Ett nytt Nationellt cybersäkerhetscenter

Ändamålsenliga och effektiva former för ledning, organisering och styrning

Del 1

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 utformas (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 delbetänkandet *Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning*.

Med detta är uppdraget i denna del slutfört.

Umeå i april 2024

Per Bergling

/Ninni Bohman Olin
Anna Wennberg

Innehåll

Sammanfattning

Nationellt cybersäkerhetscenter (NCSC) inrättades i december 2020 efter uppdrag från regeringen. Verksamheten har inte uppnått förväntade resultat. En utredning har därför tillsatts med uppdrag att utreda och föreslå ändamålsenliga och effektiva former för ledning, organisering och styrning av centrets verksamhet.

Det överordnade målet med en ändamålsenlig och effektiv ledning, organisering och styrning av NCSC ska vara att åstadkomma en nödvändig höjning av Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot och betydande it-incidenter.

Utredningen föreslår att det i förordning regleras att Försvarets radioanstalt ska ha huvudansvar för att leda samordning, utveckling och genomförande av centrets verksamhet. De sju myndigheter som redan ingår i cybersäkerhetscentrets verksamhet ska fortsätta göra detta.

Även centrets uppgifter ska anges i förordning. Centret ska präglas av ett allriskperspektiv. Även hur myndighetssamverkan inom NCSC ska ske ska regleras i förordning. Centret ska vidare ledas av en chef som anställs av regeringen.

Varje centermyndighets skyldighet att medverka i och bidra till centrets verksamhet inom ramen för sitt verksamhetsområde ska framgå av respektive myndighets instruktion. Det ska i förordning göras tydligt att den verksamhet som centermyndigheterna kan utföra inom ramen för cybersäkerhetscentret också ska utföras inom ramen för centret.

Utredningen bedömer att den operativa verksamhetens organisation inte ska regleras i förordning utan ska byggas upp utifrån cybersäkerhetscentrets behov. Centret bör utarbeta och bestämma lämpliga former för operativ samverkan och deconfliction.

Utredningen bedömer att ett effektivt utförande av NCSC:s 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. Försvarets radioanstalt och MSB bör under tiden genomföra en så nära integration av verksamheterna som möjligt.

Detta är utredningens första delbetänkande. I nästa delbetänkande behandlas personal-, arbetsgivar-, budget- och säkerhetskyddsfrågor samt informationsdelning och personuppgiftsbehandling i centrets verksamhet.

Förkortningar

I denna promemoria används bland annat följande förkortningar.

CAF	Cyber Assessment Framework
CERT	Computer Emergency Response Team
CSEC	Sveriges Certifieringsorgan för IT-säkerhet
CSIRT	Computer Security Incident Response Team
Cybersäkerhetsakten	Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013
Digg	Myndigheten för digital förvaltning
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
FCKS	Felles cyberkoordineringssenter
FE	Forsvarets Efterretningstjeneste
FIRST	Forum of Incident Response and Security Teams
FL	Förvaltningslagen (2017:900)
FOI	Totalförsvarets forskningsinstitut
GCHQ	Government Communications Headquarters
ICC	Inspektionen för cybersäkerhetscertifiering
IWWN	International Watch and Warning Network
KTH	Kungliga tekniska högskolan
MISP	Malware Information Sharing Platform
MPF	Myndigheten för psykologiskt försvar

MSB	Myndigheten för samhällsskydd och beredskap
Must	Militära underrättelse- och säkerhetstjänsten
NCC-SE	Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet
NCSC	Nationellt cybersäkerhetscenter
NIS-direktivet	Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen
NIS2-direktivet	Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148
NSM	Nasjonal sikkerhetsmyndighet
NTSG	Nationella Telesamverkansgruppen
SAMFI	Samverkansgruppen för informationssäkerhet
SKR	Sveriges kommuner och regioner
SOC	Security Operations Center
SOFF	Säkerhets- och försvarsföretagen
TDV	Tekniskt detekterings- och varningssystem
VDI	Varslingssystem for digital infrastruktur

1 Författningsförslag

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

Härigenom föreskrivs följande.

Inledande bestämmelse

1 § Vid Försvarets radioanstalt ska det finnas ett Nationellt cybersäkerhetscenter.

Uppgifter

2 § Det Nationella cybersäkerhetscentret ska utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot och betydande it-incidenter.

Cybersäkerhetscentret ska utgöra nationell plattform för privat-offentlig samverkan och vara samlad kontaktpunkt för frågor som rör informationssäkerhet och cybersäkerhet.

3 § Det Nationella cybersäkerhetscentret ska därutöver särskilt

1. förmedla råd och stöd avseende hot, sårbarheter och risker,
2. producera samlade lägesuppfattningar avseende cyberhot och betydande it-incidenter,
3. övergripande koordinera och delta i internationella samarbeten kopplade till centrets verksamhet,
4. verka för ett enhetligt informationssäkerhets- och cybersäkerhetsarbete samt
5. rapportera till regeringen om nödvändiga åtgärder för stärkt cybersäkerhet.

Deltagande myndigheter

4 § I det Nationella cybersäkerhetscentrets verksamhet deltar utöver Försvarets radioanstalt

- Försvarets materielverk,
- Försvarsmakten,
- Myndigheten för samhällsskydd och beredskap,
- Polismyndigheten,
- Post- och telestyrelsen och
- Säkerhetspolisen.

Ansvar och medverkan

5 § Försvarets radioanstalt har huvudansvaret för att leda det Nationella cybersäkerhetscentrets verksamhet. I detta ingår att ansvara för samordning, utveckling, uppföljning och rapportering av cybersäkerhetscentrets verksamhet.

Försvarets radioanstalt ska årligen till regeringen redovisa den verksamhet som bedrivits i centret. Redovisningen ska innehålla en redogörelse för verksamhetens resultat och effekter.

6 § Myndigheterna som anges i 4 § ska delta i och bidra till cybersäkerhetscentrets verksamhet inom ramen för sina verksamhetsområden.

Myndigheterna ska även bidra till planering, uppföljning och utveckling av verksamheten samt bistå Försvarets radioanstalt med stöd till centergemensamma administrativa stödfunktioner.

7 § Den verksamhet som myndigheterna i 4 § bedriver som kan utföras inom ramen för det Nationella cybersäkerhetscentret ska utföras inom ramen för centret.

En myndighet i 4 § som har författningsreglerade uppgifter att ge stöd vid hanteringen av ett cyberhot eller betydande it-incident ska, i den omfattning det är lämpligt, få stöd från övriga deltagande myndigheter.

Samverkan

9 § Vid det Nationella cybersäkerhetscentret ska det finnas ett strategiskt samverkansråd med uppgift att bidra till planering, uppföljning och rapportering av centrets verksamhet.

I det strategiska samverkansrådet företräds myndigheterna i 4 § av sina myndighetschefer. Rådet leds av generaldirektören för Försvarets radioanstalt eller generaldirektörens ställföreträdare.

1.2 Förslag till förordning om ändring i förordningen (2007:937) med instruktion för Försvarets radioanstalt

Härigenom föreskrivs i fråga om förordningen (2007:937) med instruktion för Försvarets radioanstalt att det ska införas två nya paragrafer, 4 a § och 7 a § av följande lydelse.

4 a §

Vid Försvarets radioanstalt ska det finnas ett Nationellt cybersäkerhetscenter.

Bestämmelser om verksamheten i det Nationella cybersäkerhetscentret finns i förordningen (2024:000) om Nationellt cybersäkerhetscenter.

7 a §

Chefen för det Nationella cybersäkerhetscentret anställs av regeringen.

Chefen för det Nationella cybersäkerhetscentret är underställd generaldirektören för Försvarets radioanstalt och ansvarar för sin verksamhet inför Försvarets radioanstalts ledning.

Denna förordning träder i kraft den 1 september 2024.

1.3 Förslag till förordning om ändring i förordningen (2007:854) med instruktion för Försvarets materielverk

Härigenom föreskrivs i fråga om förordningen (2007:854) med instruktion för Försvarets materielverk att det ska införas en ny paragraf, 6 a § och närmast före 6 a § en ny rubrik av följande lydelse.

Samverkan

6 a §

Försvarets materielverk ska medverka i och bidra till det Nationella cybersäkerhetscentrets verksamhet inom ramen för sitt verksamhetsområde.

Bestämmelser om verksamheten i det Nationella cybersäkerhetscentret finns i förordningen (2024:000) om Nationellt cybersäkerhetscenter.

Denna förordning träder i kraft den 1 september 2024.

1.4. Förslag till förordning om ändring i förordningen (2007:1266) med instruktion för Försvarsmakten

Härigenom föreskrivs i fråga om förordningen (2007:1266) med instruktion för Försvarsmakten att det ska införas en ny paragraf, 4 a §.

4 a §

Försvarsmakten ska medverka i och bidra till det Nationella cybersäkerhetscentrets verksamhet inom ramen för sitt verksamhetsområde.

Bestämmelser om verksamheten i det Nationella cybersäkerhetscentret finns i förordningen (2024:000) om Nationellt cybersäkerhetscenter.

Denna förordning träder i kraft den 1 september 2024.

1.5. Förslag till förordning om ändring i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap

Härigenom föreskrivs i fråga om förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap att det ska införas en ny paragraf, 11 d §.

11 d §

Myndigheten för samhällsskydd och beredskap ska medverka i och bidra till det Nationella cybersäkerhetscentrets verksamhet inom ramen för sitt verksamhetsområde.

Bestämmelser om verksamheten i det Nationella cybersäkerhetscentret finns i förordningen (2024:000) om Nationellt cybersäkerhetscenter.

Denna förordning träder i kraft den 1 september 2024.

1.6. Förslag till förordning om ändring i förordningen (2022:1718) med instruktion för Polismyndigheten

Härigenom föreskrivs i fråga om förordningen (2022:1718) med instruktion för Polismyndigheten att det ska införas en ny paragraf, 22 a §.

22 a §

Polismyndigheten ska medverka i och bidra till det Nationella cybersäkerhetscentrets verksamhet inom ramen för sitt verksamhetsområde.

Bestämmelser om verksamheten i det Nationella cybersäkerhetscentret finns i förordningen (2024:000) om Nationellt cybersäkerhetscenter.

Denna förordning träder i kraft den 1 september 2024.

1.7. Förslag till förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen

Härigenom föreskrivs i fråga om förordningen (2007:951) med instruktion för Post- och telestyrelsen att det ska införas en ny paragraf, 13 a § och närmast före 13 a § en ny rubrik av följande lydelse.

Samverkan

13 a §

Post- och telestyrelsen ska medverka i och bidra till det Nationella cybersäkerhetscentrets verksamhet inom ramen för sitt verksamhetsområde.

Bestämmelser om verksamheten i det Nationella cybersäkerhetscentret finns i förordningen (2024:000) om Nationellt cybersäkerhetscenter.

Denna förordning träder i kraft den 1 september 2024.

1.8. Förslag till förordning om ändring i förordningen (2022:1719) med instruktion för Säkerhetspolisen

Härigenom föreskrivs i fråga om förordningen (2022:1719) med instruktion för Säkerhetspolisen att det ska införas en ny paragraf, 10 a §.

10 a §

Säkerhetspolisen ska medverka i och bidra till det Nationella cybersäkerhetscentrets verksamhet inom ramen för sitt verksamhetsområde.

Bestämmelser om verksamheten i det Nationella cybersäkerhetscentret finns i förordningen (2024:000) om Nationellt cybersäkerhetscenter.

Denna förordning träder i kraft den 1 september 2024.

2 Utredningens uppdrag och arbete

2.1 Uppdraget

Det Nationella cybersäkerhetscentrets resultat har inte motsvarat uppdragsgivarens eller målgruppernas förväntningar. En utredning har därför tillsatts.

I sin första del ska utredningen analysera och lämna förslag på hur Försvarets radioanstalt ska utöva huvudansvaret för att leda samordning, utveckling och genomförande av centrets verksamhet. Utredningen ska också föreslå ändamålsenliga lednings- och ansvarsförhållanden för verksamheten, lämna förslag på former för samverkan mellan de olika myndigheterna och hur samverkan ska regleras samt analysera om myndigheterna är i behov av förtydligade uppgifter och befogenheter för att tillsammans utföra centrets uppgifter.

I sin andra del kommer utredningen lämna förslag på hur personal-, arbetsgivar-, budget- och säkerhetsskyddsfrågor ska regleras inom ramen för centrets verksamhet. Utredningen ska också analysera och föreslå hur informationsutbyte ska ske inom centret och med de aktuella myndigheterna samt mellan centret och andra offentliga och privata aktörer. Utredningen ska även se över hanteringen av personuppgifter i centrets verksamhet.

Uppdragsbeskrivningen i sin helhet finns i bilaga 1 till denna promemoria. Denna promemoria avser uppdragets första del.

Statsrådet Carl-Oskar Bohlin beslutade den 1 februari 2024 att ge utredningen ytterligare tid. Den första delredovisningen ska därför ske den 15 april 2024 och slutredovisning den 15 juni 2024.[1]

2.2 Avgränsningar

Det följer av utredningens uppdragsbeskrivning att de myndigheter som nu ingår i centerverksamheten ska fortsätta göra detta, och att deras medverkan ska ske inom ramen för respektive myndighets verksamhetsområde. Utredningen ska dock analysera om centermyndigheternas uppgifter och befogenheter behöver förtydligas.

Centrets verksamhet ska också ha det innehåll som följer av utredningens uppdragsbeskrivning. Utredningen har dock kunnat konstatera att beskrivningen innehåller vissa problematiska begränsningar, bland annat i form av begreppen *större* it-incidenter och *antagonistiska* cyberhot. Utredningen har därför valt att föreslå att centrets uppgifter inte ska vara begränsade till antagonistiska hot och att större it-incidenter ersätts med betydande it-incidenter, se vidare avsnitt 5.1.1.

[1] Regeringskansliets beslut Fö2024/00215.

2.3 Samråd och dialog

Utredningens arbete inleddes i oktober 2023. Utredningen har vid möten inhämtat synpunkter och upplysningar från Försvarets radioanstalt, Försvarsmakten, MSB, Säkerhetspolisen, Försvarets Materielverk, Polismyndigheten, Post- och telestyrelsen samt cybersäkerhetscentrets chef och kansli.

Utredningen har också haft möten med Myndigheten för psykologiskt försvar (MPF), Ekobrottsmyndigheten, Center mot våldsbejakande extremism, Sveriges kommuner och regioner (SKR), Svenskt Näringsliv, Arbetsgivarverket, Säkerhets- och försvarsföretagen (SOFF), Internetstiftelsen, TechSverige, Cybercampus och företaget Cparta. Information och upplysningar har även inhämtats från Västra Götalandsregionen, Region Gävleborg samt kommunerna Dals-Ed, Malmö, Sundsvall och Ånge.

Möten har även hållits med utredningen om genomförande av NIS2- och CER-direktiven (dir. 2023:30), utredningen om operativ krisledning vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur (Fi2023/01842) och utredningen om översyn av underrättelse-verksamheten (dir. 2023:150).

Utredningen har besökt de nationella cybersäkerhetscentren i Förenade kungariket, Danmark och Norge.

3 Nulägesbeskrivning

3.1 Cybersäkerhetscentrets uppdrag

Den 10 december 2020 uppdrog regeringen åt Försvarets radioanstalt, Försvarsmakten, MSB och Säkerhetspolisen att fördjupa samverkan inom cybersäkerhetsområdet genom ett Nationellt cybersäkerhetscenter.[2] Regeringen angav att dessa myndigheter skulle ha en nära samverkan med Försvarets materielverk, Polismyndigheten och Post- och telestyrelsen. De skulle också ges möjlighet att medverka i centrets verksamhet. Det övergripande målet med den fördjupade samverkan angavs vara att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot.

Regeringen klargjorde vidare att myndigheterna skulle bidra till verksamheten inom ramen för sina befintliga verksamhetsområden. Den fördjupade samverkan avsågs alltså inte att påverka de ingående myndigheterna befintliga ansvar. Samarbetets närmare innehåll och former skulle fastställas genom skriftliga överenskommelser mellan myndigheterna. Det framgick också av uppdraget att samverkan med privata och offentliga aktörer skulle utgöra en central del av centrets uppgifter. Vad gäller verksamhetens målgrupper angavs dessa vara både privata och offentliga aktörer. Centret avsågs även kunna delta i internationella samarbeten på myndighetsnivå.

Beskrivningen av centrets uppgifter framgår av utredningens uppdragsbeskrivning, se bilaga 1. Där anges NCSC:s verksamhet omfatta:

- 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.

[2] Regeringsbeslut Fö2019/01330.

3.2 Centrets finansiering, organisation och arbetsformer

3.2.1 Anslag för verksamheten

Försvarets radioanstalt, Försvarsmakten, MSB och Säkerhetspolisen tilldelas särskilda medel för verksamheten i NCSC. Försvarets materielverk, Polismyndigheten och Post- och telestyrelsen får däremot inga sådana medel.

De största anslagen lämnas till Försvarets radioanstalt och MSB. Dessa avses motsvara myndigheternas kostnader för gemensam lokal, kanslipersonal och rörliga kostnader för verksamheten i centret. Centermyndigheternas kostnader för personal täcks av respektive myndighets anslag och inte av de tillskott som myndigheterna får för sin medverkan i NCSC.[3]

Tabell 3.1 Fördelning av medel mellan centermyndigheterna

Siffror anges i miljoner kronor.

Myndighet	2022	2023	2024
Försvarets radioanstalt	20	20	35
Försvarsmakten	10	10	25
MSB	20	20	35
Säkerhetspolisen	10	10	25
Totalt	**60**	**60**	**120**

Redovisade medel avser enbart medel som är särskilt avsedda för verksamheten i NCSC. Medel som tilldelas myndigheterna för annan verksamhet inom informationssäkerhets- och cybersäkerhetsområdet redovisas inte.

3.2.2 Centrets styrning och ledning

Centret har idag flera nivåer av styrning och ledning. Generaldirektörsgruppen som består av generaldirektörerna för de sju samverkande myndigheterna, fattar konsensusbeslut i principiella frågor, till exempel gällande centrets budget, ekonomi och aktivitetsplan.

I den strategiska ledningsgruppen ingår avdelningschefer direkt underställda centermyndigheternas generaldirektörer. Den strategiska ledningsgruppen ser till att cybersäkerhetscentret får resurser och personal. Gruppen fattar vidare beslut om NCSC:s strategiska inriktning. Besluten fattas i konsensus.

Point of Contact-gruppen består av kontaktpersoner från de olika centermyndigheterna. Dessa medverkar i det dagliga arbetet och den operativa ledningen av NCSC. Gruppen möts varje vecka under ledning av centerchefen.

[3] Jfr Myndigheternas svar på uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter, Fö2019/01000/SUND, s. 9.

Chefen för cybersäkerhetscentret tillsätts av Försvarets radioanstalt. Chefen ansvarar för, leder och samordnar den dagliga verksamheten i centret i enlighet med den aktivitetsplan som fastställts av generaldirektörsgruppen. Samordningsarbetet sköter chefen tillsammans med centrets kansli. Kansliet samordnar också myndigheternas expertkompetens i den gemensamma verksamheten.

De samverkande myndigheterna har skapat flera gemensamma arbetsgrupper för specifika delar av centrets verksamhet. Det finns till exempel grupper för hantering av incidenter, lägesbilder, extern samverkan och övning. Det finns även grupper för den stödjande verksamheten, till exempel juridik, lokaler, säkerhet, upphandling, ekonomi och kommunikation. Dessa arbetsgrupper hålls ihop av kanslipersonalen. Samtliga myndigheter bidrar till stödfunktionerna i någon omfattning, till exempel genom att bidra med personal till arbetsgrupperna.

3.3 Myndigheternas verksamhetsområden

3.3.1 Allmänt

Av det Nationella cybersäkerhetscentrets uppdrag från 2020 framgår att centermyndigheterna deltar i och bidrar till verksamheten inom ramen för sina befintliga uppgifter. Det innebär att varje myndighets möjlighet att bidra till centrets verksamhet styrs och begränsas av hur myndighetens verksamhetsområde beskrivs i lag och instruktion.[4] Konstruktionen innebär också att myndigheternas bidrag till centret blir olika stora, då vissa kan bidra till flera av centrets verksamheter medan andra bara kan bidra till en eller ett fåtal beroende på vilket eller vilka verksamhetsområden myndigheten har.

3.3.2 Försvarets radioanstalt

Försvarets radioanstalt är en civil myndighet som bedriver signalspaning och utgör en del av Sveriges underrättelsetjänst. Signalunderrättelseverksamheten riktas mot utländska förhållanden och ger stöd för svensk försvars-, utrikes- och säkerhetspolitik. Uppdragsgivare för signalunderrättelseverksamheten är regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen inom Polismyndigheten.

Försvarets radioanstalt arbetar också med cybersäkerhet och har bland annat i uppdrag att stödja insatser vid nationella kriser med it-inslag, medverka till identifieringen av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser och ge annat tekniskt stöd.[5] Försvarets radioanstalt är Sveriges expertmyndighet för

[4] Jfr regeringsuppdrag Fö2019/01330, s. 3 och SOU 2004:23, *Från verksförordning till myndighetsförordning,* s. 85.
[5] 1 och 4 §§ förordningen (2007:937) med instruktion för Försvarets radioanstalt.

teknisk it-säkerhet. Uppdragsgivare för denna del av verksamheten är både statliga myndigheter och enskilda verksamhetsutövare.

En annan uppgift är att utveckla och placera ut tekniskt detekterings- och varningssystem (TDV). TDV erbjuds till de i samhället mest skyddsvärda verksamheterna.[6]

3.3.3 Försvarsmakten

Försvarsmaktens huvuduppgift är att försvara Sverige mot ett väpnat angrepp, främja Sveriges säkerhet och hävda Sveriges territoriella integritet. Försvarsmakten ska även med myndighetens befintliga förmåga och resurser kunna lämna stöd till civil verksamhet.[7] Inom cybersäkerhetsområdet ansvarar Försvarsmakten för Sveriges offensiva och defensiva cyberförsvarsförmåga och ska kunna möta ett antagonistiskt hot med stöd av andra myndigheter, till exempel Försvarets radioanstalt och övriga försvarsunderrättelsemyndigheter, Säkerhetspolisen och MSB.[8]

Inom Försvarsmakten finns även den militära underrättelse- och säkerhetstjänsten (Must). Must bedriver försvarsunderrättelseverksamhet och militär underrättelsetjänst som syftar till att ge underlag som stöd till svensk utrikes-, säkerhets- och försvarspolitik och att kartlägga yttre hot mot Sverige. Arbetet sker genom inhämtning, analys och bearbetning av information. Utifrån inhämtad information gör Must analyser och bedömningar om till exempel utvecklingen i olika geografiska områden och om utländska aktörers avsikter och förmågor.[9]

3.3.4 MSB

MSB har ett brett verksamhetsområde som omfattar en mängd uppgifter inom samhällsskydd och beredskap. Verksamhetsområdet omfattar även flera uppgifter inom informationssäkerhets- och cybersäkerhetsområdet. MSB ska bland annat stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner, regioner, företag och organisationer. Myndigheten har också uppdraget att vara nationellt samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE).[10]

MSB har i uppdrag att ansvara för Sveriges nationella CSIRT, CERT-SE. CERT-SE stödjer samhället i förebyggande och hantering av it-incidenter. CERT-SE stödjer både privat och offentlig sektor med ett särskilt fokus på samhällsviktig verksamhet. MSB ska genom CERT-SE samordna insatser vid större it-säkerhetsincidenter, samverka med

[6] https://fra.se/cyberforsvar/dethargorfra.4.55af049f184e92956c42b0a.html, senast hämtad 2024-04-12.
[7] 1 och 2 §§ förordningen (2007:1266) med instruktion för Försvarsmakten.
[8] Prop. 2020/21:30, *Totalförsvaret 2021–2025,* s. 152.
[9] https://www.forsvarsmakten.se/sv/organisation/hogkvarteret/militara-underrattelse-och-sakerhetstjansten/, senast hämtad 2024-04-10.
[10] 11 a och 11 c §§ förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

myndigheterna inom NCSC och vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder.[11]

Av MSB:s uppdrag följer också andra uppgifter kopplade till NIS-direktivet[12]. Med uppdraget att ansvara för Sveriges nationella CSIRT följer uppgiften att delta i EU:s CSIRT-nätverk och utgöra sambandsfunktion för gränsöverskridande samarbete mellan motsvarande myndigheter i andra EU-länder.

MSB representerar även Sverige i andra europeiska och internationella forum, bland annat CSIRT Network och International Watch and Warning Network (IWWN).[13]

3.3.5 Säkerhetspolisen

Säkerhetspolisen är Sveriges nationella säkerhetstjänst och bedriver underrättelse- och säkerhetsarbete. Till Säkerhetspolisens uppgifter hör bland annat att förebygga, förhindra och upptäcka brottslig verksamhet som till exempel innefattar brott mot rikets säkerhet eller terrorbrott samt fullgöra uppgifter enligt säkerhetsskyddslagen (2018:585).

Säkerhetspolisen får också ge tekniskt stöd inom säkerhetsskydd. Säkerhetsskydd innefattar att vidta åtgärder för att höja säkerhetsnivån i samhället genom analyser, registerkontroll, tillsyn och rekommendationer till myndigheter och delar av näringslivet som har betydelse för Sveriges säkerhet.[14]

3.3.6 Polismyndigheten

Till Polismyndighetens uppgifter hör att förebygga, förhindra och upptäcka brottslig verksamhet och andra störningar av den allmänna ordningen eller säkerheten. Polismyndigheten ska också utreda och beivra brott som hör under allmänt åtal och lämna allmänheten skydd, upplysningar och annan hjälp, när sådant bistånd lämpligen kan ges av polisen samt fullgöra den verksamhet som ankommer på Polismyndigheten enligt särskilda bestämmelser.[15]

Polismyndigheten arbete innefattar även verksamhet som syftar till att förebygga, förhindra och upptäcka brottslig verksamhet. Denna verksamhet omfattar bland annat underrättelseverksamhet.[16] Polismyndigheten deltar också i omfattande internationellt samarbete, bland annat gemen-

[11] 11 b § förordningen med instruktion för Myndigheten för samhällsskydd och beredskap och https://cert.se/om-cert-se/, senast hämtad 2024-04-10.
[12] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet).
[13] https://www.informationssakerhet.se/om-informationssakerhet2/cert-se/, senast hämtad 2024-04-15.
[14] 3 § polislagen (1984:387) samt 1 och 6 §§ förordningen (2022:1719) med instruktion för Säkerhetspolisen och https://www.sakerhetspolisen.se/om-sakerhetspolisen/sakerhetspolisens-uppdrag.html, senast hämtad 2024-04-14.
[15] 2 § polislagen.
[16] Ds 2018:35, *Polisens tillgång till uppgifter från signalspaning*, s. 33.

samma brottsutredningar, gränsöverskridande insatser och utbyte av underrättelseinformation.[17]

3.3.7 Försvarets materielverk

Försvarets materielverk arbetar bland annat med att upphandla, utveckla och leverera materiel och tjänster till det svenska försvaret och att biträda Försvarsmakten i planeringen av materiel- och logistikförsörjningen.

Vid Försvarets materielverk finns även Sveriges nationella certifieringsorgan för it-säkerhet i produkter och system (CSEC). Som nationellt certifieringsorgan för IT-säkerhet ansvarar CSEC för att ta fram och utveckla regler för granskning av IT-säkerhet i produkter och system.[18]

Vid myndigheten finns också Inspektionen för cybersäkerhetscertifiering (ICC), vilken ansvarar för alla samverkans- och tillsynsuppgifter som följer av det europeiska ramverket för cybersäkerhetscertifiering.[19]

3.3.8 Post- och telestyrelsen

Post- och telestyrelsen har ett samlat ansvar inom områdena post och elektronisk kommunikation. Med begreppet elektronisk kommunikation avses telekommunikationer, it och radio.

Post- och telestyrelsen har bland annat till uppgift att främja tillgången till säkra och effektiva elektroniska kommunikationer, följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation samt verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder och verka för ökad krishanteringsförmåga.

Post- och telestyrelsen ska också verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation. Detta ska ske genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer. Post- och telestyrelsen ska även lämna råd och stöd till myndigheter, kommuner och regioner samt till företag, organisationer och andra enskilda i frågor om nätsäkerhet.[20]

3.4 Privat-offentlig samverkan i NCSC

NCSC har i uppgift att vara samlad kontaktpunkt för frågor som rör informationssäkerhet och cybersäkerhet och utgöra nationell plattform för privat-offentlig samverkan. NCSC har också i uppgift att samla befintliga

[17] https://polisen.se/om-polisen/internationell-verksamhet/, senast hämtad 2024-04-10.
[18] 1 och 5 §§ förordningen (2007:854) med instruktion för Försvarets materielverk.
[19] 3 § förordningen (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt samt Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).
[20] 1 och 4 §§ förordningen (2007:951) med instruktion för Post- och telestyrelsen.

informationsinsatser riktade till näringslivet inom ramen för centret så långt det är möjligt. Samverkan ska alltså omfatta många målgrupper med olika behov.

Sedan hösten 2022 driver NCSC pilotprojektet NCSC finansforum, vars syfte är att främja utökat samarbete och informationsutbyte mellan aktörer i sektorn och relevanta myndigheter. Inom projektet genomförs bland annat gemensamma övningar och kommunikationsinsatser. Liknande former av samverkan har inletts med energi-, telekom-, transport-, säkerhets- och försvarssektorn.

NCSC genomför även föreläsningar för och håller sammankomster med branschorganisationer, företag och myndigheter.[21]

3.5 Problem i styrning, ledning och organisation

Utredningen konstaterar att cybersäkerhetscentrets arbete försvåras av problem och utmaningar relaterade till styrning, ledning och organisation av verksamheten. Dessa kan kategoriseras och beskrivas som följer:

NCSC saknar tydliga mål, uppdrag och ansvarsfördelning

De samverkande myndigheterna har svårt att förstå centrets uppgifter. Detta leder ofta till olika och motsägelsefulla prioriteringar mellan myndigheterna och att vissa uppgifter i centret inte prioriterats alls. Flera av centermyndigheterna har till exempel endast intresserat sig för informationsdelning i de fall informationen rört angrepp av statsunderstödda aktörer. Centrets uppgifter omfattar dock inte enbart denna typ av cyberangrepp, utan även andra it-incidenter vilket Riksrevisionen bedömt inte har fått genomslag i verksamheten.[22]

Även ansvarsfördelningen mellan myndigheterna anses otydlig och har lett till situationer där ingen myndighet anser sig ha befogenhet eller intresse att gå till handling. Problemen förvärras av avsaknaden av en chef med tydligt mandat att leda verksamheten.

Det saknas central styrning på informationssäkerhets- och cybersäkerhetsområdet, både generellt och av NCSC

Det finns tydliga brister i styrningen av det tvärsektoriella informationssäkerhets- och cybersäkerhetsområdet.[23] Någon gemensam sammanhållande funktion inom Regeringskansliet finns inte, och de olika interdepartementala arbetsgrupperna som ska underlätta informationsutbyte och gemensam styrning har inte varit framgångsrika.[24] Sådana styrningsproblem är visserligen typiska för tvärsektoriella områden, men

[21] Regeringsuppdrag Fö2023/00907.
[22] Riksrevisionen, *Regeringens styrning av samhällets information- och cybersäkerhet – både brådskande och viktig* (RiR 2023:8), s. 44.
[23] Jfr RiR 2023:8, Totalförsvarets forskningsinstitut, *Delat ansvar är ingens ansvar? En analys av den svenska statsförvaltningens ansvar och styrning vad gäller svenskt informations- och cybersäkerhetsarbete* (FOI-R—5546—SE) samt Kungliga ingenjörsvetenskapsakademin, *Cybersäkerhet för ökad konkurrenskraft*.
[24] RiR 2023:8, s. 60.

dess konsekvenser blir särskilt allvarliga när resurserna är knappa och snabb förmågehöjning behövs.[25]

Styrningen av centret har också brister. Riksrevisionen beskriver styrningen som otydlig och otillräcklig.[26] Utredningen delar den bilden. Utredningen anser att det delade ansvaret mellan olika statsråd vid flera departement förklarar flera problem.

Delat ledningsansvar är tidskrävande och ineffektivt

Centret är ett ”fördjupat samarbete” mellan flera myndigheter och därmed inte en självständig myndighet eller del av en specifik myndighet. Med detta följer att viktiga beslut förutsätter samförstånd mellan myndigheterna innan beslut kan fattas. Ofta krävs samförstånd även i mindre eller triviala angelägenheter rörande verksamheten. Tiden innan alla myndigheter har berett frågor internt och återkommit med besked kan vara mycket lång. Den strategiska inriktningen av verksamheten fungerar heller inte så väl som den borde eftersom forumen för strategisk samverkan inte kunnat ägna sig åt enbart strategiska frågor.

Den speciella samverkanskonstruktionen har också gett upphov till problem rörande informationsdelning, diarieföring av inkomna och upprättade handlingar, upphandling, gemensam it-drift och lokalförsörjning.

Centerchefen kan inte fatta nödvändiga beslut och saknar rådighet över centrets resurser

Centrets chef har ansvar för verksamheten men saknar befogenhet att fatta nödvändiga beslut. Centerchefen har inte heller arbetsgivaransvar för och kan inte effektivt arbetsleda den personal som centermyndigheterna placerat i verksamheten. Centerchefens uppgifter är mer att leda centrets kansli och samordningen av centermyndigheternas bidrag till verksamheten.[27] Det är alltså centermyndigheterna som ”äger” och beslutar över väsentliga delar av NCSC:s resurser och verksamhet. Det innebär att verksamheten är svårstyrd och att utrymmet att bedriva någon operativ verksamhet är begränsat.

Utbudsstyrd tilldelning av viktiga resurser

Vilka resurser och vilken personal cybersäkerhetscentret kan förfoga över bestäms i liten utsträckning av centret självt, utan avgörs av vad varje myndighet anser sig kunna erbjuda eller avvara. Centrets verksamhet är därför inte så efterfråge- eller målgruppsstyrd som den borde vara.

Besvikelse och förväntningar

Centret har inte kunnat leverera den information eller det stöd som regeringen eller målgrupperna efterfrågat. Näringslivet och andra

[25] Jfr SOU 2021:89 volym 2, *Sverige under pandemin*, s. 747–749 som identifierar liknande problem gällande det svenska smittskyddet under coronapandemin.
[26] RiR 2023:8, s. 67.
[27] Jfr Myndigheternas svar på regeringsuppdrag (Fö2019/01000/SUND) inför inrättandet av ett nationellt cybersäkerhetscenter, s. 7.

intressenter har inte heller känt att deras bidrag till verksamheten alltid tagits väl om hand eller tillräckligt uppskattas av myndigheterna.[28]

Den sista tidens allvarliga incidenter och attacker har också visat på allvarliga brister i förmågan att hantera samhällskritiska incidenter och attacker och att denna generella förmåga måste höjas snabbt. Det finns med andra ord både besvikelse och irritation över det som varit och höga förväntningar på det nya centret och dess verksamhet.

[28] RiR 2023:8 s. 5.

4 Internationell utblick

4.1 Nationella cybersäkerhetscenter i andra länder

Nationella cybersäkerhetscenter finns i många andra länder. Vissa cybersäkerhetscenter är en del av signalspaningsmyndigheter. Så är fallet till exempel i Danmark, Förenade Kungariket och Australien.[29] I Norge tillhör cybersäkerhetscentret en särskild säkerhetsmyndighet medan det i Finland är en del av Transport- och kommunikationsverket som har ett brett uppdrag inom flera verksamhetsområden och sektorer.[30] I Estland tillhör cybersäkerhetscentret en myndighet med särskilt ansvar för cybersäkerhet och nationella informationssystem.[31] I Kanada är centret en egen myndighet.[32] I Nederländerna har justitie- och säkerhetsdepartementet samlat bland annat den nationella incidenthanteringen i ett cybersäkerhetscenter som är underställt departementet.[33]

Utredningen har besökt cybersäkerhetscentren i Förenade kungariket, Danmark och Norge. De följande avsnitten presenterar dessa cybersäkerhetscenter närmare.

4.2 Förenade kungariket

Det brittiska nationella cybersäkerhetscentret (National Cyber Security Centre) inrättades i oktober 2016 som en del av signalunderrättelsemyndigheten Government Communications Headquarters (GCHQ).[34] I samband med bildandet överfördes flera olika offentliga myndigheters organ med ansvar för cybersäkerhetsfrågor, bland annat den nationella CERT-funktionen, till cybersäkerhetscentret.[35] Målsättningen var att genom nära och effektiva samarbeten mellan myndigheter, näringsliv, akademien, internationella partners och enskilda göra den digitala miljön i landet säkrare.

I centrets uppgifter ingår bland annat att ge råd och stöd till regeringen och andra offentliga och privata aktörer kring informationssäkerhets- och cybersäkerhetsfrågor. En viktig uppgift är också att vara statens ansikte utåt i cybersäkerhetsfrågor. Cybersäkerhetscentret är alltså en utåtriktad

[29] SOU 2021:63, *Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem,* s. 275, 299 och 336.
[30] SOU 2021:63, s. 262–263 och 267–269.
[31] https://www.ria.ee/en/authority-news-and-contact/authority-and-management/tasks-and-structure-authority, senast hämtad 2024-02-29.
[32] SOU 2021:63, s. 323.
[33] SOU 2021:63, s. 279.
[34] United Kingdom Intelligence Services Act 1994, section 3 och United Kingdom *National Cyber Security Strategy 2016 to 2021*, s. 29.
[35] https://www.ncsc.gov.uk/section/about-ncsc/what-we-do, senast hämtad 2024-02-26.

organisation, men har tillgång till GCHQ:s underrättelseverksamhet och tekniska expertis.[36]

Cybersäkerhetscentret arbetar med incidenthantering och att minska skadorna som drabbar enskilda organisationer eller samhället. Alla typer av incidenter hanteras inte, utan centret är inriktat på de som är av mer allvarlig karaktär och som potentiellt kan påverka stora delar av samhället. Centret arbetar också för att minska cybersäkerhetsrisker, bland annat genom att säkra nätverk både i den offentliga och den privata sektorn. Inom centret finns de nationella CSIRT-funktionerna; CERT-UK och GovCERT.[37]

Målgrupperna är breda och innefattar bland annat näringslivet, offentliga organ, välgörenhetsorganisationer och allmänheten. Centret utformar vägledningar samt ger stöd och råd till privata och offentliga aktörer om cybersäkerhet. Centret har bland annat skapat särskilda vägledningar för småföretag, välgörenhetsorganisationer och aktörer inom juristbranschen.[38]

Cybersäkerhetscentret arbetar inte med att ta fram reglering eller föreskrifter eller att utöva tillsyn. Detta är ett medvetet val för att underlätta effektiv informationsdelning mellan myndigheter och privat sektor. Däremot arbetar centret med att stödja myndigheter och offentliga organ som har till uppgift att ta fram föreskrifter eller utöva tillsyn.[39]

För delning av information finns en plattform som möjliggör delning i en säker miljö. Information delas både av centret och av personer som arbetar i den privata sektorn.[40] Centret arbetar också med sektorsspecifika samverkansgrupper som syftar till att öka samhällets motståndskraft mot cyberattacker.[41]

Cybersäkerhetscentret har skapat ett Cyber Assessment Framework (CAF) som är ett verktyg för att bedöma en samhällsviktig organisations cybersäkerhetsnivå.[42]

Det brittiska cybersäkerhetscentret har också skapat olika former av certifieringar för personal, produkter, tjänster och organisationer. Ett antal leverantörer av tjänster inom riskhantering, säkerhetsarkitektur samt revision och granskning har certifierats.[43]

För närmare integrering mellan cybersäkerhetscentret och näringslivet har centret ett särskilt program för sekundering av personal, Industry100. Programmet möjliggör placering av personal från privata bolag i

[36] United Kingdom *National Cyber Security Strategy 2016 to 2021*, s. 29.
[37] United Kingdom *National Cyber Security Strategy 2016 to 2021*, s. 29 och Royal United Services Institute for Defence and Security Studies, Hannigan, *Organising a Government for Cyber – The Creation of the UK's National Cyber Security Centre*, s. 18.
[38] https://www.ncsc.gov.uk/section/about-ncsc/what-we-do, senast hämtad 2024-02-26.
[39] Hannigan, *Organising a Government for Cyber – The Creation of the UK's National Cyber Security Centre*, s. 16–17.
[40] https://www.ncsc.gov.uk/cisp/home, senast hämtad 2024-02-27 och Hannigan, *Organising a Government for Cyber – The Creation of the UK's National Cyber Security Centre* s. 22.
[41] NCSC *Annual Review 2023*, s. 23.
[42] https://www.ncsc.gov.uk/collection/caf, senast hämtad 2024-02-26.
[43] https://www.ncsc.gov.uk/section/products-services/ncsc-certification, senast hämtad 2024-02-26.

centerverksamheten.[44] Det är inte bara personer med teknisk expertis som placeras utan även jurister och andra professioner.[45]

4.3 Danmark

Det danska nationella cybersäkerhetscentret (Center for Cybersikkerhed) är en del av Forsvarets Efterretningstjeneste (FE) och inrättades i december 2012. FE är Danmarks utlandsunderrättelsetjänst och militära underrättelsetjänst, och bedriver informationsinhämtning genom bland annat signalspaning och fysisk inhämtning.[46]

Cybersäkerhetscentret arbetar främst med att stärka cybersäkerheten inom samhällsviktiga sektorer. Eftersom centret är en del av FE har det tillgång till underrättelsebaserad kunskap om cyberfrågor. Centret är både nationell it-säkerhetsmyndighet och nationellt kompetenscentrum inom cybersäkerhet. Målet med verksamheten är bidra till en hög nivå av informationssäkerhet i den digitala infrastruktur som samhällsviktiga verksamheter är beroende av. Centret består av sju avdelningar: beredskap, tele och standarder, cyberanalys, cyberoperationer, försvar och ackreditering, rådgivning och standardisering, cybersituationscentret, samt strategi, kommunikation och EU.[47]

Arbetet med att stärka cybersäkerheten sker bland annat genom rådgivning om hur myndigheter och näringsliv kan förebygga, motverka och skydda olika verksamheter mot cyberattacker. Genom sin nätsäkerhetstjänst analyserar centret både myndigheters och företags nätverkskommunikation för att upptäcka eventuella intrång. Om en attack eller incident inträffar informerar centret den drabbade organisationen och ger råd om det behövs.[48]

Under år 2018 etablerades ett cybersituationscenter inom ramen för cybersäkerhetscentret. Dess syfte är att skapa en nationell cyberlägesbild. Situationscentret kan också utfärda varningar och rekommendationer i samband med en specifik cyberattack, aktuella cyberhot eller andra it-säkerhetsincidenter som kan vara av intresse för myndigheter, företag och andra aktörer.[49]

Cybersäkerhetcentret representerar Danmark i flera olika internationella CSIRT-nätverk såsom FIRST (Forum of Incident Response and Security Teams) och IWWN. Centret deltar även i andra internationella nätverk och samarbeten inom ramen för NATO och EU. Cybersäkerhetscentret är Danmarks nationella CSIRT och deltar i det europeiska CSIRT-nätverket. Centret är också kontaktpunkt för gränsöverskridande incidenter inom EU.

[44] https://www.ncsc.gov.uk/section/industry-100/about, senast hämtad 2024-02-26.
[45] https://www.ncsc.gov.uk/blog-post/i100-insider-the-cyber-security-advocate, senast hämtad 2024-02-26.
[46] https://www.fe-ddis.dk/da/om-os/sadan-arbejder-fe/Efterretningskredsloeb/, senast hämtad 2024-04-12.
[47] https://www.cfcs.dk/da/om-os/organisation/, senast hämtad 2024-04-05.
[48] https://www.cfcs.dk/da/handelser/, senast hämtad 2024-04-10.
[49] https://www.fmn.dk/da/arbejdsomraader/cybersikkerhed/center-for-cybersikkerhed/, senast hämtad 2024-02-27.

Centrets avdelning för rådgivning och standardisering är också ansvarig myndighet för informationssäkerhet och beredskap inom teleområdet.[50]

4.4 Norge

Det norska nationella cybersäkerhetscentret (Nasjonalt cybersikkerhetssenter) är en del av Nasjonal sikkerhetsmyndighet (NSM) och inrättades i november 2019. NSM är en tvärsektoriell myndighet med ett generellt ansvar för säkerhetsfrågor, vilket innefattar digital säkerhet, personalsäkerhet och fysisk säkerhet.[51] Eftersom NSM:s verksamhet både är militär och civil styrs myndigheten och dess verksamhet gemensamt av justitie- och beredskapsdepartementet samt försvarsdepartementet.[52]

Det norska cybersäkerhetscentret har till uppdrag att skydda grundläggande samhällsfunktioner, offentlig förvaltning och näringslivet mot cyberangrepp. Arbetet omfattar bland annat att ge råd, genomföra tillsyn och utföra andra kontrollaktiviteter inom både det civila och militära området till skydd för bland annat samhällsviktig information, system och infrastruktur. Cybersäkerhetscentret är vidare en arena för nationellt och internationellt samarbete inom bland annat detektion, hantering och analys av incidenter. För Norges räkning deltar cybersäkerhetscentret i internationella CERT- och CSIRT-nätverk och är till exempel medlem i FIRST och IWWN.[53]

Centret samarbetar med näringslivet, akademin, försvaret och andra delar av offentlig sektor. För att underlätta informationsdelning och bygga upp samarbetsstrukturer har cybersäkerhetscentret ett partnerskapsprogram där både offentliga och privata verksamheter deltar. Verksamheterna som deltar i partnerskapsprogrammet bjuds in för att de är ägare av kritisk digital infrastruktur inom de mest samhällskritiska sektorerna. För att säkerställa överblick av potentiella incidenter har centret även kontakt med de delar av näringslivet som levererar tjänster till kritisk infrastruktur.[54]

Cybersäkerhetscentret arbetar förebyggande genom att utfärda varningar gällande sårbarheter, viktiga uppdateringar och incidenter. Centret utfärdar också råd, varningar och rekommendationer om digital säkerhet till både offentlig och privat sektor. De varningar som centret utfärdar rör i regel samhällsviktig verksamhet eller risker och hot som påverkar stora delar av samhället.[55]

Vidare arbetar centret med att koordinera och hantera allvarliga cyberattacker mot kritisk infrastruktur. Arbetet inkluderar upptäckt av incidenter, incidenthantering och analys av inträffade incidenter.

[50] https://www.fe-ddis.dk/da/om-os/organisation/, senast hämtad 2024-02-27.
[51] https://nsm.no/, senast hämtad 2024-02-27.
[52] Hovedinstruks for Nasjonal sikkerhetsmyndighet, 2019-05-03, s. 3.
[53] https://nsm.no/fagomrader/digital-sikkerhet/ och https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/handtering-av-dataangrep/hendelseshandtering, senast hämtad 2024-02-27.
[54] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/ och https://www.nsmmagasin.no/lofoten-de-gronne-oyene/, senast hämtad 2024-02-27.
[55] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/, senast hämtad 2024-02-27.

Cybersäkerhetscentret är den nationella responsfunktionen för allvarliga cyberangrepp och är nationell CSIRT-funktion. Vid cybersäkerhetscentret finns ett operationscenter som är bemannat dygnet runt och som bland annat varnar om sårbarheter och larm från det nationella anmälningssystemet för digital infrastruktur.[56]

Inom ramen för cybersäkerhetscentrets verksamhet finns också Felles cyberkoordineringssenter (FCKS). FCKS är ett samarbete mellan den norska utlandsunderrättelsetjänsten Etterretningstjeneste, inrikesunderrättelsetjänsten Politiets sikkerhetstjeneste och NSM. I cyberkoordineringscentret arbetar personal från de olika myndigheterna tillsammans. Målet med FCKS är att snabbt kunna koordinera sektorsövergripande incidenter och att myndigheterna ska kunna skapa en uppdaterad gemensam lägesbild. När incidenter inträffar ska samarbetet mellan myndigheterna intensifieras.[57]

Cybersäkerhetscentret erbjuder både offentliga och privata aktörer en rad tekniska tjänster. Samhällsviktiga verksamheter kan erbjudas delta i sensornätverket Varslingssystem for digital infrastruktur (VDI). Centret erbjuder även tjänster i form av penetrationstester och sårbarhetskartläggningar.[58]

[56] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/handtering-av-dataangrep/hendelseshandtering, senast hämtad 2024-02-26.
[57] https://www.etterretningstjenesten.no/om-etterretning/etterretning-og-sikkerhet-i-norge, senast hämtad 2024-02-27.
[58] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/tekniske-sikkerhetstjenester/, senast hämtad 2024-02-26.

5 Ett nytt Nationellt cybersäkerhetscenter

5.1 Mål och utgångspunkter

Utredningens bedömning: Stärkt svensk cybersäkerhet kräver tydlig kraftsamling till NCSC, utvecklad och kravställd samverkan, ett allriskperspektiv och att näringslivets förmågor tas bättre tillvara.

För att nå det övergripande målet med NCSC – att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot och betydande it-incidenter – bedömer utredningen att tydlig kraftsamling till NCSC och Försvarets radioanstalt måste ske. Verksamheten ska därför breddas och omfatta ett allriskperspektiv och samverkan mellan centermyndigheterna och andra offentliga och privata aktörer måste fördjupas.

Vidare ska följande utgångspunkter gälla:

- Försvarets radioanstalt har tydligt huvudansvar att leda samordningen, utvecklingen och genomförandet av centrets verksamhet.
- Försvarets radioanstalt och de övriga sex centermyndigheterna samverkar effektivt i centret och bidrar till verksamheten inom ramen för sina respektive verksamhetsområden.
- NCSC har en stark operativ organisation under centerchefens ledning.
- NCSC är nationell plattform för privat-offentlig samverkan och samlad kontaktpunkt för frågor som rör informations-säkerhets- och cybersäkerhetsfrågor.
- NCSC bedriver en målgrupps- och efterfrågeorienterad verksamhet i vilken näringslivets och andra intressenters behov och resurser effektivt tas tillvara.

Särskilt om allriskperspektiv och spetskompetens

Utredningen noterar att jämförbara utländska cybersäkerhetscenter har ett tydligt allriskperspektiv i sina verksamheter. Med allriskperspektiv avses en strävan att bedöma alla typer av risker för det som ska skyddas och att analysera alla möjliga orsaker till att en risk realiseras.[59] Många offentliga och privata intressenter i Sverige anser att NCSC behöver ha en liknande ambition. På så sätt skulle det bli tydligt vilket ansvar centret har och det

[59] Se vidare om Förenade kungariket, Danmark och Norge i avsnitt 4.2, 4.3 och 4.4. Jfr även SOU 2021:63 s. 261–349 där fler länders organisation på cybersäkerhetsområdet redovisas.

skulle också bli tydligare för målgrupperna vart de ska vända sig för råd och stöd.

NCSC:s verksamhet utgår redan till viss del från ett allriskperspektiv. Centret ska till exempel vara samlad kontaktpunkt för informationssäkerhets- och cybersäkerhetsfrågor, en nationell plattform för privat-offentlig samverkan och verka för ett enhetligt informationssäkerhets- och cybersäkerhetsarbete. Men det behöver förtydligas att allriskperspektivet ska gälla i stort sett hela centrets verksamhet, och att centret vid varje händelse och tidpunkt ska vidta de åtgärder som innebär störst effekt och samhällsnytta på informationssäkerhets- och cybersäkerhetsområdet.

Men detta innebär inte att centret ska arbeta med alla frågeställningar eller incidenter på informationssäkerhets- och cybersäkerhetsområdet. För detta finns inte resurser, varken nu eller i framtiden. Centrets fokus ska vara att utveckla och stärka arbetet med att upptäcka, förebygga och hantera hot och incidenter av en viss allvarlighetsgrad samt att verka för en generell höjning av cybersäkerheten och resiliensen nationellt.

I vissa delar av verksamheten kan inte allriskperspektivet vara centrum eller styrande. Det faller sig till exempel naturligt att vissa centermyndigheter har spetskompetenser inom specifika områden och att de i första hand bidrar med stöd och information som avser de allra mest skyddsvärda och samhällskritiska verksamheterna. Utredningen anser att kombinationen av ett tydligare allriskperspektiv i verksamheten kombinerat med en förmåga att utnyttja spetskompetens vad gäller de svåraste och mest allvarliga incidenterna, kommer främja målet om stärkt nationell förmåga att förebygga, upptäcka och hantera hot och risker på informationssäkerhets- och cybersäkerhetsområdet.

Särskilt om värdet av samverkan och gemensamma insatser

Informationssäkerhets- och cybersäkerhetsområdet är tvärsektoriellt och inga risker och hot kan hanteras av en myndighet ensam. Det krävs därför gemensamma insatser för att höja den allmänna nivån av cybersäkerhet i samhället. För att genomföra verkningsfulla åtgärder inom sektorn krävs både gemensam planering och kraftsamling mellan centermyndigheterna och mellan NCSC och andra intressenter. Utredningen bedömer därför att fördjupad samverkan fortsätter vara en förutsättning för att uppnå hållbara resultat och göra det mesta av begränsade resurser. Företrädare för centermyndigheterna, näringslivet och andra aktörer lyfter att personalen inte räcker till för att bemanna liknande funktioner eller utföra samma uppgifter på flera ställen. Det samarbete och det informationsutbyte som sker inom NCSC är därför en viktig beståndsdel i att stärka den nationella förmågan att förebygga, upptäcka och hantera cyberhot och betydande it-incidenter.

5.1.1 En förordning om Nationellt cybersäkerhetscenter

Utredningens förslag: Centrets uppgifter ska regleras i förordningen om nationellt cybersäkerhetscenter. Av denna ska framgå att det Nationella cybersäkerhetscentret ska utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot och betydande it-incidenter.

Cybersäkerhetscentret ska utgöra nationell plattform för privat-offentlig samverkan och vara samlad kontaktpunkt för frågor som rör informationssäkerhet och cybersäkerhet. Det Nationella cybersäkerhetscentret ska därutöver särskilt

1. förmedla råd och stöd avseende hot, sårbarheter och risker,
2. producera samlade lägesuppfattningar avseende cyberhot och betydande it-incidenter,
3. övergripande koordinera och delta i internationella samarbeten kopplade till centrets verksamhet,
4. verka för ett enhetligt informationssäkerhets- och cybersäkerhetsarbete samt
5. rapportera till regeringen om nödvändiga åtgärder för stärkt cybersäkerhet.

Förordningens uppräkning av centrets uppgifter ska inte vara uttömmande.

Utredningen har uppmärksammat en osäkerhet och ambivalens gällande cybersäkerhetscentrets mål och uppgifter. Detta påverkar både incitamenten att medverka i verksamheten och arbetets effektivitet, se vidare avsnitt 3.5. Det ska därför i en förordning om Nationellt cybersäkerhetscenter klargöras vad centrets mål och uppgifter är samt att centermyndigheterna ska bidra till dessa.

Det bör noteras att denna utrednings uppdragsbeskrivning redan innehåller en angivelse av vilket uppgifter NCSC ska ha, se bilaga 1. Men utredningen anser inte att den generella förmågehöjning som är utredningens överordnade syfte är möjlig inom dessa ramar. Efter samtal med uppdragsgivaren har utredningen därför valt att ange centrets uppgifter på ett annorlunda och mer ändamålsenligt sätt i förslaget till förordning.

En sådan justering rör begreppet *större* it-incidenter. Eftersom detta begrepp saknar enhetlig definition ska det ersättas med begreppet *betydande* it-incidenter, som definieras i artikel 23 i NIS2-direktivet[60]. En incident ska enligt direktivet anses vara betydande om den har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten eller om den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada. I ett delbetänkande om genomförande av NIS2-direktivet föreslås också att definitionen ska anges i en ny lag om cybersäkerhet. Av denna nya lag skulle vidare följa att regeringen eller den

[60] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148.

myndighet som regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande incident.[61] Begreppet betydande it-incident gör det alltså möjligt att tydligare beskriva centrets uppgifter och bör därför användas i förordningen om Nationellt cybersäkerhetscenter.

Utredningen anser inte heller att centrets uppdrag längre ska vara begränsat till att avse *antagonistiska* cyberhot. En sådan begränsning innebär nämligen att ett hot måste kunna attribueras till en aktör med en specifik intention för att centret ska kunna agera. För att göra det möjligt för centret att effektivt bidra till att öka den samlade informationssäkerheten och cybersäkerheten i samhället ska uppdraget avse cyberhot utan begränsande kvalificeringar.

I uppdragsbeskrivningen används också ordet *cyberattack*. Utredningen har i stället valt att i beskrivningen av centrets uppgifter använda det definierade begreppet *cyberhot*. I EU:s cybersäkerhetsakt definieras cyberhot som en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer.[62]

Utredningen har av liknande anledning valt att använda begreppet *lägesuppfattning* i stället för *lägesbild*. I NIS2-direktivet anges att den nationella CSIRT-enheten ska tillhandahålla dynamiska risk- och incidentanalyser och situationsmedvetenhet gällande cybersäkerhet. Utredningen om genomförande av NIS2- och CER-direktiven har valt att använda begreppet lägesuppfattning för att beskriva detta.[63] Användningen av detta begrepp innebär en tydligare definition av uppgiften för NCSC och stämmer överens med den nationella CSIRT:ens föreslagna uppdrag, vilket har betydelse för utredningens bedömning i avsnitt 5.3.3.

Uppdragen till NCSC kommer alltså vara breda och täcka ett stort antal behov och utmaningar. Men centret kommer ändå behöva hantera nya och oförutsedda uppgifter. Flexibilitet och anpassningsförmåga är därför nödvändiga. Uppräkningen av centrets uppgifter i förordningen ska därmed inte vara uttömmande.

[61] SOU 2024:18, *Nya regler om cybersäkerhet,* s. 374–375.
[62] Artikel 2 punkten 8 cybersäkerhetsakten.
[63] SOU 2024:18, s. 306.

5.2 Ledning och styrning av NCSC

Utredningens förslag: Det nationella cybersäkerhetscentret blir en del av Försvarets radioanstalt och myndigheten får därmed huvudansvar för NCSC. Detta ska framgå av förordningen med instruktion för Försvarets radioanstalt och förordningen om Nationellt cybersäkerhetscenter.

Utredningen bedömer att många problem när det gäller NCSC:s mål och resultat beror på oklarheter i styrningen och ledningen, se avsnitt 3.5. Styrning, ledning och ansvar ska därför förtydligas i förordningen om Nationellt cybersäkerhetscenter och förordningen med instruktion för Försvarets radioanstalt.

Av Försvarets radioanstalts instruktion ska framgå att cybersäkerhetscentret är en del av Försvarets radioanstalt. NCSC är alltså inte en egen myndighet eller juridisk person, utan ingår i Försvarets radioanstalts organisation och ledningsstruktur. Med denna konstruktion följer att NCSC kan dra nytta av en etablerad myndighets verksamhet, administrativa strukturer och processer.

I Försvarets radioanstalts huvudansvar för centret ska ingå att leda samordningen, utvecklingen och genomförandet av verksamheten. Ansvaret innefattar även att rapportera och redovisa till regeringen samt att ansvara för administrativa funktioner och andra verksamhetsförutsättningar, bland annat lokaler och tekniska system. Försvarets radioanstalts förtydligade ansvar innebär dock inte att de övriga centermyndigheterna blir mindre viktiga eller utan ansvar. De ska fortsätta att samverka i och bidra till centrets verksamhet på det sätt som framgår av förordningen om Nationellt cybersäkerhetscenter och respektive myndighets ändrade instruktion, se vidare avsnitt 5.3.

Särskilt om samordning, uppföljning, rapportering och redovisning

Verksamheten har vid flera tillfällen försvårats eller förhindrats av problem i samordningen och koordinationen av de medverkande myndigheterna. Problemen kan förväntas minska med ett tydligt huvudansvar för verksamheten, men samordning kommer fortfarande att behövas eftersom myndigheter med olika verksamhetsområden även framöver ska arbeta tillsammans mot gemensamma mål.

Försvarets radioanstalt ska som huvudansvarig för centret leda samordningen på en övergripande och strategisk nivå. Försvarets radioanstalt och dess generaldirektör ska också leda det strategiska samverkansråd som ska inrättas, se avsnitt 5.4.1 nedan. Försvarets radioanstalt ska även ha ett särskilt ansvar att följa upp och analysera genomförandet av cybersäkerhetscentrets uppgifter.

Försvarets radioanstalt ska ha ansvar att rapportera till regeringen om nödvändiga åtgärder för stärkt cybersäkerhet. Denna uppgift framgår av cybersäkerhetscentrets uppdrag så som det formulerats i utredningsuppdraget. Övriga centermyndigheter ska bidra med underlag till rapporteringen. Även dessa bidrag behöver samordnas av Försvarets radioanstalt.

I den redovisning som årligen ska lämnas till regeringen ska Försvarets radioanstalt lämna en analys av verksamhetens resultat och effekter. Centermyndigheterna ska gemensamt säkerställa att Försvarets radioanstalt har ett fullgott underlag för den redovisning som ska lämnas till regeringen. Här har Försvarets radioanstalt en ytterligare samordningsuppgift.

Ansvar i förhållande till regeringen

I Försvarets radioanstalts huvudansvar ingår vidare att ansvara för cybersäkerhetscentrets verksamhet i förhållande till regeringen. Försvarets radioanstalts huvudman är vid försvarsdepartementets enhet för försvarsunderrättelser. En del av NCSC:s rapportering kommer alltså gå via Försvarets radioanstalt till enheten för försvarunderrättelser. Försvarets radioanstalts myndighetsdialog, som också kommer röra centret, sker likaså med enheten för försvarsunderrättelser. Cyberfrågorna och NCSC:s verksamhet faller dock under enheten för cyber- och hybridfrågors ansvar. Därför behöver en ytterligare dialogkanal mellan centret och denna enhet och ansvarigt statsråd etableras för att underlätta effektiv myndighetsstyrning och återrapportering. Även andra departement, bland annat justitiedepartementet som huvudman för Polismyndigheten och Säkerhetspolisen och finansdepartementet som huvudman för Post- och telestyrelsen, behöver hållas kontinuerligt informerade om verksamheten i centret.

Försvarets radioanstalt ska ansvara för gemensamma administrativa stödfunktioner och lämpliga lokaler

NCSC saknar nu vissa administrativa stödfunktioner, ändamålsenliga lokaler och tekniska system för en fullt utvecklad och samlokaliserad verksamhet.

I Försvarets radioanstalts huvudansvar ingår att säkerställa att centret har de administrativa stödfunktioner som verksamheten behöver, bland annat ett kansli. I ansvaret ingår även att se till att centret har tillgång till ändamålsenliga och säkra lokaler samt gemensamma tekniska system. Det bör i sammanhanget noteras att de olika myndigheterna har olika långtgående krav på bland annat säkerhetsskydd och it-system (inklusive system för hantering av information som är hemlig), vilket innebär att centrets lokaler måste anpassas för varje myndighets särskilda behov.

Den lokal som nu är under projektering kommer först att kunna tas i bruk om flera år. Innan dess behöver verksamheten bedrivas i den nuvarande tillfälliga lokalen. Försvarets radioanstalts ansvar omfattar även att säkerställa att verksamheten kan bedrivas i denna lokal. Försvarets radioanstalt bör därför säkerställa att nödvändiga överenskommelser för detta ingås med MSB som nu förfogar över och ansvarar för denna lokal.

Utredningen anser också att Försvarets radioanstalt bör söka en mindre men centralt belägen lokal där samverkan med en vidare krets aktörer enkelt kan ske och olika former av utåtriktad verksamhet kan bedrivas. En sådan lokal är särskilt viktig för att göra ett fördjupat samarbete med näringslivsaktörer möjligt. Lokalen behöver inte möta samma höga krav på säkerhet som centrets andra lokaler.

Ett center med en egen profil

Som nämnts ovan ska NCSC vara en del av Förvarets radioanstalt och dra nytta av dess strukturer och starka organisation. Men uppgifterna och målgrupperna gör det viktigt att centret har en egen särskild, mer utåtriktad och öppen profil. Den utåtriktade profilen är central för att centret ska kunna fullgöra uppgiften att vara nationell plattform för privat- och offentlig samverkan och utgöra en samlad kontaktpunkt för frågor som rör informationssäkerhet och cybersäkerhet. Sådan profilering av cybersäkerhetscenter som är del av signalspaningsmyndigheter har skett i flera andra länder. Det har redan nämnts i avsnitt 4.2 att det brittiska cybersäkerhetscentret är en del av GCHQ men har en utåtriktad profil och ett annat arbetssätt än GCHQ i övrigt. NCSC bör ha samma inriktning och ta fasta sådana framgångsrika exempel på konsekvent varumärkesbyggande.

5.2.1 Centerchefen

Utredningens förslag: Chefen för cybersäkerhetscentret ska anställas av regeringen. Chefen ska vara direkt underställd och rapportera till generaldirektören för Försvarets radioanstalt.
Utredningens bedömning: Chefen bör bland annat företräda centret och verksamhetsområdet samt leda verksamheten mot uppsatta mål.

Det nya cybersäkerhetscentret ska ha en chef som anställs av regeringen och som är direkt underställd chefen för Försvarets radioanstalt. Detta ska framgå av förordningen med instruktion för Försvarets radioanstalt. Denna konstruktion borde inte medföra några större förändringar i Försvarets radioanstalts organisations- och ledningsstrukturer i övrigt.

Vanligen anställs endast myndighetschefer och överdirektörer av regeringen men många myndigheter har chefer för avdelningar eller funktioner som utses av regeringen, till exempel chefen för Center mot våldsbejakande extremism och chefen för Polismyndighetens avdelning för särskilda utredningar. Vissa anställningar inom Försvarsmakten, bland annat som general och amiral beslutas också av regeringen.[64]

Att chefen anställs av regeringen visar på det nya centrets betydelse, den kraftsamling som nu sker och vikten av fortsatt myndighetssamverkan. Regeringen får därmed också möjlighet att välja en person med förutsättningar att klara uppgiften.

Utredningen anser att chefen och företrädaren för centerverksamheten måste ha lång erfarenhet av strategiskt ledarskap, hög integritet och kunna nå ut till och bygga förtroende bland nya målgrupper och samarbetspartners. Uppgiften att förklara svenska informationssäkerhets- och cybersäkerhetsintressen i olika sammanhang samt representera centret och sektorn i olika samarbetsforum och sammanslutningar förutsätter också goda sakkunskaper. Dessutom behöver chefen vara en god

[64] 7 och 12 §§ förordningen (2016:1201) med instruktion för Brottsförebyggande rådet, 2 b § polislagen och 39 § förordningen (2022:1718) med instruktion för Polismyndigheten samt 24 § förordningen med instruktion för Försvarsmakten.

kommunikatör och van vid mediakontakter. Centerchefens mandat ska vara större och tydligare definierat. I chefens uppgifter ska ingå att:

- ansvara för den operativa verksamheten i NCSC och leda operativ samverkan mellan centermyndigheterna,
- företräda centret och sektorn samt delta i olika svenska och internationella samarbetsforum och sammanslutningar,
- utarbeta styrdokument för centrets verksamhet utifrån uppsatta mål och verksamhetens behov,
- upprätta underlag till verksamhetsplanering, budgetunderlag och årsredovisning,
- leda bemanningsplanering och rekrytering av personal till NCSC och samordning med andra centermyndigheter,
- rapportera till generaldirektören för Försvarets radioanstalt och
- hålla det strategiska samverkansrådet informerat om verksamheten.

5.2.2 Beslutsfattande i NCSC

Utredningens bedömning: Det behövs inte någon särskild reglering av hur beslutsfattande ska ske inom ramen för NCSC.

Beslut i verksamheten måste kunna tas snabbt, effektivt och med lagligt stöd. Verksamheten måste därför bedrivas i enlighet med en tydlig arbets- och delegationsordning. När NCSC blir en del av Försvarets radioanstalt kommer många delar av verksamheten att kunna bedrivas i enlighet med Försvarets radioanstalts styrdokument. Med detta följer tydligare ansvar, kortare beslutsvägar och mer rationella arbetsprocesser. Detta gäller även för saker som upphandling och diarieföring.

I rättsligt hänseende kommer NCSC bli en del av Försvarets radioanstalt som är en förvaltningsmyndighet. Förvaltningslagen (2017:900), FL, kommer därmed att gälla även för centret. Större delen av FL gäller dock enbart vid ärendehandläggning och inte vid faktiskt handlande. Ett ärende kännetecknas av att det regelmässigt avslutas genom ett beslut av något slag som innebär faktiska verkningar för någon.[65] Med faktiskt handlande avses att myndigheten vidtar en viss faktisk åtgärd. Att en myndighet till exempel lämnar upplysningar och råd utgör faktiskt handlande och inte beslut i FL:s mening, även om den information som lämnas kan påverka mottagarens handlande.[66]

NCSC:s uppgifter innefattar bland annat att förmedla råd och stöd, producera lägesuppfattningar samt vara en plattform för samverkan mellan offentlig och privat verksamhet, vilket inte är ärendehandläggning.[67] Eftersom NCSC inte kommer att ha någon reglerande funktion eller några uppgifter som innebär att centret ska arbeta med myndighetsutövning kommer centret mycket sällan tillämpa förvaltningslagens bestämmelser

[65] Prop. 2016/17:180, *En modern och rättssäker förvaltning – en ny förvaltningslag,* s. 286.
[66] Prop. 2016/17:180, s. 24–25.
[67] Se avsnitt 5.1.1 och bilaga 1 för ytterligare beskrivning av centrets uppgifter.

om ärendehandläggning.[68] De eventuella förvaltningsbeslut som kan behöva fattas kan därför fattas av personer anställda vid Försvarets radioanstalt och som enligt Försvarets radioanstalts arbetsordning delegerats rätten att fatta beslut. Detta förutsätter inte någon särskild reglering.

5.3 Övriga centermyndigheters medverkan och bidrag

Utredningens förslag: Den verksamhet som centermyndigheterna bedriver som kan utföras inom ramen för det Nationella cybersäkerhetscentret *ska* utföras inom ramen för centret. Genom sådan kraftsamling till NCSC kan den samlade informationssäkerhets- och cybersäkerhetförmågan höjas.

Den ursprungliga idén med centret var att genom samverkan mellan sju utvalda myndigheter med unika kompetenser och resurser skapa mervärde och höjd förmåga. Men någon ledande eller huvudansvarig myndighet utsågs inte. Som framgår av avsnitt 3.2 har i stället fyra myndigheter (Försvarets radioanstalt, Försvarsmakten, MSB och Säkerhetspolisen) haft i uppdrag att ha fördjupad samverkan, och de övriga tre (Försvarets materielverk, Polismyndigheten samt Post- och telestyrelsen) getts möjlighet att medverka i verksamheten.

Utredningen anser att uppdelningen i två kategorier – fördjupad samverkan och medverkan – varit ett grundläggande problem för styrning, ledning och engagemang. Alla myndigheterna måste fortsättningsvis anses lika viktiga och förväntas bidra till verksamheten. Detta innebär inte att medverkan och bidrag måste vara identiska. Vissa myndigheter har inom sitt instruktionsenliga verksamhetsområde flera verksamheter som kan kopplas till cybersäkerhetscentret, medan andra endast har en eller ett fåtal. Det viktiga är i stället att den informationssäkerhets- och cybersäkerhets-verksamhet som myndigheterna *kan* leverera inom ramen för centret också *ska* levereras inom ramen för centret. Först då kan hela området få nödvändig täckning, synergier skapas och parallella strukturer undvikas. Försvarets radioanstalt får som huvudansvarig för centret och verksamhet en viktig roll att uppmärksamma och agera om centrets samtliga uppgifter och verksamheter trots allt inte täcks eller principen inte respekteras.

Försvarets radioanstalts huvudansvar innebär inte att Försvarets radioanstalt tar över någon annan myndighets uppgifter eller verksamhets-område i centret.[69] Om den incident eller händelse som ska hanteras är av sådan natur att den faller in under NCSC:s verksamhetsområde bör hanteringen i så stor utsträckning som möjligt ske inom ramen för centerverksamheten i enlighet med principen att den verksamhet som kan utföras inom ramen för centret ska utföras inom ramen för centret.

[68] Vissa bestämmelser om grunderna för god förvaltning gäller dock även i annan förvaltningsverksamhet än ärendehandläggning, se 5–8 §§ FL.
[69] Jfr SOU 2004:23, s. 85.

5.3.1 Skyldighet att medverka och bidra

Utredningens förslag: Centermyndigheternas skyldighet att medverka i och bidra till cybersäkerhetscentret inom ramen för sina verksamhetsområden ska regleras i varje myndighets instruktion.
Utredningens bedömning: I nuläget finns inget ytterligare behov av förtydligade uppgifter eller befogenheter men NCSC bör få i uppdrag att utvärdera om sådana förtydliganden senare behövs.

För att centret ska kunna drivas effektivt och utvecklas krävs att centermyndigheterna bidrar med resurser som centret behöver.

Skyldigheten att bidra ska framgå av respektive myndighets instruktion. Utredningen har övervägt hur en sådan reglering bör utformas för göra tydligt vad som förväntas av varje myndighet, tillåta nödvändiga anpassningar och möjliggöra särskilda tillskott vid speciella insatser, till exempel vid större incidenter.

Utredningen anser att det är enkelt att i reglering fastslå att varje myndighet ska bidra till verksamheten men svårt att reglera på vilket sätt utan att därmed begränsa centrets förmåga att hantera ändrade förutsättningar. Utredningen anser därför att regleringen ska vara förpliktande men inte detaljerad. Den ska också vara likalydande för de deltagande myndigheterna. Det finns visserligen risk att myndigheterna att myndigheterna kan göra olika tolkningar av sin skyldighet att bidra, men denna bör minska med ökad gemensam planering. Sådan planering skulle också ge myndigheterna bättre möjlighet att prioritera internt. Försvarets radioanstalt som huvudansvarig för centret och ledare av det strategiska samverkansrådet får en viktig uppgift att se till att förutsättningarna för sådan planering finns.

Denna strategiska planering behöver ske med utgångspunkt i regeringens prioriteringar inom informationssäkerhets- och cybersäkerhetsområdet. Planering med utgångspunkt i regeringens prioriteringar förutsätter dock att prioriteringarna är samstämmiga och kommer till likalydande uttryck i regleringsbrev och myndighetsdialoger. Myndigheterna och centret har också ansvar att tydligt påpeka när så inte är fallet, eller när de ser att ytterligare resurser behövs.

Regleringen i förordningen ska således vara av innebörden att centermyndigheterna ska fortsätta att medverka i och bidra till verksamheten inom ramen för sina verksamhetsområden. Samordning av respektive myndighets bidrag till verksamheten i NCSC ska ske i det strategiska samverkansrådet, se avsnitt 5.4.1.

Av utredningsuppdraget framgår att utredningen ska analysera om centermyndigheterna är i behov av förtydligade uppgifter och befogenheter för att NCSC:s uppdrag ska kunna genomföras på ett bättre och mer effektivt sätt än vad som görs idag.[70] Vad gäller Försvarets radioanstalt bedömer utredningen att det föreligger behov av förtydligade uppgifter och befogenheter för att myndigheten ska kunna ta sitt nya huvudansvar, se avsnitt 5.2.

[70] Regeringsbeslut Fö2023/01606 s. 2.

För övriga centermyndigheter kan utredningen inte se behov av några ytterligare förtydliganden utöver de föreslagna tilläggen med innebörd att myndigheterna ska bidra till och medverka i cybersäkerhetscentrets verksamhet inom ramen för sina verksamhetsområden. Centret bör dock få i uppdrag att senare utvärdera om centret eller de deltagande myndigheterna har det rättsliga handlingsutrymme som verksamheten kräver.

5.3.2 Myndigheternas författningsreglerade uppgifter vid attacker och incidenter

Utredningens förslag: Centermyndigheter som har i uppgift att ge stöd vid hanteringen av cyberhot eller betydande it-incident ska få stöd från andra centermyndigheter i den utsträckning det är lämpligt.

Flera centermyndigheter har författningsreglerade uppgifter i fråga om exempelvis incidenthantering. Försvarets radioanstalt ska till exempel ge stöd vid nationella kriser med it-inslag och MSB har i uppdrag att ansvara för en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter (CERT-SE).[71] Även Försvarsmakten och Säkerhetspolisen har författningsreglerade uppgifter kopplade till incidenthantering.

Myndigheter som har sådana författningsreglerade uppgifter bör i så stor utsträckning som möjligt utföra dessa inom ramen för centerverksamheten. När det är nödvändigt och rättsligt möjligt bör de också få stöd från andra centermyndigheter att hantera situationen. Sådant stöd kan exempelvis bli aktuellt om händelsen har kopplingar till flera centermyndigheters operativa uppgifter.

5.3.3 CSIRT-funktionen CERT-SE

Utredningens bedömning: Verksamheten i CERT-SE bör så snart som möjligt överföras till Försvarets radioanstalt och NCSC. Hur denna överföring ska gå till bör utredas. Under tiden bör verksamheterna bedrivas så integrerat som möjligt.

MSB:s verksamhet inom ramen för Sveriges nationella CSIRT, CERT-SE, har beskrivits i avsnitt 3.3.4. Det finns flera överlappningar och oklara gränssnitt mellan den nationella CSIRT-funktionen och cybersäkerhetscentret. Bland annat har både NCSC och CSIRT-funktionen i uppgift att förebygga och hantera incidenter och att tillhandahålla lägesuppfattningar.[72]

[71] Jfr 4 § förordningen med instruktion för Försvarets radioanstalt och 11 b § förordningen med instruktion för Myndigheten för samhällsskydd och beredskap.
[72] Jfr 11 b § förordningen med instruktion för Myndigheten för samhällsskydd och beredskap, https://cert.se/om-cert-se/, senast hämtad 2024-04-09 samt regeringsbeslut Fö2023/01606 s. 3.

I betänkandet om genomförande av NIS2-direktivet föreslås verksamheten i CSIRT:en utökas ytterligare.[73] Bland annat föreslås CSIRT:en får ansvar att övervaka och analysera cyberhot och incidenter samt tillhandahålla varningar och information. CSIRT:en ska också ta emot incidentrapporter samt vidta åtgärder, erbjuda stöd och tillhandahålla lägesuppfattningar. Det föreslås vidare att CSIRT:en ska upprätta samarbetsförbindelser med relevanta intressenter inom privat och offentlig sektor samt bidra till samverkan rörande cybersäkerhet. MSB föreslås få ansvar för den nationella CSIRT:en och bli nationell cyberkrishanteringsmyndighet.[74]

Utredningen konstaterar att om dessa förslag genomförs kommer överlappningarna bli ännu fler och gränsdragningsproblemen ännu tydligare. Både privata och offentliga intressenter tycker redan nu att ordningen med två entiteter med liknande uppgifter är förvirrande och ineffektiv. Många anser att det är svårt eller oklart att veta vart man ska vända sig när behov uppstår. Utredningen bedömer därför att starka praktiska, resursekonomiska och säkerhetsrelaterade skäl talar för att verksamheterna sammanförs vid en myndighet. Den samlade svenska nationella förmågan att förebygga, upptäcka och hantera cyberattacker och betydande it-incidenter skulle därmed stärkas. Även ansvarsutkrävande skulle väsentligt underlättas.

Försvarsberedningen har i delbetänkandet *Kraftsamling* anfört att det kan övervägas att det ansvar för informationssäkerhet och cybersäkerhet som idag finns på MSB ska organiseras som en ny myndighet.[75] Utredningen anser emellertid att knappa resurser, i synnerhet kompetens, utnyttjas mer effektivt om verksamheten hos MSB i stället överförs till NCSC vid Försvarets radioanstalt och att Försvarets radioanstalt utses till nationell cyberkrishanteringsmyndighet.

Vad gäller de tekniska förutsättningarna för Försvarets radioanstalt att ansvara för den verksamhet som nu utförs av den nationella CSIRT:en och den verksamhet som kan tillkomma enligt NIS2-direktivet noterar utredningen att Försvarets radioanstalt är Sveriges expertmyndighet för teknisk it-säkerhet och har den tekniska förmåga som krävs.[76]

De närmare rättsliga, organisatoriska och praktiska förutsättningarna för en verksamhetsöverföring, bland annat hur en sådan skulle påverka MSB:s krishanterings-, informationssäkerhets- och cybersäkerhetsarbete och särskilt de ansvarsområden som följer av NIS-direktiven, bör dock utredas närmare i ett annat sammanhang.[77]

Vad gäller den viktiga frågan vilka incidenter som hanteras inom centret så bör uppmärksammas att utredningen i beskrivningen av centrets uppdrag valt att använda samma begrepp, *betydande* it-incidenter, och att utgå från samma breda definition, som NIS2-utredningen föreslår ska gälla

[73] SOU 2024:18, s. 15–20.
[74] SOU 2024:18, s. 61–63 och 122.
[75] Ds 2023:34, *Kraftsamling – Inriktningen av totalförsvaret och utformningen av det civila försvaret,* s. 235.
[76] Jfr angående vilka krav som ställs på den nationella CSIRT:en artikel 10 och 11 i NIS2-direktivet samt SOU 2024:18 s. 295–310.
[77] Det kan noteras att flera andra jämförbara länder valt att organisera verksamheten på ett liknande integrerat sätt. Bland annat i Danmark är den nationella CSIRT-funktionen och det nationella cybersäkerhetscentret en del av signalspaningsmyndigheten, se avsnitt 4.3.

för den nationella CSIRT:en. Utredningen är visserligen medveten om att CERT-SE:s uppdrag kan uppfattas som innefattande ännu mer då MSB:s instruktion inte innehåller någon gradering av de incidenter som CERT-SE ska förebygga och hantera.[78] Men utredningen anser att en överföring av all CERT-SE:s verksamhet ändå är möjlig eftersom utredningens förslag om centrets uppgifter inte är uttömmande, se avsnitt 5.1.1.

Under tiden fram till en verksamhetsöverföring kan ske bör myndigheterna bedriva en så nära och integrerad verksamhet som lagstiftning och myndighetsuppdrag tillåter. NCSC och CERT-SE finns redan i samma lokal, så de praktiska förutsättningarna bör vara goda. Särskilda överenskommelser som underlättar en nära verksamhet bör ingås mellan Försvarets radioanstalt och MSB.

5.3.4 Andra myndigheter med tangerande uppdrag

Utredningens bedömning: NCSC bör upparbeta nära samarbeten även med andra relevanta myndigheter. Myndigheten för psykologiskt försvar bör bli en centermyndighet.

Den nuvarande konstruktionen med sju centermyndigheter är en följd av det tidigare samarbetet inom ramen för samverkansgruppen för informationssäkerhet (SAMFI). Under utredningens gång har flera intressenter påtalat att det finns ytterligare myndigheter som är värdefulla för cybersäkerhetscentret att skapa ett närmare samarbete med, däribland myndigheter i beredskapssektorerna. Ett mindre antal myndigheter har också föreslagits bli medlemmar i centret, däribland Myndigheten för psykologiskt försvar (MPF), Myndigheten för digital förvaltning (Digg) och Totalförsvarets forskningsinstitut (FOI).

Utredningen håller med om att cybersäkerhetscentret måste knyta till sig och upparbeta samarbeten med ytterligare myndigheter. Detta följer också av uppgiften att utveckla och stärka arbetet för att förebygga, upptäcka och hantera cyberattacker och större it-incidenter, liksom av uppgiften att vara en samverkansplattform.

Särskilt om MPF

MPF följer i sitt operativa arbete utländska antagonistiska aktörer och påverkansaktiviteter som kan riktas mot Sverige. I verksamheten ingår även att identifiera effekter av påverkansaktiviteter, bland annat inom cyberområdet. MPF har också behov av information från aktörer som arbetar med att upptäcka och attribuera cyberrelaterade hot och incidenter för att analysera omfattning, inriktning och konsekvenser av påverkansaktiviteter, och för att kunna samordna bemötandet av dessa.

Utredningen bedömer att det finns ömsesidiga fördelar med en nära operativ samverkan mellan MPF och NCSC. Sådan samverkan kan bland annat bestå i utbyte av information och bedömningar i syfte att skapa lägesuppfattningar rörande allvarliga antagonistiska hot mot Sverige.

[78] Jfr 11 b § förordningen med instruktion för Myndigheten för samhällsskydd och beredskap.

Utredningen bedömer därför att MPF så snart som möjligt bör bli en centermyndighet.

5.4 Samverkan inom NCSC

Utredningens bedömning: Samverkan är helt nödvändig för NCSC:s verksamhet. Men framgångsrik samverkan förutsätter en gemensam syn på vad som ska åstadkommas. NCSC bör få i uppdrag att formulera en vision och tydliga verksamhetsmål.

Det finns en generell skyldighet för myndigheter att samverka med andra myndigheter inom sitt verksamhetsområde.[79] Men utredningen bedömer att denna generella skyldighet inte är tillräcklig för att säkerställa att samverkan i NCSC fungerar på ett ändamålsenligt sätt. Ytterligare reglering är därför nödvändig.

Utredningen anser att centrets myndighetsöverskridande verksamhet förutsätter en hög grad av samverkan. Men erfarenheten från centrets verksamhet visar också att reglering av samverkan måste struktureras så att den sker när det verkligen behövs och att den inte bromsar eller hindrar den dagliga eller operativa verksamheten. Centret behöver därför en genomtänkt och gemensam vision och tydliga verksamhetsmål. Centret behöver även beakta vad som ska åstadkommas genom samverkan, hur samverkan på olika nivåer ska gå till och hur varje myndighet ska bidra. Utredningen anser att NCSC snarast bör få i uppdrag att genomföra detta arbete.

5.4.1 Samverkan på strategisk nivå

Utredningens förslag: Samverkan på strategisk nivå ska regleras i förordningen om nationellt cybersäkerhetscenter. Samverkan ska ske i det strategiska samverkansrådet. Rådet ska ledas av generaldirektören för Försvarets radioanstalt. I rådet ska centermyndigheternas generaldirektörer eller chefer på motsvarande nivå ingå.

Utredningen föreslår att samverkan kring bland annat övergripande och långsiktiga inriktningar, mål, resurssättning, resultatbedömning och återrapportering ska ske i ett *strategiskt samverkansråd.* Rådet ska regleras i förordningen om Nationellt cybersäkerhetscenter och bestå av generaldirektörerna eller chef på motsvarande nivå för de sju centermyndigheterna. Rådets arbete ska ledas och samordnas av generaldirektören för Försvarets radioanstalt. I rådets uppgifter ska ingå att ge råd till generaldirektören för Försvarets radioanstalt i frågor rörande den strategiska ledningen av cybersäkerhetscentrets verksamhet samt att bistå och ge råd vid beredning av bland annat budgetunderlag, verksamhetsplanering, årsrapporter och annan rapportering och redovisning till regeringen.

[79] Jfr 8 § FL och 6 § andra stycket myndighetsförordningen (2007:515).

Uppgiften att leda samordningen i rådet innebär inte att Försvarets radioanstalt ska styra över de andra myndigheternas bidrag till verksamheten. Sådana beslut fattas alltid av varje myndighet för sig.[80] Men generaldirektören för Försvarets radioanstalt har en viktig uppgift att se till att alla rådets medlemmar arbetar målmedvetet och effektivt för att säkerställa att centret får de resurser som verksamheten faktiskt behöver.

Då en välfungerande samverkan på ledningsnivå och ett gott samtalsklimat är grundläggande för en fungerande verksamhet i centret så ska det strategiska samverkansrådet verka för att överbrygga olikheter i myndighetskultur och olika utgångspunkter. Den föreslagna visionen och verksamhetsmålen kan förutses underlätta detta arbete, se avsnitt 5.4. I detta arbete bör rådet beakta andra framgångsrika exempel, bland annat det myndighetsgemensamma arbetet mot organiserad brottslighet.[81]

Det strategiska samverkansrådet ska också initiera och underlätta genomförandet av analyser, planering och andra åtgärder som behövs för att cybersäkerhetscentret så snart som möjligt ska kunna inleda sin verksamhet som en del av Försvarets radioanstalt.

5.4.2 Samverkan på operativ nivå

Utredningens bedömning: Samverkan på operativ nivå är nödvändig men bör inte regleras i förordning. Formerna för sådan samverkan bör i stället bestämmas utifrån verksamhetens behov. Det bör senare utvärderas om utformningen av samverkan är ändamålsenlig eller om det finns behov att reglera samverkansformer även på operativ nivå.

Ändamålsenlig och effektiv operativ samverkan behövs i NCSC. Utredningen har övervägt om formerna för operativ samverkan ska regleras särskilt. En fördel med reglering kan vara att den gör det tydligare varför samverkan ska ske, i vilket sammanhang och med vem. Men utredningen anser att det ännu saknas kunskaper om vilken samverkan som faktisk kommer behövas och hur den bör genomföras, och anser det därför olämpligt att redan nu reglera detta. Cybersäkerhetscentret bör i stället skapa egna strukturer efter verksamhetens behov. Möjligen kan viss reglering vara befogad för att möjliggöra speciella samverkansbehov som kan uppstå vid allvarliga eller extraordinära händelser.

Utredningen vill framhålla vikten av att operativ samverkan sker både kontinuerligt och i anslutning till specifika händelser. Inom ramen för denna samverkan bör formerna för incidenthantering utformas.

Om händelser inträffar som kräver gemensam och snabb respons är det viktigt att etablerade samverkansformer redan finns i verksamheten. Myndigheterna bör till exempel vid behov kunna samverka om personal- och resurstillskott till centerverksamheten med kort varsel. NCSC måste därför ha en smidig operativ samverkan som kan aktiveras snabbt och effektivt. De personer som representerar myndigheterna i den operativa

[80] Jfr SOU 2004:23, s. 85.

[81] https://polisen.se/om-polisen/polisens-arbete/organiserad-brottslighet/myndighetsgemensam-satsning-mot-organiserad-brottslighet/, senast hämtad 2024-04-10.

samverkan bör vara resursägare som snabbt kan avdela resurser till verksamheten när sådana behov uppstår. Det eventuella behovet av reglering av formerna för operativ samverkan bör följas upp vid en senare utvärdering av centrets verksamhet.

5.4.3 Deconfliction

Utredningens bedömning: NCSC bör få i uppdrag att utarbeta former för deconfliction i verksamheten. Både skyddsintresset och underrättelseintresset bör vara adekvat representerat.

Med *deconfliction* avses den intresseavvägning som behöver göras mellan intresset av att hålla viktig offensiv kunskap hemlig så att den kan nyttjas i den egna verksamheten, och intresset att delge kunskap till verksamheter som utsatts för cyberangrepp eller som riskerar att bli utsatta. Att det kan uppstå svårhanterliga motsättningar mellan dessa intressen vid exempelvis incidentrapportering och informationsdelning är väl känt.[82] Sådana intressemotsättningar kan förväntas även i NCSC:s verksamhet. Utredningen bedömer därför att en tydlig process för *deconfliction* behöver skapas.

Utredningen har övervägt om denna bör regleras i förordning men kommit fram till att ändamålsenliga former för *deconfliction* bäst skapas inom ramen för den operativa verksamheten. I detta arbete, liksom i processens senare tillämpning, är det viktigt att det noga beaktas att både skyddsintresset och underrättelseintresset ska vara adekvat representerat. Vid en myndighet vars övriga uppdrag har ett starkt underrättelseintresse finns annars stor risk att underrättelseintresset blir styrande.

5.5 Näringslivet, offentliga aktörer och andra intressenter

Utredningens bedömning: Cybersäkerhetscentret bör stärka och fördjupa samverkan med näringslivet och andra privata och offentliga intressenter. NCSC bör därför få i uppdrag att utreda relevanta målgruppers förväntningar och behov, liksom hur intressenterna kan bidra till centrets verksamhet och mål.

Cybersäkerhetscentret bör även stärka och fördjupa samverkan med relevanta forskningsmiljöer, särskilt med Cybercampus Sverige.

Näringslivet och andra intressenter

I utredningens uppdrag anges att centret ska utgöra en nationell plattform för privat-offentlig samverkan. I uppdraget anges också att centret ska utgöra en samlad kontaktpunkt för frågor som rör informationssäkerhet

[82] Jfr SOU 2010:25, s. 38 och Nicander, *Cybersäkerhet måste formas på rätt sätt*, https://www.svd.se/a/Adv823/cybersakerhet-maste-formas-pa-ratt-satt, senast hämtad 2024-03-11.

och cybersäkerhet och förmedla råd och stöd avseende hot, sårbarheter och risker.

Som framgår av avsnitt 3.4 har cybersäkerhetscentret redan i uppgift att samla befintliga informationsinsatser riktade till näringslivet inom centrets ram så långt det är möjligt och centret bedriver redan idag samverkan med näringslivet inom olika sektorer.[83] Men bland annat Kungliga ingenjörsvetenskapsakademin och Försvarsberedningen anser att den nuvarande ambitionsnivån inte är tillräcklig och att näringslivets förväntningar och resurser måste tas bättre till vara.[84] Företrädare för näringslivets har i olika sammanhang uttryck att centermyndigheterna och NCSC inte är tillräckligt intresserade eller förmår dra nytta av den stora och ibland unika kunskap och kompetens som näringslivet besitter. Det har också påtalats att den informationsdelning som faktiskt sker är ensidig: staten tar emot information men ger ingenting tillbaka.[85]

NCSC bör därför arbeta kontinuerligt med att stärka strukturerna för informationsutbyte och annan samverkan med näringslivets intressenter. Här bör uppmärksammas att näringslivet inte är homogent och att olika aktörer därför har olika behov och förutsättningarna. Det är också viktigt att beakta att kategorin ”privata intressenter” även omfattar andra intressenter: ideella föreningar, trossamfund, politiska partier med flera.

Utredningen bedömer därför att NCSC bör ges i uppdrag att genomföra en systematisk kartläggning och analys av olika målgruppers behov och förutsättningar att bidra. Denna kartläggning ska ske i samverkan med representanter för företag, organisationer och offentliga intressenter. Analysen ska senare ligga till grund för förslag på ändamålsenliga och effektiva former för strukturerad privat-offentlig samverkan. Den ska också ligga till grund för ett mer effektivt informationsutbyte mellan centret och privata aktörer. Arbetet ska redan upparbetade och väl fungerande samverkansformer beaktas, till exempel Nationella Telesamverkansgruppen (NTSG)[86] och andra sektorsspecifika forum. Även centrets internationella motsvarigheters arbete, till exempel det norska partnerskapsprogrammet och det brittiska Industry100-programmet bör kunna vara inspiration vid utarbetandet av olika samverkansformer. Inom näringslivet finns även flera forum för hotinformation och delning av information kring incidenter där NCSC skulle kunna delta eller bidra med information. [87]

[83] Jfr Regeringsuppdrag Fö2023/00907.
[84] Kungliga ingenjörsvetenskapsakademin, *Cybersäkerhet för ökad konkurrenskraft*, 2022, s. 5 och Ds 2023:34 s. 235.
[85] Se bland annat RiR 2023:8, s. 52, 65 och 68, FOI-R—5546—SE, s. 69 samt https://www.techsverige.se/techagenda/stark-informations-och-cybersakerheten/, senast hämtad 2024-04-12.
[86] Gruppen består av myndigheter (bland annat Post- och telestyrelsen, Försvarsmakten och Trafikverket) samt operatörer med verksamhet som påverkar den kritiska nationella infrastrukturen för elektronisk kommunikation.
[87] Exempelvis finns inom flera branscher Malware Information Sharing Platforms (MISP).

Offentliga aktörer

Av utredningens uppdragsbeskrivning framgår att även offentligrättsliga aktörer, bland annat andra statliga myndigheter, regioner och kommuner, är intressenter och målgrupper i cybersäkerhetscentrets verksamhet.[88]

Vad gäller kommuner och regioner ansvarar dessa för viktiga delar av välfärden och grundläggande samhällsfunktioner. Dessa aktörer måste därför snabbt kunna både förmedla och nås av information när något händer. De kan också ha ett intresse att få bidra till och dra nytta av lägesuppfattningar och annan saklig och verifierad information.

I Norge inkluderas i partnerskapsprogrammet både näringslivsaktörer och offentliga intressenter. Det svenska cybersäkerhetscentret bör sträva efter en liknande lösning. Det är också viktigt att relevanta offentliga aktörer inkluderas i den kartläggning av målgrupper och deras olika behov som ska genomföras, se avsnittet ovan.

Akademin och forskarsamhället

Det finns ett ömsesidigt behov av fördjupat samarbete och samverkan mellan centret och olika akademiska verksamheter. Centret behöver bland annat kunna konsultera forskare och ha enkel tillgång till forskningsrön. Undervisning och forskning behöver likaså informeras av centret om verkliga problem och erfarenheter. Det är också viktigt att genom strukturerat samarbete mellan akademi och praktik bidra till den långsiktiga kompetensförsörjningen inom området.

Cybercampus Sverige vid Kungliga tekniska högskolan (KTH) är ett samarbete mellan universitet, yrkeshögskolor, institut, myndigheter och företag över hela Sverige. Dess syfte är att stärka både kompetensförsörjning och forskning inom cybersäkerhet och cyberförsvar.[89] Utredningen anser att NCSC bör bedriva organiserat samarbete och samverkan med Cybercampus Sverige inom ramen för centrets uppdrag. Utredningen anser också att NCSC bör upprätthålla goda kontakter och i relevanta fall bedriva samarbete med andra initierade forsknings- och undervisningsaktörer i Sverige och internationellt.

5.6 Internationella samarbeten

Utredningens förslag: Cybersäkerhetscentret ska övergripande koordinera och delta i internationella samarbeten kopplade till centrets verksamhet.

NCSC behöver vara representerat i internationella och regionala forum och delta i gränsöverskridande samarbeten. Vid en kommande överföring av verksamheten i CERT-SE till Försvarets radioanstalt och NCSC kan dessa behov förutses bli ännu större då verksamheten kommer att innehålla ännu mer internationellt och europeiskt samarbete. Även bilaterala

[88] Regeringsbeslut Fö2023/01606 s. 3.
[89] https://www.kth.se/om/nyheter/centrala-nyheter/sveriges-nya-cybercampus-invigt-1.1314934 senast hämtad 2024-03-21.

överenskommelser kan aktualisera behov internationell samverkan för NCSC.[90]

NCSC:s möjligheter att delta i internationell samverkan bestäms av de möjligheter som centermyndigheterna har att verka internationellt. Centermyndigheternas internationella ansvar följer av deras instruktioner och annan lagstiftning, vilket innebär att myndigheterna och särskilt Försvarets radioanstalt har en viktig roll i att säkerställa att NCSC får möjlighet att utföra sina internationella och gränsöverskridande uppgifter på ett ändamålsenligt och effektivt sätt.

Regeringen kan också underlätta NCSC:s internationella arbete genom att bestämma att Sverige ska företrädas av Försvarets radioanstalt och NCSC i relevanta internationella och regionala sammanhang.

5.7 NCSC:s fortsatta utveckling

Utredningens bedömning: Flera aspekter av NCSC:s uppgifter och verksamhet behöver följas upp och utvecklas ytterligare. Verksamheten behöver också kontinuerligt anpassas till nya uppgifter och förutsättningar.

Planera för uppföljning och kontinuerlig verksamhetsutveckling

NCSC är nu föremål för genomgripande förändringar för att bättre svara mot nya och högre förväntningar. Målet är att centret ska bli navet i det nationella cybersäkerhetsarbetet. Hur väl de föreslagna styrnings-, lednings- och organisationsformerna svarar mot dessa förväntningar behöver följas upp. Utredningen anser att en verksamhetsöversyn bör genomföras inom något år.

Dialog om bredare uppgifter

Omvärldsförändringar, lagstiftning, EU-reglering eller politiska beslut kan göra att regeringen vill bredda NCSC:s uppgifter eller betona vissa inriktningar ytterligare. Det kan bland annat finnas skäl att göra exempelvis certifiering till en mer framträdande del av verksamheten. Centrets ledning kan också se behov av justerade uppgifter för att möta särskilda behov. En kontinuerlig dialog om uppgifternas innehåll är därför viktig.

Utökade myndighetsuppdrag

Det finns olika uppfattningar om centermyndigheternas nuvarande instruktionsenliga uppdrag gör det möjligt att bidra till alla centrets uppgifter. En kartläggning och analys kan därför behöva genomföras, och förslag till förtydliganden och förändringar presenteras.

[90] Jfr till exempel bilateral överenskommelse med Frankrike om förnyat strategiskt innovationspartnerskap, https://www.regeringen.se/rattsliga-dokument/sveriges-internationella-overenskommelser/2024/01/fornyat-strategiskt-innovationspartnerskap-mellan-sverige-och-frankrike-for-hallbara-digitala-och-motstandskraftiga-samhallen/, senast hämtad 2024-04-08.

Särskilda målgruppers förväntningar och behov

Centret kapacitet kommer gradvis öka. Fler målgruppers behov kan då tillgodoses. Den föreslagna målgruppskartläggningen och rekommendationerna bör därför omfatta ett brett spektrum av sannolika och möjliga aktörer.

Underlätta gemensamma insatser

Det bredare uppdraget med allriskperspektiv skapar fler möjligheter att arbeta tillsammans näringslivet, akademin och andra intressenter utanför myndighetssfären. Det är viktigt att centret tar till vara dessa möjligheter, och även beaktar att vad nya aktörer, till exempel mindre företag och ideella föreningar, kan tillföra verksamheten.

Etablera ett Security Operations Center

Centret kommer med stor sannolikhet att behöva ett eget Security Operations Center (SOC) som kan identifiera, analysera och motverka digitala hot. Detta måste utformas med NCSC:s särskilda uppdrag och behov för ögonen. Det nödvändiga kartläggnings- och analysarbetet behöver inledas snart.

6 Konsekvenser och finansiering

6.1 Allmänt

Att en utredare fått i uppdrag att föreslå en mer ändamålsenlig och effektiv ledning, organisering och styrning av NCSC och lämna förslag på en ny reglering beror på att den förväntade effekten av NCSC:s verksamhet inte uppnåtts.

Utredningen anser att den föreslagna regleringen och styrningsmodellen ger bättre förutsättningar att bedriva verksamheten på ett effektivt och ändamålsenligt sätt. Om inga åtgärder vidtas kommer stora hinder för en effektiv och ändamålsenlig verksamhet att kvarstå, bland annat komplicerade administrativa processer, osäkerhet om beslutsmandat och problem med koordination och samordning. Detta skulle i sin tur innebära hinder för centrets och samhällets förmåga att hantera cyberhot och betydande it-incidenter.

De som berörs av utredningens förslag är Försvarets radioanstalt, Försvarets materielverk, Försvarsmakten, MSB, Polismyndigheten, Säkerhetspolisen samt Post- och Telestyrelsen. Några andra aktörer påverkas inte i någon väsentlig omfattning.

6.2 Konsekvenser för informationssäkerheten och cybersäkerheten i Sverige

Utredningens bedömning: En mer ändamålsenlig och effektiv styrning och organisation av NCSC kommer att leda till förbättrad förmåga att förebygga, upptäcka och hantera cyberhot och betydande it-incidenter. På sikt kommer detta leda till en högre nivå av informationssäkerhet och cybersäkerhet i samhället.

De föreslagna förändringarna i ledning och styrning av det nationella cybersäkerhetscentrets verksamhet innebär en tydligare ansvarsuppdelning mellan Försvarets radioanstalt och de övriga centermyndigheterna. Den osäkerhet som tidigare kringgärdat denna fråga bör alltså minska. Det blir också möjligt att fokusera samverkan på centerverksamhetens behov i stället för grundläggande verksamhetsförutsättningar.

Att centermyndigheternas information och relevanta verksamheter koncentreras till NCSC innebär färre administrativa och praktiska problem och att begränsade resurser – inte minst personal – utnyttjas bättre. Med en mer effektiv och välfungerade verksamhet i NCSC ökar cybersäkerheten i samhället och stora kostnader kopplade till cyberhot och incidenter undviks.

6.3 Konsekvenser och kostnader för Försvarets radioanstalt

Utredningens bedömning: Att NCSC blir en del av Försvarets radioanstalt placerar ett tydligt ansvar hos en aktör. Med detta följer behov av anpassningar och ytterligare medel. Av de medel som tidigare har tilldelats Försvarets radioanstalt, MSB, Försvarsmakten och Säkerhetspolisen för driften av NCSC bör en betydande del framöver tilldelas Försvarets radioanstalt.

För Försvarets radioanstalt innebär utredningens förslag att myndigheten blir huvudansvarig för verksamheten och får ett nytt uppdrag och ett utökat verksamhetsområde. Detta uppdrag omfattar bland annat att leda den samordning och samverkan som verksamheten förutsätter, tillhandahålla gemensamma administrativa stödfunktioner och lämpliga lokaler och att förestå en öppnare och mer utåtriktad verksamhet. Det innebär att Försvaret radioanstalt behöver genomföra vissa förändringar i organisationen, nyanställa personal och i viss mån använda sig av nya och mer utåtriktade arbetssätt.

Av Totalförsvarspropositionen framgår att för 2024 tilldelas cybersäkerhetscentrets verksamhet 120 miljoner kronor. Dessa medel tilldelas Försvarets radioanstalt, Försvarsmakten, MSB och Säkerhetspolisen. För 2025 ska enligt Totalförsvarspropositionen NCSC:s verksamhet tilldelas 150 miljoner.[91] Dessa medel täcker de kostnader som Försvarets radioanstalt förväntas ha för att vara huvudansvarig för verksamheten. Utredningen utgår från att medel kommer fortsätta tilldelas minst i samma omfattning. Försvarets radioanstalt beräknar att kostnaderna för den verksamhet som myndigheten anser NCSC bör ha kommer att öka årligen i takt med att verksamheten utvecklas till ett fullt utbyggt center.

Mot bakgrund av det större uppdrag som Försvarets radioanstalt kommer att ha och Försvarets radioanstalts egna beräkningar gör utredningen bedömningen att Försvarets radioanstalt kommer behöva tilldelas ytterligare medel för verksamheten i NCSC.

Utredningen bedömer att Försvarets radioanstalts större ansvar för cybersäkerhetscentret motiverar att en betydande del av de medel som hittills tilldelats Försvarets radioanstalt, Försvarsmakten, MSB och Säkerhetspolisen för driften av NCSC i stället fördelas till Försvarets radioanstalt.

[91] Prop. 2020/21:30 s. 126.

6.4 Konsekvenser och kostnader för övriga centermyndigheter

Utredningens bedömning: Den nya organisationen av NCSC innebär att samtliga centermyndigheter ska bedriva kravställd samverkan i NCSC inom sina nuvarande verksamhetsområden. Kostnaderna för denna, liksom för den medverkande personalen, är sådana att de nu ryms inom myndigheternas befintliga anslag.

Utredningen föreslår inte några utökade verksamhetsområden för de övriga sex centermyndigheterna. Att myndigheternas medverkan i cybersäkerhetscentret regleras i respektive myndighets instruktion innebär enbart ett förtydligande av redan rådande ordning och vad som följer av FL och myndighetsförordningen. Men för MSB kan konsekvenser följa av utredningens bedömning att närmare integration av CERT-SE ska ske i cybersäkerhetscentret. Även om vissa kostnader kan uppstå till följd av den närmare integrationen bedömer utredningen att dessa är begränsade och kan finansieras genom myndighetens befintliga anslag.

Vad gäller de övriga fem centermyndigheternas kostnader för medverkan i NCSC förväntas även dessa fortsättningsvis främst avse personalkostnader.

Av myndigheternas svar på regeringsuppdraget att inrätta cybersäkerhetscentret framgår att de beräknade kostnaderna för verksamheten som redovisas i underlaget är exklusive kostnader för den egna operativa personalen som ska tjänstgöra i centret. Personalen som är anställd vid myndigheterna och tjänstgör i centret är i regel inte anställd specifikt för centerverksamheten utan för myndighetens vanliga verksamhet. Av myndigheternas egna bedömningar av kostnaderna för verksamheten i NCSC kommer ett fullt utbyggt cybersäkerhetscenter med cirka 250 årsarbetskrafter dock innebära behov av nyrekrytering till både Försvarets radioanstalt och övriga myndigheter för att säkerställa en långsiktig utveckling av verksamheten.[92]

Ett fullt utbyggt cybersäkerhetscenter kommer dock inte att bli verklighet förrän den avsedda lokalen kan tas i bruk. Sannolikt dröjer detta flera år. Under denna tid kommer utvecklingsmöjligheterna för verksamheten att i viss mån vara begränsade.

Utredningen gör därför bedömningen att de närmaste årens personalkostnader kommer rymmas inom myndigheternas nuvarande anslag. Samtliga sex myndigheter kan därför i nuläget medverka i cybersäkerhetscentrets verksamhet inom ramen för sina befintliga anslag.

6.5 Konsekvenser för andra aktörer

Andra myndigheter och offentliga organ

Ett NCSC med bättre organisation, styrning och ledning samt en mer öppen profil skapar ökade möjligheter till samverkan med andra

[92] Svar på regeringsuppdrag Fö2019/01000/SUND, s. 9.

myndigheter och offentliga organ. Ett mer effektivt och operativt NCSC innebär också att fler offentliga aktörer kan bidra till och ta del av samordnade lägesbilder och annan viktig information.

NCSC förutses inte få någon reglerande roll, arbeta med tillsyn eller fatta beslut som påverkar andra offentliga organs verksamhet eller myndighetsutövning. Utredningens förslag och bedömningar innehåller alltså ingenting som får uppenbara kostnadsdrivande effekter för andra myndigheter och offentliga organ. Snarare kan den ökade förmåga och resiliens som förväntas av förslagen på sikt leda till lägre kostnader.

Företag

Många företag önskar att cybersäkerhetscentret ska samverka med näringslivet i större utsträckning än vad som hittills skett. En sådan ökad samverkan och informationsutbyte skulle stärka såväl staten som näringslivet och innebära flera positiva effekter för den samlade informationssäkerheten och cybersäkerheten i samhället.

Eftersom NCSC inte ska ha någon reglerande roll eller arbeta med tillsyn, sanktioner eller beslut kommer den förändrade verksamheten inte innebära någon ökad regelbörda eller kostnader för företag eller privata aktörer. Snarare bör förslagen leda till ökad resiliens och förmåga bland dessa aktörer, och i förlängningen till minskade kostnader.

6.6 Övriga konsekvenser

Utredningen bedömer inte att förslagen påverkar Sveriges åtaganden i förhållande till EU. De EU-rättsliga krav som gäller den nationella CSIRT:en påverkas inte av utredningens bedömning att den nationella CSIRT:en ska integreras i cybersäkerhetscentret i så stor utsträckning som möjligt. MSB är fortfarande ansvarig myndighet för Sveriges åtaganden som följer av NIS-direktivet och föreslås vara ansvarig myndighet för den nationella CSIRT:en även enligt Utredningen om genomförande av NIS2- och CER-direktivens förslag. Eftersom någon verksamhetsöverföring inte föreslås i nuläget får förslagen inte några konsekvenser i förhållande till EU och de åtaganden Sverige har i förhållande till unionen.

Utredningen har inte identifierat några konsekvenser för domstolarna eller jämställdheten. Förslagen bedöms inte heller få några konsekvenser för den kommunala självstyrelsen eller kommunernas organisation.

7 Ikraftträdande

Utredningens förslag: Förordningen om Nationellt cybersäkerhetscenter och de föreslagna förändringarna av centermyndigheternas instruktioner föreslås träda i kraft den 1 september 2024.

Några övergångsbestämmelser bedöms inte nödvändiga.

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.