behandlingen sker för någon annans räkning. FRA-PuL gäller behandling både i försvarsunderrättelseverksamheten, utvecklingsverksamheten och informationssäkerhetsverksamheten.[76]

Av 2 kap. 1 § FRA-PuL framgår att personuppgifter bara får behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Det anges också att personuppgifter inte får behandlas för något ändamål som är oförenligt med det ändamål som de ursprungligen behandlades för. Detta är ett uttryck för finalitetsprincipen.

Verksamheten i NCSC avser främst informationssäkerhetsområdet. För informationssäkerhetsverksamheten anges två ändamål för behandling, dels om det är nödvändigt för att kunna skydda den egna myndigheten, dels för att kunna stödja andra verksamheter som är av betydelse för Sveriges säkerhet. Uppgiften att lämna stöd till andra verksamheter ska följa av lag eller förordning eller beslut av regeringen i ett enskilt fall. Uppgifter får dock också behandlas för att tillhandahålla information som behövs med anledning av samverkan med andra som verkar på informationssäkerhetsområdet såväl inom som utom landet i den utsträckning det följer av lag eller förordning eller om regeringen har beslutat om det i ett enskilt fall.[77]

Försvarets radioanstalt får också behandla personuppgifter för sekundära ändamål. Uppgifter från försvarsunderrättelseverksamheten kan behandlas i syfte att tillhandahålla information som behövs i informationssäkerhetsverksamheten. Omvänt kan också behandling av personuppgifter från informationssäkerhetsverksamheten behandlas i försvarsunderrättelseverksamheten när det gäller allvarliga yttre hot mot samhällets infrastrukturer eller främmande underrättelseverksamhet mot svenska intressen.[78]

[74] Vissa myndigheters personuppgiftsbehandling står dock under ytterligare tillsyn. Statens inspektion för försvarsunderrättelseverksamheten (SIUN) granskar Försvarets radioanstalts och Försvarsmaktens behandling av personuppgifter inom ramen för försvarsunderrättelseverksamheten. Säkerhets- och integritetsskyddsnämnden utövar tillsyn över Polismyndighetens och Säkerhetspolisens personuppgiftsbehandling.
[75] 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt.
[76] Prop. 202/21:224, s. 60–61.
[77] 2 kap. 7–8 §§ FRA-PuL.
[78] 2 kap. 4 och 8 §§ FRA-PuL samt 1 § andra stycket p. 5 och 7 lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.

Försvarets radioanstalts möjligheter att medge direktåtkomst[79] skiljer sig mellan de olika verksamhetsgrenarna. Försvarsmakten och Säkerhetspolisen får medges direktåtkomst till vissa personuppgifter inom försvarsunderrättelseverksamheten. Utländsk underrättelse- eller säkerhetstjänst får också medges direktåtkomst till vissa personuppgifter i försvarsunderrättelseverksamheten om det behövs för samarbetet mot terrorism eller för annat internationellt säkerhetssamarbete. För informationssäkerhetsverksamheten kan direktåtkomst medges en utländsk organisation inom informationssäkerhetsområdet om det behövs samarbetet mot it-relaterade hot mot samhällsviktiga system. Regeringen får vidare meddela föreskrifter om direktåtkomst till uppgiftssamlingar i andra fall. I förordningen (2021:1208) om behandling av personuppgifter vid Försvarets radioanstalt (FRA-PuF) anges fler sammanhang då direktåtkomst medges.[80]

Av FRA-PuF följer att i underrättelseverksamheten får Regeringskansliet, Säkerhetspolisen, Nationella operativa avdelningen i Polismyndigheten, MSB, Inspektionen för strategiska produkter, Försvarsmakten, Försvarets materielverk, Totalförsvarets forskningsinstitut och Tullverket medges direktåtkomst till personuppgifter som utgör underrättelser och som finns i uppgiftssamlingar.[81]

Försvarsmakten och Säkerhetspolisen får vidare medges direktåtkomst till personuppgifter som utgör analysresultat och som behandlas i en uppgiftssamling för informationssäkerhetsverksamhet.[82]

Försvarets radioanstalt får lämna ut personuppgifter elektroniskt på annat sätt än genom direktåtkomst om regeringen har meddelat föreskrifter eller fattat beslut om det i ett enskilt fall. Av FRA-PuF följer att Försvarets radioanstalt får lämna ut personuppgifter elektroniskt till andra statliga myndigheter på annat sätt än genom direktåtkomst.[83]

Därmed finns med nu gällande bestämmelser möjlighet för Försvarets radioanstalt att lämna uppgifter till andra statliga myndigheter. Det saknas dock motsvarande möjlighet att lämna ut personuppgifter elektroniskt till kommuner, regioner och privata aktörer.

6.2.2 Försvarsmakten

Försvarsmaktens personuppgiftsbehandling styrs av lagen (2021:1171) om behandling av personuppgifter vid Försvarsmakten (FM-PuL). Av 2 kap. 1 § FM-PuL framgår att personuppgifter bara får behandlas för särskilda, uttryckligt angivna och berättigade ändamål. Den rättsliga grunden för personuppgiftsbehandling vid Försvarsmaktens deltagande i NCSC är 2 kap. 2 § i FM-PuL. Där framgår att Försvarsmakten får behandla personuppgifter om det är nödvändigt för att planera, förbereda och genomföra verksamhet som rör Sveriges försvar och säkerhet, eller internationellt försvars- och säkerhetssamarbete. Försvarsmaktens uppgift

[79] Med direktåtkomst avses att någon har tillgång till någon annans register eller databas och har möjlighet att söka i den men inte påverka innehållet.
[80] 3 kap. 2–6 §§ FRA-PuL.
[81] 3 kap. 10 § FRA-PuF.
[82] 3 kap. 11 § FRA-PuF.
[83] 2 kap. 2 § FRA-PuF.

att bedriva sådan verksamhet som anges i första stycket ska följa av lag, förordning, kollektivavtal eller annat avtal, eller ett särskilt beslut där regeringen har gett myndigheten i uppdrag att utföra uppgiften.

Av 3 kap. 8 § förordningen (2021:1207) om behandling av personuppgifter vid Försvarsmakten (FM-PuF) framgår att Nationella operativa avdelningen i Polismyndigheten, Säkerhetspolisen, MSB, Försvarets materielverk, Försvarets radioanstalt och Post- och telestyrelsen får medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 2 § FM-PuL. Direktåtkomsten får endast avse personuppgifter som behandlas inom ramen för Försvarsmaktens deltagande i Nationellt cybersäkerhetscenter och som har gjorts gemensamt tillgängliga inom Försvarsmakten. Vid sådan direktåtkomst har myndigheterna rätt att ta del av de personuppgifter som omfattas av åtkomsten.

6.2.3 Säkerhetspolisen

Säkerhetspolisens personuppgiftsbehandling i den brottsbekämpande verksamheten styrs av BDL och lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område.[84]

Vid behandling av personuppgifter som rör nationell säkerhet tillämpas lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Av 2 kap. 1 § punkterna 1 och 4 framgår att personuppgifter bland annat får behandlas om det är nödvändigt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot Sveriges säkerhet, terrorbrott, eller tryckfrihetsbrott och yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv eller fullgöra någon annan uppgift som rör nationell säkerhet och som anges i lag eller förordning eller särskilt beslut av regeringen. När Säkerhetspolisen behandlar personuppgifter som inte rör nationell säkerhet i syfte att bekämpa och lagföra brott ska myndigheten tillämpa BDL och lagen om polisens behandling av personuppgifter inom brottsdatalagens område.

Av 2 kap. 19 § lagen om Säkerhetspolisens behandling av personuppgifter följer att personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.[85]

6.2.4 Polismyndigheten

Polismyndighetens personuppgiftsbehandling i den brottsbekämpande verksamheten styrs av BDL och lagen om polisens behandling av personuppgifter inom brottsdatalagens område. Av 2 kap. 1 § BDL följer att personuppgifter får behandlas om det är nödvändigt för att Polismyndigheten ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet.

[84] En utredning har tillsatts avseende Säkerhetspolisens informationshantering. Inom ramen för den utredningen ska myndighetens personuppgiftsbehandling ses över, se dir. 2023:64.
[85] Av 3 kap. 5 och 6 §§ lagen om Säkerhetspolisens behandling av personuppgifter följer att Polismyndigheten, Försvarsmakten och Försvarets radioanstalt kan få del av uppgifter med direktåtkomst.

Med uppgift avses en uppgift som framgår av lag, förordning eller ett särskilt beslut i vilket regeringen uppdragit åt myndigheten att utföra uppgiften.

Av 1 kap. 1 § punkten 1 lagen om polisens behandling av personuppgifter på brottsdatalagens område följer att lagen gäller för Polismyndigheten utöver BDL om uppgifterna behandlas i syfte att bland annat förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller upprätthålla allmän ordning och säkerhet.

Av 2 kap. 1 § i lagen om polisens behandling av personuppgifter inom brottsdatalagens område följer att personuppgifter får behandlas om det är nödvändigt för att Polismyndigheten bland annat ska kunna förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, upprätthålla allmän ordning och säkerhet eller fullgöra förpliktelser som följer av internationella åtaganden.

Personuppgifter får enligt 2 kap. 12 § i lagen om polisens behandling av personuppgifter inom brottsdatalagens område lämnas ut på annat sätt än genom direktåtkomst om det inte är olämpligt. För bland annat Säkerhetspolisen finns det möjlighet att medges direktåtkomst.[86]

6.2.5 Försvarets materielverk, MSB samt Post- och telestyrelsen

Försvarets materielverk, MSB samt Post- och telestyrelsen behandlar personuppgifter med stöd av GDPR. Behandlingen sker med stöd av artikel 6.1. punkterna b) och e). Av artikel 6.1. framgår att behandlingen är laglig endast om den sker med någon av de villkor som framgår av punkterna som räknas upp i artikeln.[87]

I punkten b) anges att behandlingen är tillåten om den är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

I punkten e) anges att behandlingen är laglig när den är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Som utredningen redan kommit fram till kommer NCSC i regel inte fatta förvaltningsrättsliga beslut och inte heller utföra någon form av myndighetsutövning. Arbete inom NCSC är däremot en uppgift av allmänt intresse i GDPR:s mening eftersom uppgifter som lämnats åt myndigheter att utföra är av allmänt intresse.[88]

6.2.6 Personaladministrativ verksamhet

I den personaladministrativa verksamheten tillämpar samtliga myndigheter utom Försvarsmakten artikel 6.1 punkten b) i GDPR. I

[86] Direktåtkomst för bland annat Säkerhetspolisen är tillåten i den utsträckning som följer av 3 kap. 7 §, 5 kap. 10 § och 5 kap. 17 § lagen om polisens behandling av personuppgifter inom brottsdatalagens område.
[87] Jfr. även 2 kap. 1 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.
[88] Jfr. Prop. 2017/18:105, s. 56–57 och se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 5.2.2.

punkten b) anges att behandlingen är tillåten om den är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås. Uppgifter som behandlas för detta ändamål är exempelvis namn och kontaktuppgifter.[89]

6.2.7 Tekniska system

Inom NCSC kommer arbetet behöva bedrivas både med gemensam hantering i it-system dit alla myndigheter har tillgång och genom att de anställda har tillgång till den egna myndighetens system när de arbetar i centrets verksamhet.

Även om det huvudsakligen blir Försvarets radioanstalt som bestämmer ändamål och medel för behandlingen, kommer det finnas tillfällen då behandlingen av personuppgifter i centrets verksamhet kommer följa av någon av de andra centermyndigheternas uppdrag och specifika registerförfattningar. Denna centermyndighet blir då personuppgifts-ansvarig. Så kan bli fallet om en myndighets personal i centret hanterar information i den egna myndighetens it-system och detta system inte är tillgängligt för de andra centermyndigheterna.[90]

Även inom ramen för it-systemet med gemensam tillgång kommer troligtvis viss behandling enbart vara hänförlig till en specifik myndighet. Om det i systemet går att avskilja delar av systemet som enbart är tillgängligt för en viss centermyndighet och dess personal kommer personuppgiftsbehandlingen som vidtas där ske genom att personalen är företrädare för myndigheten där de är anställda. Då styrs behandlingen av myndighetens egen registerförfattning och myndigheten är därmed ansvarig för personuppgiftsbehandlingen.[91]

Det tekniska systemet kommer dock att tillhöra Försvarets radioanstalt som också av administrativa och tekniska skäl kan komma att behandla personuppgifter som finns i systemet och egentligen enbart är tillgängliga för en annan centermyndighet. Det kan därför finnas behov av att teckna personuppgiftsbiträdesöverenskommelser för den hanteringen.[92]

Ett gemensamt personuppgiftsansvar skulle teoretiskt kunna bli aktuellt om det inte går att urskilja vilken myndighet som har utfört en specifik behandling i en produkt som är gemensam mellan flera olika centermyndigheter och det heller inte på annat sätt går att urskilja någon tydlig fördelning av ansvaret. Det är dock i så fall avgörande att myndigheterna gemensamt bestämmer ändamål med och medlen för behandling. Eftersom ändamål och medel för behandlingen inom ramen för NCSC i stor utsträckning bör bestämmas av Försvarets radioanstalt eller annars av en specifik myndighet till exempel inom ramen för dess interna tekniska system bör det vara i mycket få situationer ett gemensamt personuppgiftsansvar kan uppstå. Även när myndigheter samarbetar med varandra som inom NCSC och gör ett gemensamt arbete framgår det ofta av de faktiska omständigheterna vilken myndighet som är ansvarig för

[89] Försvarsmaktens behandling av personuppgifter i personaladministrativ verksamhet sker med stöd av 2 kap. 2 § första stycket p. 1 FM-PuL.
[90] Jfr. Ds 2016:31, s. 109–110.
[91] Jfr. Ds 2016:31, s. 110–111.
[92] Jfr. Ds 2016:31, s. 110–111.

vilken behandling, till exempel beroende på vilken myndighet som har tillgång till ett specifikt system eller att myndigheten har en viss roll i en del av en process.[93]

6.3 Slutsatser om personuppgiftsbehandling

Utredningens bedömning: Det behöver inte införas något nytt författningsstöd för centermyndigheternas behandling av personuppgifter inom NCSC. Försvarets radioanstalt bör få utökade möjligheter att dela personuppgifter elektroniskt på annat sätt än genom direktåtkomst. Det kan också komma att finnas behov av utökad direktåtkomst för centermyndigheterna.

Det behövs inget nytt författningsstöd för personuppgiftsbehandling

Centermyndigheterna deltar i verksamheten i NCSC inom ramen för sina verksamhetsområden. Medverkan i centrets verksamhet innebär alltså inte att det tillkommer någon ny grund för behandling av personuppgifter utan de grunder som framgår av GDPR och aktuella registerlagstiftningar täcker även de uppgifter som myndigheterna utför i centret.

Behandlingen av personuppgifter kommer förenklas av att NCSC blir en del av Försvarets radioanstalt. Försvarets radioanstalt kommer bli personuppgiftsansvarig för större delen av den behandling som sker inom centret. FRA-PuL och FRA-PuF kommer tillämpas i större utsträckning eftersom det i regel kommer vara Försvarets radioanstalt som bestämmer ändamål och medel för behandlingen av personuppgifter inom NCSC.

Utredningen bedömer att personuppgiftsbehandlingen i centrets verksamhet inte kräver några lagändringar. I vissa delar kommer andra myndigheter bestämma över behandlingen om det är uppgifter som till exempel behandlas i deras interna tekniska system. Ett behov av överenskommelser om behandling kan då uppstå beroende på verksamhetens organisation, vilket inte bör vara problematiskt eftersom centret redan i nuläget arbetar med sådana överenskommelser.

Försvarets radioanstalt bör få utökade möjlighet att dela personuppgifter elektroniskt

Det finns dock åtgärder som bör genomföras för att förenkla förutsättningarna för verksamheten i centret. Möjligheten för Försvarets radioanstalt att dela personuppgifter elektroniskt till fler än statliga myndigheter hade underlättat centrets arbete. I nuläget kan Försvarets radioanstalt inte elektroniskt dela personuppgifter med till exempel kommuner och regioner och inte heller med privata aktörer. Begränsningar i detta avseende kan påverka centret effektivitet och möjligheter att dela information. Möjligheterna för Försvarets radioanstalt att dela personuppgifter elektroniskt på annat sätt än genom direktåtkomst kan utökas genom en ändring av 2 kap. 2 § FRA-PuF.

[93] Jfr. Prop. 2017/18:36, s. 17–19.

Det kan finnas ett behov av utökad direktåtkomst

Utökade möjligheter till direktåtkomst hos Försvarets radioanstalt skulle också kunna vara en möjlighet för ökad effektivitet i centrets verksamhet. Det finns i nuläget vissa möjligheter att medge direktåtkomst för centermyndigheterna. Den största möjligheten finns inom Försvarsmakten där det i 3 kap. 8 § FM-PuF framgår att samtliga centermyndigheter kan medges direktåtkomst till personuppgifter som behandlas med stöd av 2 kap. 2 § FM-PuL.

Försvarets radioanstalts möjligheter att medge direktåtkomst är mer begränsade och avser för informationssäkerhetsverksamheten endast Försvarsmakten och Säkerhetspolisen. Att det saknas möjlighet för Försvarets radioanstalt att medge direktåtkomst till samtliga centermyndigheter kan påverka effektiviteten i NCSC:s arbete. Det beror dock på hur det gemensamma arbetet kommer att fungera i praktiken. Det är därmed svårt att dra slutsatser kring om behovet av delning av personuppgifter mellan centermyndigheterna redan tillgodoses av möjligheten att lämna ut uppgifter elektroniskt på annat sätt än genom direktåtkomst.

Att medge fler myndigheter direktåtkomst till Försvarets radioanstalts uppgiftssamlingar innebär dessutom att avvägningar måste göras kring skyddet för den personliga integriteten. Det krävs också säkerhetsskyddsmässiga överväganden med hänsyn till den säkerhetskänsliga verksamhet som Försvarets radioanstalt bedriver.

7 Säkerhetsskydd

7.1 Övergripande ansvar m.m.

Utredningens bedömning: Försvarets radioanstalt är verksamhetsutövare för centrets verksamhet och har det övergripande ansvaret för säkerhetsskyddet.

Försvarets radioanstalts säkerhetskyddschef blir säkerhetsskyddschef även för centrets verksamhet.

Att centret blir en del av Försvarets radioanstalt medför att ansvaret för säkerhetsskyddet i centret bli tydligare.

Av 2 kap. 1 § säkerhetsskyddslagen (2018:585) följer att den som till någon del bedriver säkerhetskänslig verksamhet och därmed är verksamhetsutövare ska utreda behovet av säkerhetsskydd. Denna utredning kallas för säkerhetsskyddsanalys. Det yttersta ansvaret för säkerhetsskyddet åvilar den som är chef för verksamhetsutövaren.[94] Eftersom centret föreslås bli en del av Försvarets radioanstalt är i huvudsak Försvarets radioanstalt att bedöma som verksamhetsutövare för centret och är i och med det skyldig att utreda behovet av säkerhetsskydd. Det yttersta ansvaret för säkerhetsskyddet för NCSC kommer generaldirektören för Försvarets radioanstalt att ha.

Med säkerhetsskyddsanalysen som utgångspunkt ska verksamhetsutövaren, planera och vidta säkerhetsskyddsåtgärder. Med säkerhetsskyddsåtgärder avses åtgärder som syftar till informationssäkerhet, fysisk säkerhet och personalsäkerhet, se mer om detta nedan i avsnitt 7.2.1–7.2.3. De olika säkerhetsskyddsåtgärderna måste samverka med varandra för att ge ett heltäckande säkerhetsskydd.[95]

Då säkerhetsanalysen ska göras så nära verksamheten som möjligt kommer Försvarets radioanstalt att behöva göra en särskild säkerhetsanalys avseende centrets verksamhet. Därutöver ska verksamhetsutövaren kontrollera säkerhetsskyddet i verksamheten samt anmäla och rapportera sådant som är av vikt för säkerhetsskyddet och i övrigt vidta de åtgärder som krävs enligt säkerhetsskyddslagen.[96]

Säkerhetsskyddschef

Det kommer behövas en säkerhetsskyddschef med ansvar för centrets verksamhet i enlighet med 2 kap. 7 § säkerhetsskyddslagen. Säkerhets-

[94] Waern, Degerfeldt, Leeman, *Säkerhetsskyddslagen*, (2022-11-01, JUNO), kommentaren till 2 kap. 1 §.
[95] SOU 2021:63, *Sveriges säkerhet – behov av starkare skydd för närverks- och informationssystem*, s. 84–85 och 130.
[96] Se 2 kap. 1 § andra stycket säkerhetsskyddsförordningen (2021:955) för närmare krav på säkerhetsskyddsanalys, 2 kap. 2–9 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1) som är relevant för myndigheter under Säkerhetspolisens tillsyn samt 2 kap. 1–5 §§ Försvarsmaktens föreskrifter om säkerhetsskydd (FFS 2019:2).

skyddschefen ska leda och samordna säkerhetsskyddsarbetet samt kontrollera att verksamheten bedrivs i enlighet med lagen och de föreskrifter som meddelats i anslutning till lagen. Detta ansvar kan inte delegeras. Säkerhetsskyddschefen ska vara direkt underställd chefen för verksamhetsutövarens verksamhet, om en sådan chef finns, och annars verksamhetsutövarens ledning. I en statlig myndighet är myndighetschefen att anse som chefen för verksamhetsutövarens verksamhet.[97]

Denna chef ska vara navet i verksamhetens säkerhetsorganisation och ha mycket god kännedom om hot mot verksamheten, sårbarheter och konsekvenser av att sårbarheter utnyttjas. Säkerhetsskyddschefen behöver därför både stå ledningen och den säkerhetskänsliga verksamheten nära.[98]

Eftersom centret föreslås bli en del av Försvarets radioanstalt kommer Försvarets radioanstalts säkerhetsskyddschef även bli säkerhetsskyddschef för centrets verksamhet. Att så är fallet är en förutsättning för att Försvarets radioanstalt ska kunna få en övergripande bild av behovet av säkerhetsskydd inom NCSC. Detta innebär att Försvarets radioanstalts säkerhetsskyddschef kommer att få ett utökat ansvar och behöver nära följa centrets verksamhet. Som redan anförts finns det inte någon möjlighet för säkerhetsskyddschefen att delegera sitt ansvar men att ansvaret inte kan delegeras utgör inte hinder mot att arbetsuppgifter delegeras till andra medarbetare. En sådan delegation påverkar dock inte säkerhetsskyddschefens ansvar.[99]

Säkerhetsskyddsavtal

En grundläggande princip inom säkerhetsskyddet är att säkerhetskänslig verksamhet ska ha samma skydd oavsett var och hur den bedrivs. Med detta följer i enlighet med 4 kap. 1 § säkerhetsskyddslagen att en verksamhetsutövare som avser att genomföra en upphandling, ingå ett avtal eller inleda en samverkan eller samarbete med en annan aktör i vissa fall ska ingå ett säkerhetsskyddsavtal med aktören. Detta avtal ska ingås innan motparten engageras i verksamheten. Säkerhetsskyddsavtal är av grundläggande betydelse för möjligheten att anlita konsulter och leverantörer och även i övrigt bedriva samverkan och samarbete med externa aktörer i säkerhetskänslig verksamhet. Om en verksamhetsutövare i stället avser att anställa eller ta emot tidvis tjänstgörande personer i verksamheten ska reglerna om personalsäkerhet tillämpas.[100]

Säkerhetsskyddsanalysen bör leda fram till en förståelse av vilka delar av organisationen som är skyddsvärda och där det krävs säkerhetsskyddsavtal. Säkerhetsskyddsanalysen kan exempelvis ha visat att ett visst informationssystem innehåller säkerhetsskyddsklassificerade uppgifter och därför måste skyddas med särskilda informationssäkerhetsåtgärder.[101]

Enligt 4 kap. 2 § säkerhetsskyddslagen gäller kravet på säkerhetsskyddsavtal mellan myndigheter endast vid anskaffning av en vara, tjänst

[97] Prop. 2020/21:194, *Ett starkare skydd för Sveriges säkerhet,* s. 25 och 127.
[98] Waern, Degerfeldt, Leeman, *Säkerhetsskyddslagen*, (1 november 2022, JUNO), kommentaren till 2 kap. 7 §.
[99] Prop. 2020/21:194, s. 26.
[100] Waern, Degerfeldt, Leeman, *Säkerhetsskyddslagen*, (1 november 2022, JUNO), kommentaren till 4 kap. 1 §.
[101] Waern, Degerfeldt, Leeman, *Säkerhetsskyddslagen*, (1 november 2022, JUNO), kommentaren till 4 kap. 1 §.

eller byggentreprenad. Det finns därmed inte något lagkrav på att det ska finnas någon säkerhetsskyddsöverenskommelse mellan centermyndigheterna i andra situationer. Inte heller borde en sådan överenskommelse bli aktuell vid inlån av personal.[102]

Anledningen till detta är att statliga myndigheter ingår i den juridiska personen staten. Ett ytterligare skäl är att båda parter omfattas av regleringen i OSL och de säkerhetsskyddsklassificerade uppgifter som kan behöva delas mellan myndigheter inom ramen för ett samarbete eller samverkan normalt är sådana att de omfattas av sekretess som gäller oavsett i vilken verksamhet de förekommer. Frånvaro av krav på säkerhetsskyddsavtal innebär inte att en myndighet som verksamhetsutövare kan bortse från säkerhetsskyddet under ett visst förfarande, utan detta får då tillgodoses på andra sätt. Bland annat kan det finnas anledning att ingå någon annan form av säkerhetsskyddsöverenskommelse.[103]

Tillsyn

Försvarsmakten, Säkerhetspolisen och andra tillsynsmyndigheter ansvarar för tillsyn och kontroll av säkerhetsskyddet för de verksamhetsutövare som ska tillämpa säkerhetsskyddslagen. Försvarsmakten utövar bland annat tillsyn över sin verksamhet och de myndigheter som ligger under försvarsdepartementet. Säkerhetspolisen ansvarar för tillsyn över bland annat övriga myndigheter samt regioner och kommuner.[104]

Eftersom Försvarsmakten är tillsynsmyndighet över Försvarets radioanstalt kommer Försvarsmakten huvudsakligen även utöva tillsyn över centrets verksamhet. Det finns dock delar vad gäller säkerhetsskyddet som andra centermyndigheter är ansvariga för och tillsynen för dessa är beroende på vilken centermyndighet som är ansvarig, se till exempel avsnitt 7.2.1 nedan om informationssäkerhet. Det är vidare så att myndigheterna ska tillämpa olika föreskrifter beroende på om de tillhör Säkerhetspolisens eller Försvarsmaktens tillsynsområde.

7.2 Säkerhetsskyddsåtgärder

7.2.1 Informationssäkerhet

Vad gäller informationssäkerheten framgår det av 2 kap. 2 § säkerhetsskyddslagen att informationssäkerhet ska förebygga att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs, och förebygga skadlig inverkan i övrigt på uppgifter och informationssystem som gäller säkerhetskänslig verksamhet. Säkerhetsklassificerade uppgifter avser, enligt 1 kap. 2 § säkerhetsskyddslagen, uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av

[102] Jfr. Ds 2022:26, s. 90–91.
[103] Waern, Degerfeldt, Leeman, *Säkerhetsskyddslagen*, (1 november 2022, JUNO), kommentaren till 4 kap. 2 § och prop. 2020/21:194, s. 36.
[104] 8 kap. 1 § säkerhetsskyddsförordningen, SOU 2021:63 s. 143 och https://www.forsvarsmakten.se/sv/om-forsvarsmakten/vart-arbetssatt/intern-tillsyn-och-kontroll/, senast hämtad 2024-06-13.

sekretess enligt OSL eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.

I centrets verksamhet kan det komma att finnas uppgifter som är säkerhetsskyddsklassificerade. Det kommer därför ställas höga krav på centrets hantering av uppgifter både internt mellan centermyndigheterna och avseende vad som delas till andra aktörer, såsom till andra myndigheter och näringslivet. Det följer av 3 kap. 5 § säkerhetsskyddsförordningen att innan säkerhetsskyddsklassificerade uppgifter som behandlas i ett informationssystem utanför verksamhetsutövarens kontroll ska denne försäkra sig om att säkerhetsskyddet för uppgifterna i systemet är tillräckligt. Vidare framgår att om uppgifter ska kommuniceras till ett informationssystem utanför verksamhetsutövarens kontroll, ska uppgifterna skyddas med hjälp av kryptografiska funktioner som har godkänts av Försvarsmakten.

Informationssäkerhet måste även beaktas innan information lämnas till centret. Deltagande myndigheter måste avgöra om information kan delas och i vilken utsträckning, se vidare om informationsdelning i avsnitt 5.

Centermyndigheterna kommer troligen att använda sig av egna informationssystem[105] inom ramen för arbetet i centret. Innehållet i dessa system måste respektive myndighet själv vara ansvarig för medan säkerhetsskyddet kopplat till driften kommer ligga på Försvarets radioanstalt som ansvarig för den fysiska säkerheten. Om hemliga uppgifter hanteras i systemen ankommer det på den myndigheten som äger systemet att avgöra om Försvarets radioanstalts säkerhetsskyddsåtgärder tillgodoser den egna myndighetens krav.

7.2.2 Fysisk säkerhet

Med fysisk säkerhet avses enligt 2 kap. 3 § säkerhetsskyddslagen att förebygga att obehöriga får tillträde till områden, byggnader och andra anläggningar eller objekt där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller där säkerhetskänslig verksamhet i övrigt bedrivs och förebygga skadlig inverkan på sådana områden, byggnader, anläggningar eller objekt.

Försvarets radioanstalt kommer att ha ansvar för bland annat lokaler för centrets verksamhet och blir därmed ansvarig för den fysiska säkerheten. Det är även så att Försvarets radioanstalt är säkerhetsskyddsansvarig för den fysiska säkerheten under tiden som verksamheten bedrivs i MSB:s lokaler. För att Försvarets radioanstalt ska kunna utöva detta ansvar krävs det ett nära samarbete mellan Försvarets radioanstalt och MSB.[106]

7.2.3 Personalsäkerhet

Av 2 kap. 4 § säkerhetsskyddslagen framgår att personalsäkerhet ska förebygga att personer som inte är pålitliga från säkerhetsskyddspunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskydds-

[105] Informationssystem definieras i 1 kap. 3 § tredje stycket säkerhetsskyddsförordningen som ”ett system av sammansatt mjuk- och hårdvara som behandlar information".
[106] Se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 5.2.

klassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig och säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd. Personalsäkerheten består alltså av två delar, säkerhetsprövning och utbildning. Den som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas. Detta framgår av 3 kap. 1 § säkerhetsskyddslagen. Denna prövning ska enligt 3 kap. 3 § samma lag, göras innan deltagandet i den säkerhetskänsliga verksamheten. Säkerhetsprövningen får göras mindre omfattande om det finns särskilda skäl.[107]

Av 3 kap. 4 § andra stycket säkerhetsskyddslagen följer att säkerhetsprövningen görs av den som beslutar om anställning eller annat deltagande i den säkerhetskänsliga verksamheten.[108]

Det huvudsakliga ansvaret för säkerhetsprövningen ligger på den verksamhet där den kontrollerade anställs, anlitas eller deltar genom annat deltagande. Det är vid verksamheten som det finns bäst kännedom om risker och sårbarheter och vilka krav som bör ställas.[109]

Säkerhetsprövning av personal från centermyndigheterna

Försvarets radioanstalt kommer enligt utredningens förslag vara huvudansvarig för centrets verksamhet och generaldirektören för Försvarets radioanstalt är den som har det yttersta ansvaret för säkerhetsskyddet i centrets verksamhet. Men utifrån vad som framgår av säkerhetsskyddslagen[110] ligger ansvaret för säkerhetsprövningen inte på Försvarets radioanstalt utan på den som beslutar om deltagande i den säkerhetskänsliga verksamheten. Eftersom Försvarets radioanstalt inte beslutar om placering i verksamheten för andra centermyndigheters personal, kan inte Försvarets radioanstalt ansvara för säkerhetsprövningen av dem.

Detta kan anses gå emot att det är den som är ansvarig för verksamheten där den kontrollerande ska delta som har ansvaret för säkerhetsprövningen. Det kan även innebära svårigheter för att få samtliga delar av säkerhetsskyddet att samverka med varandra för ett heltäckande skydd vilket ställer krav på alla samverkande myndigheter. Vidare finns det bestämmelser i Säkerhetspolisens föreskrifter om säkerhetsskydd och Försvarsmaktens föreskrifter om säkerhetsskydd där formuleringarna utgår från att säkerhetsprövningarna utförs av den som är ansvarig för verksamheten.[111]

Det går dock inte att enligt utredningens uppfattning komma till någon annan slutsats än att säkerhetsprövningen ska genomföras av den myndighet som beslutar om deltagande i centret, dvs. personalens ordinarie arbetsgivare. Utredningen vill dock framhålla att eftersom deltagande i centrets verksamhet ska beslutas efter överenskommelse mellan arbetsgivaren och Försvarets radioanstalt bör Försvarets

[107] Se vidare 3 kap. 2 § säkerhetsskyddslagen och 5 kap. 2–3 §§ säkerhetsskyddsförordningen vad gäller säkerhetsprövningens syfte och dess innehåll.
[108] Bestämmelsen anger även att det finns undantag från denna huvudprincip.
[109] Waern, Degerfeldt, Leeman, *Säkerhetsskyddslagen*, (2022-11-01, JUNO), kommentaren till 3 kap. 4 §.
[110] Jfr. 3 kap. 4 § andra stycket säkerhetsskyddslagen.
[111] Jfr. 6 kap. 1–6 §§ PMFS 2022:1 och 6 kap. 1–8 §§ FFS 2019:2.

radioanstalt ha möjlighet att ställa krav på bland annat viss säkerhetsklass[112] för den personal som ska tjänstgöra i centret. Försvarets radioanstalt bör även ha en möjlighet att hindra personal från deltagande om myndigheten anser att personalen inte uppfyller kraven för deltagande i den säkerhetskänsliga verksamheten.

Säkerhetsprövning av inlånad personal

Vad gäller inlånad personal är det den inlånande myndigheten som är den som beslutar om sådan personal ska få delta i den säkerhetskänsliga verksamheten. Det är därmed den inlånande myndigheten, alltså Försvarets radioanstalt, som har ansvar för säkerhetsprövning av denna personal.[113]

7.3 Slutsatser om säkerhetsskydd

Försvarets radioanstalt blir enligt utredningens förslag huvudansvarig för cybersäkerhetscentrets verksamhet och får det övergripande säkerhetsskyddsansvaret för verksamheten i centret. Men samtliga centermyndigheter har säkerhetsskyddsarbete att utföra i samband med deltagandet i centret, bland annat rörande informationssäkerhet och personalsäkerhet. Detta säkerhetsskyddsarbete behöver samordnas.

Ansvaret för att säkerhetspröva den personal som deltar i centrets verksamhet kommer att vara uppdelat. Personal från Försvarets radioanstalt och de som omfattas av personallån kommer att säkerhetsprövas av Försvarets radioanstalt. Personal från övriga centermyndigheter kommer att säkerhetsprövas av de myndigheter där de är anställda och som beslutar om deras placering i centrets verksamhet.

Det kan i vissa sammanhang finnas skäl att ingå säkerhetsskyddsöverenskommelser mellan de deltagande myndigheterna.

[112] Jfr. 3 kap. 10 § säkerhetsskyddslagen.
[113] Jfr. Ds 2022:26, s. 84–85.

8 Konsekvenser och finansiering

8.1 Allmänt

Utredningen har i sitt första delbetänkande gjort en konsekvensanalys av de föreslagna förändringarna i cybersäkerhetscentrets organisation, ledning och styrning. Konsekvensanalysen i detta delbetänkande är till viss del en fördjupning och förlängning av den analys som gjorts i det första delbetänkandet. Analyserna bör därför läsas gemensamt.[114]

8.2 Konsekvenser och kostnader för Försvarets radioanstalt

8.2.1 Nytt arbetssätt och nya verksamhetsförutsättningar

För Försvarets radioanstalt innebär utredningens förslag betydande förändringar. Myndigheten kommer att bedriva en ny typ av verksamhet med annan inriktning än myndighetens verksamhet i övrigt. Verksamheten i NCSC innebär också att det krävs en lång uppbyggnadsfas innan verksamheten är fullt utbyggd.

Ett cybersäkerhetscenter med allriskperspektiv innebär ett utökat rekryteringsbehov och att nya yrkeskategorier behöver anställas av Försvarets radioanstalt. Försvarets radioanstalts roll innebär att myndigheten behöver växa mer än övriga centermyndigheter för att kunna möta de behov som följer av NCSC:s uppgifter. Att anställa ny personal och att säkerhetspröva den är tidskrävande. Även den personal som lånas in från andra myndigheter måste säkerhetsprövas.

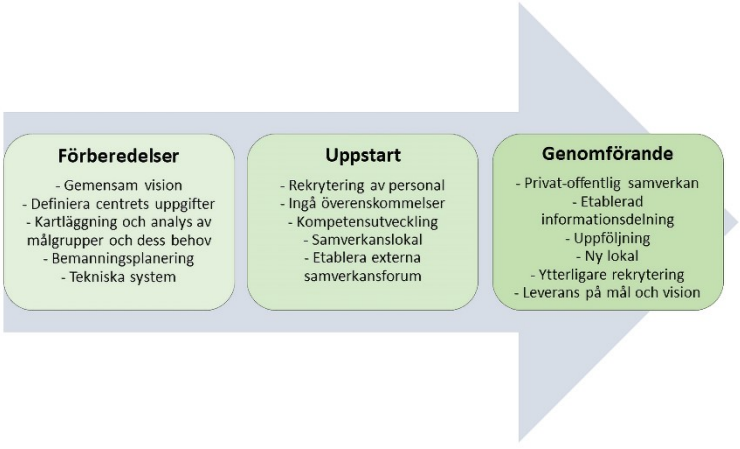
Försvarets radioanstalt som blir huvudansvarig för säkerhetsskyddsarbetet inom NCSC måste också analysera den nya verksamheten och arbeta in den i sin säkerhetsskyddsorganisation. Delar av säkerhetsskyddsarbetet kommer vidare ligga kvar på respektive centermyndighet vilket ställer krav på samverkan mellan myndigheterna för att centret ska få ett heltäckande säkerhetsskydd.

Försvarets radioanstalt blir också ansvarig för att ändamålsenliga lokaler och andra fysiska förutsättningar för verksamheten finns. Den permanenta lokalen kan vara färdigställd först år 2030. Eftersom den nuvarande lokalen är begränsad i sin storlek kommer det innebära svårigheter för centrets verksamhet att växa de närmaste åren. Det är först när centrets lokal blir verklighet som ett fullt utbyggt NCSC har möjlighet att etableras. Försvarets radioanstalt kan, innan lokalen blir tillgänglig, vidta åtgärder i

[114] Se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 6.

form av att bland annat ta fram gemensamma it-system, initiera utökad samverkan med näringslivet och skapa förutsättningar för samlokalisering av relevanta förmågor från de olika centermyndigheterna. Vissa aspekter av centrets verksamhet behöver också utredas vidare.

Etableringen kan förmodas innefatta följande faser:



Dessa faser visar att centrets verksamhet måste byggas upp successivt och att det inte kan förväntas att centret ska kunna göra allt som följer av dess uppdrag direkt. Verksamheten i centret kommer också ständigt behöva anpassas för att svara mot de behov som bland annat uppstår av den snabba tekniska utvecklingen hos målgrupperna.

8.2.2 Samverkan är fortfarande en del av verksamheten

Som utredningen kom fram till i första delbetänkandet bygger centrets verksamhet även fortsättningsvis på samverkan mellan de deltagande myndigheterna.[115]

I detta delbetänkande föreslår utredningen en bestämmelse som klargör att personal från de olika centermyndigheterna ska placeras i centret och att detta ska ske efter överenskommelse med Försvarets radioanstalt. Den personal som tjänstgör i centret ska kunna arbetsledas av centerchefen. Det innebär att Försvarets radioanstalt måste göra överenskommelser med övriga centermyndigheter för att det ska komma till stånd och dessutom ha kontinuerlig dialog kring bland annat arbetsförutsättningar och arbetsmiljö med övriga deltagande myndigheter.

Verksamheten i NCSC ställer stora krav på att de ingående myndigheterna samverkar och samarbetar för att gynna verksamheten i NCSC. Detta innebär ökad administration för framför allt Försvarets radioanstalt kopplat till den koordination och de överenskommelser som behöver finnas mellan myndigheterna.

[115] Se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 5.3 och 5.4.

8.3 Ekonomiska konsekvenser för Försvarets radioanstalt

Centret och dess breddade uppdrag medför betydligt ökade kostnader för Försvarets radioanstalt. Kostnaderna hänför sig bland annat till kostnader för lokal, personal och teknikutveckling. Försvarets radioanstalt har angett att kostnaderna för verksamheten kommer att uppgå till cirka 49 miljoner kronor år 2024, 160 miljoner kronor år 2025 och därefter öka årligen för att år 2030 nå en högsta nivå på 296 miljoner kronor när verksamheten kan genomföras i den avsedda lokalen.

Av Totalförsvarspropositionen framgår att för år 2024 tilldelas cybersäkerhetscentrets verksamhet 120 miljoner kronor. Dessa medel tilldelas Försvarets radioanstalt, Försvarsmakten, MSB och Säkerhetspolisen. För år 2025 ska enligt Totalförsvarspropositionen centrets verksamhet tilldelas 150 miljoner kronor.[116]

Som utredningen redan angett i sitt första delbetänkande bör huvuddelen av medlen som avser centerverksamheten tillfalla Försvarets radioanstalt.[117]

De 150 miljoner kronor som ska tilldelas centrets verksamhet år 2025 täcker inte helt de kostnader för verksamheten som Försvarets radioanstalt har beräknat att kostnaderna kommer uppgå till. I sin beräkning har Försvarets radioanstalt bland annat beaktat en eventuell verksamhetsöverföring och att myndigheten får i uppdrag att bli nationell cyberkrishanteringsmyndighet. Utredningen har förordat men inte föreslagit en verksamhetsöverföring utan anser att en sådan bör utredas i ett annat sammanhang. Det är positivt om en verksamhetsöverföring kan förberedas av Försvarets radioanstalt men kostnaderna på grund av dessa omständigheter är svåra att uppskatta eftersom ett genomförande av en verksamhetsöverföring inte är beslutat.

Utredningen anser att Försvarets radioanstalt måste få tillräckliga medel för att utveckla verksamheten i NCSC. De medel som avsatts till centrets verksamhet i Totalförsvarspropositionen för år 2025 bör därför tillföras Försvarets radioanstalt. Detta täcker enligt utredningens uppfattning de kostnader som Försvarets radioanstalt förväntas ha för att vara huvudansvarig för verksamheten. Det måste dock beaktas, som redogjorts för ovan, att beräkningarna i viss mån utgår från en eventuell verksamhetsöverföring och att verksamhetens inriktning och omfattning föreslås förändras jämfört med idag. Utredningen utgår från att medel kommer fortsätta tilldelas i en omfattning som medger att verksamheten utvecklas över tid. Myndigheterna har redan i svaret på regeringsuppdraget att inrätta cybersäkerhetscentret angett årliga kostnader om cirka 300 miljoner kronor för ett fullt utbyggt cybersäkerhetscenter, vilket är i linje med de beräkningar som Försvarets radioanstalt gjort för kostnadsutvecklingen över tid.[118]

[116] Prop. 2020/21:30, *Totalförsvaret 2021–2025*, s. 126.
[117] Se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 6.
[118] Myndigheternas svar på regeringsuppdrag (Fö2019/01000/SUND) inför inrättandet av ett nationellt cybersäkerhetscenter, s. 9.

8.4 Konsekvenser för övriga centermyndigheter

För de övriga centermyndigheterna innebär utredningens förslag konsekvenser främst på grund av att myndigheternas personal kommer att tjänstgöra i centret. Med det följer en risk för påverkan på myndighetens egen verksamhet och att effektiviteten där kan försämras. En stor del av uppgifterna som centermyndigheterna ska utföra inom ramen för centret är dock sådana uppgifter som de utför idag. Avsikten med NCSC är vidare att det gemensamma arbetet i centret ska stärka samhällets cybersäkerhet vilket ligger i allas intresse. Därtill kan samverkan ge positiva effekter för myndigheternas egen verksamhet.

Ett fullt utbyggt center innebär också konsekvenser för de deltagande myndigheterna eftersom det troligtvis kommer innebära behov av nyrekrytering av personal även för de övriga centermyndigheterna. Med det följer att fler säkerhetsprövningar behöver genomföras vilket är resurskrävande. Detta behov kommer dock troligtvis att bli större först när centret tillträtt sin permanenta lokal.

Förslagen får vidare konsekvenser vad gäller arbetsledning. För att arbetet inom centret ska bli så effektivt som möjligt behöver personalen som tjänstgör i centret underställas centerchefens ledning och utföra arbete som är detsamma eller närliggande till personalens ordinarie uppgifter på hemmamyndigheten. Detta ställer krav på att myndigheten där personalen är anställd medger att arbetsledning sker från centrets chef under den tiden då personalen arbetar i centret. Det kan innebära att personal som arbetar deltid i centrets verksamhet och deltid på hemmamyndigheten kan stå under delad arbetsledning. Detta bör dock inte vara något problem så länge ramarna för detta formuleras i överenskommelser mellan myndigheterna.

Det finns aspekter av samverkan som kan bli svårare att hantera, exempelvis arbetsmiljöfrågor. För personal som är anställda hos övriga centermyndigheter innebär det att centrala delar av ansvaret för deras arbetsmiljö kommer att finnas hos myndigheten som är arbetsgivare, även om arbetet sker i centret. Det kan därför medföra svårigheter för centermyndigheterna att faktiskt kunna ta ansvaret för arbetsmiljön. Svårigheterna innebär att det ställs höga krav på respektive arbetsgivare att undersöka arbetsmiljön och att man gör det regelbundet för att eventuella problem ska fångas upp. Det krävs därför en god dialog mellan hemmamyndigheten och Försvarets radioanstalt för att ansvaret för arbetsmiljön ska fungera så bra som möjligt.

8.5 Ekonomiska konsekvenser för övriga centermyndigheter

För de övriga centermyndigheterna innebär utredningens förslag ökade kostnader för framför allt personal men även administration. Utredningen har redan i sitt första delbetänkande redogjort för att kostnaderna kan förväntas att öka i takt med att centrets verksamhet utökas och byggs upp. Utredningen har bedömt att omfattningen av myndigheternas nuvarande medverkan kan finansieras inom befintliga anslag men att de på sikt kommer att behöva resurstillskott för att finansiera sin medverkan.

Ekonomiska tillskott är utöver vinsterna med själva samverkan ett viktigt incitament för att myndigheterna ska kunna bidra till och medverka i centrets verksamhet i tillräckligt stor omfattning.[119]

Utredningen vill framhålla att ekonomiska tillskott till samtliga centermyndigheter på sikt är en förutsättning för en välfungerande verksamhet i NCSC och att det krävs ekonomiska incitament och bidrag till de övriga myndigheterna över tid för att möjliggöra deras deltagande i verksamheten. Utredningen har dock bedömt att det är först när verksamheten kan expandera ytterligare som kostnaderna för övriga centermyndigheter kommer att öka på ett sådant sätt att tillskott utöver befintliga anslag behövs. Vad gäller personalen som arbetar i centret så finansieras denna nu inom befintliga ekonomiska ramar och det bör vara möjligt att fortsätta göra så en tid framöver. När verksamheten i centret utökas kan det finnas behov av att nyanställa personal särskilt för verksamheten i NCSC även för de andra centermyndigheterna. Det finns därmed behov av finansiering i framtiden.

8.6 Konsekvenser för andra aktörer

För andra myndigheter och offentliga organ innebär utredningens slutsatser i detta delbetänkande inte några väsentliga tillkommande kostnader.

För företagen innebär utredningens slutsatser i delbetänkandet inte några utökade kostnader. Delbetänkandet avser i huvudsak frågor som påverkar centrets interna arbete.

Vad gäller informationsdelning med näringslivet har utredningen identifierat potentiella svårigheter kring att det saknas sekretesskydd för affärs- och driftsförhållanden när information lämnas till centret. Utredningen bedömer att detta kan påverka viljan att lämna information till centret, vilket i sin tur riskerar påverka verksamhetens effektivitet.

8.7 Övriga konsekvenser

Utredningen bedömer inte att förslagen påverkar Sveriges åtaganden i förhållande till EU. Utredningen har inte identifierat några konsekvenser för domstolarna eller jämställdheten. Förslagen bedöms inte heller få några konsekvenser för den kommunala självstyrelsen eller kommunernas organisation.

[119] Se *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*, avsnitt 6.4.

9 Ikraftträdande

Utredningens förslag: Den föreslagna bestämmelsen om placering av personal från de deltagande myndigheterna i NCSC i förordningen om nationellt cybersäkerhetscenter föreslås träda i kraft den 1 september 2024.

Några övergångsbestämmelser bedöms inte nödvändiga.

Utredningen föreslår i första delbetänkandet att den nya förordningen om Nationellt cybersäkerhetscenter och följdändringarna i bland annat Försvarets radioanstalts instruktion träder i kraft den 1 september 2024. Det innebär att även den bestämmelse som nu föreslås i 8 § bör träda kraft samma datum. Detta för att ge Försvarets radioanstalt möjligheter och mandat att sätta i gång och effektivt driva arbetet med att utveckla NCSC.

Uppdrag att lämna förslag på hur en ändamålsenlig och effektiv ledning, organisering och styrning av Nationellt cybersäkerhetscenter ska utformas

Uppdraget i korthet

En utredare ska biträda Försvarsdepartementet genom att lämna förslag på former för en ändamålsenlig och effektiv ledning, organisering och styrning av Nationellt cybersäkerhetscenter (NCSC). Utredaren ska föreslå hur Försvarets radioanstalt kan ges ett huvudansvar för att leda samordningen, utvecklingen och genomförandet av centrets verksamhet, inklusive att ansvara för centrets kanslifunktion, i syfte att ge NCSC förutsättningar att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra större it-incidenter.

Utredaren ska vidare lämna förslag på hur samarbetet mellan de sju statliga myndigheterna inom centret kan organiseras och styras och hur deras uppdrag att bidra till centrets verksamhet ska formuleras.

Centret ska samverka med såväl privata som offentliga aktörer och även kunna samarbeta med internationella motsvarigheter utanför Sverige.

Uppdraget ska delredovisas senast den 29 februari 2024 och slutredovisas senast den 30 april 2024.

Nationellt cybersäkerhetscenter

Den 10 december 2020 beslutade den dåvarande regeringen att uppdra åt Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap och Säkerhetspolisen att fördjupa samverkan inom cybersäkerhetsområdet, genom ett nationellt cybersäkerhetscenter (Fö2019/01330). De fyra myndigheterna gavs i uppdrag att, inom ramen för centret, koordinera arbetet med att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter, förmedla råd och stöd avseende hot, sårbarheter och risker samt utgöra en nationell plattform för samverkan och informationsutbyte med privata och offentliga aktörer inom cybersäkerhetsområdet.

Av uppdraget framgick att samverkan skulle utvecklas stegvis under perioden 2021—2023 och att de fyra uppdragsmyndigheterna skulle ha en

nära samverkan med Försvarets materielverk, Polismyndigheten och Post- och telestyrelsen, vilka skulle ges möjlighet att medverka i cybersäkerhetscentrets verksamhet. Av uppdraget framgick också att regeringen avsåg att under 2023 ta ställning till hur cybersäkerhetscentrets verksamhet fortsatt bör inriktas och bedrivas efter 2023.

Behovet av en utredning

Verksamheten inom NCSC har inte nått den effekt som krävs för att centret fullt ut ska uppnå sitt syfte. Organisationsformen, där fyra myndigheter har ett lika stort ansvar, blir otydlig för myndigheterna och svår för regeringen att styra och följa upp. Det finns därför behov av att etablera en mer ändamålsenlig, effektiv och tydlig ledning, utveckling och styrning av verksamheten inom centret.

Uppdraget

Utredaren ska utgå ifrån att Försvarets radioanstalt ges ett huvudansvar för att leda samordningen, utvecklingen och genomförandet av centrets verksamhet, inklusive att ansvara för centrets kanslifunktion. Vidare ska utredaren utgå ifrån att de övriga sex myndigheter som idag ingår i centret ska göra det även fortsatt, inom ramen för sina respektive verksamhetsområden.

Utredaren ska lämna förslag på hur huvudansvaret för Försvarets radioanstalt ska utformas så att verksamheten som NCSC bedriver kan ledas, organiseras och styras på ett ändamålsenligt och effektivt sätt. Syftet med NCSC ska vara att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra större it-incidenter. Målgrupp för centrets verksamhet är såväl privata som offentliga aktörer. Centret ska även kunna samarbeta med internationella motsvarigheter utanför Sverige.

Krav på rättssäkerhet, effektivitet och insyn måste alltid tillgodoses i handläggningen av förvaltningsuppgifter. Inför den fortsatta verksamheten behöver uppgifter och mandat tydliggöras i författning eller beslut. Det behöver klargöras vem som är behörig att fatta beslut, vem som ska ansvara för verksamheten inför regeringen och tydliggöras hur ansvarsförhållandena ser ut mellan centrets myndigheter, utifrån deras respektive verksamhetsområden.

För att säkerställa att de olika myndigheterna på lämpligt sätt kan dela information, även sekretessbelagd, sinsemellan ska utredaren analysera behovet av informationsutbyte samt hur sådant utbyte kan möjliggöras. Utredaren ska föreslå de författningsändringar som bedöms nödvändiga för att informationsutbytet inom centret ska fungera. I syfte att utveckla samverkan med näringslivet ska utredaren också analysera hur relevant och lämpligt informationsutbyte mellan centret och berörda privata aktörer

kan möjliggöras, samt föreslå eventuella författningsändringar som bedöms nödvändiga.

För att säkerställa att inga problem uppstår rörande hantering av personuppgifter på grund av den förändrade ansvarsfördelningen och organiseringen ska utredaren också analysera och vid behov lämna förslag på ytterligare reglering avseende personuppgiftsbehandling inom centret. Det finns också ett behov av att klargöra hur personal-, arbetsgivar-, budget- och säkerhetsskyddsfrågor inom centerkansliet ska hanteras när en myndighet får ett särskilt utpekat ansvar för dessa.

Utredaren ska utgå ifrån att verksamheten i centret ska omfatta att

- utveckla och stärka arbetet för att förebygga, upptäcka och hantera cyberattacker och andra större it-incidenter,
- utgöra en nationell plattform för privat-offentlig samverkan och förmedla råd och stöd avseende hot, sårbarheter och risker,
- producera samlade lägesbilder avseende cyberhot och större it-incidenter, utgöra en samlad kontaktpunkt för frågor som rör informations- och cybersäkerhet,
- övergripande koordinera internationella samarbeten kopplade till centrets verksamhet,
- verka för ett enhetligt informations- och cybersäkerhetsarbete, samt
- rapportera till regeringen om nödvändiga åtgärder för stärkt cybersäkerhet.

Utredaren ska därför

- analysera och lämna förslag på hur Försvarets radioanstalts huvudansvar för att leda samordningen, utvecklingen och genomförandet av centrets verksamhet, inklusive ansvaret för centrets kanslifunktion, ska utformas och hur dessa uppgifter ska regleras,
- analysera och lämna förslag på hur formerna för samverkan mellan Försvarets radioanstalt och de övriga myndigheterna i centret ska organiseras och regleras,
- analysera och föreslå ändamålsenliga ansvars- och ledningsförhållanden i verksamheten och mellan samverkande myndigheter,
- analysera och föreslå hur personal-, arbetsgivar-, budget- och säkerhetsskyddsfrågor inom verksamheten ska regleras,
- analysera och föreslå hur nödvändigt utbyte av information, även innehållande sekretesskyddade uppgifter, inom centret och mellan centret och privata aktörer ska fungera,
- analysera och vid behov lämna förslag på hur hantering av personuppgifter ska ske inom centret,
- analysera om de myndigheter som samverkar i centret är i behov av förtydligade uppgifter och befogenheter för att tillsammans utföra centrets ovan angivna uppgifter på ett effektivt sätt och vid behov lämna förslag på förändringar, samt

- lämna förslag på de författningsändringar eller andra åtgärder som bedöms nödvändiga.

Utredningsarbetet

Utredaren ska analysera och redovisa konsekvenserna av sina förslag inklusive hur medel ska fördelas mellan Försvarets radioanstalt och de övriga ingående myndigheterna. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna ska utredaren lämna förslag om hur dessa ska finansieras. Utredaren ska vad gäller finansiering beakta de tillskott som aviserades i totalförsvarspropositionen för 2020 (prop. 2020/21:30).

Utredaren ska säkerställa att de förslag som lämnas är förenliga med nuvarande och kommande krav som uppställs i EU-rätten och med Sveriges internationella åtaganden i övrigt.

Utredningen ska inhämta synpunkter och upplysningar från Försvarets radioanstalt, Säkerhetspolisen, Myndigheten för samhällsskydd och beredskap, Försvarsmakten, Försvarets materielverk, Polismyndigheten samt Post- och telestyrelsen. Utredaren ska också inhämta synpunkter från kommuner, regioner och relevanta branschorganisationer. Vid behov ska utredaren inhämta synpunkter och upplysningar även från andra aktörer som kan vara berörda.

Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och kommittéväsendet. Av särskild vikt är Utredningen om genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft (Fö 2023:01).

Utredaren har möjlighet att ta upp även andra frågor som har samband med de frågeställningar som ska utredas under förutsättning att uppdraget ändå kan redovisas i tid.

Redovisning av uppdraget

Uppdraget ska i de delar som avser hur Försvarets radioanstalts huvudansvar ska utformas, hur formerna för samverkan mellan Försvarets radioanstalt och de övriga myndigheterna ska organiseras och regleras, hur ändamålsenliga ansvars- och ledningsförhållanden i verksamheten och mellan de samverkande myndigheterna ska åstadkommas, huruvida myndigheterna i centret är i behov av förtydligade uppgifter och befogenheter, samt därtill hörande förslag avseende författningsändringar och andra åtgärder redovisas den 29 februari 2024.

De delar av uppdraget som avser hur personal-, arbetsgivar-, budget- och säkerhetsskyddsfrågor inom verksamheten ska regleras, hur nödvändigt

utbyte av information inom centret och mellan centret och privata aktörer ska fungera, hur hantering av personuppgifter ska ske inom centret, samt därtill hörande förslag avseende författningsändringar och andra åtgärder ska redovisas senast den 30 april 2024.