Myndigheten för samhällsskydd och beredskap

Datum
2021-11-17

Ärendenr
MSB 2021-10146

Uppdrag till MSB att vidta förberedelser för att bli nationellt samordningscenter kopplat till det europeiska kompetenscentret för cybersäkerhet

Redovisning av regeringsuppdrag Ju2021/03097

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Telefon: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Org.nr: 202100-5984

INNEHÅLLSFÖRTECKNING

Sammanfattning

MSB har fått regeringens uppdrag att förbereda för inrättandet av Sveriges nationella samordningscenter (NSC) för forskning och innovation inom cybersäkerhet och presenterar i denna redovisning ett förslag på hur NSC ska sättas upp under 2022. MSB tar upp vilka uppgifter myndigheten avser att utföra som NSC, hur NSC ska styras och organiseras inom myndigheten, vad MSB behöver för resurser och vilka samverkansgränssnitt som kan bidra till MSB:s uppdrag som NSC. Regeringsuppdraget har genomförts i samverkan med Vinnova och DIGG och i dialog med RISE och andra relevanta aktörer.

Sveriges samhällsviktiga tjänster genomgår en avancerad digital transformation. Men informations- och cybersäkerhetsarbetet halkar efter, vilket gör samhället alltmer sårbart för cyberincidenter. Samtidigt har vi gjort oss beroende av icke-europeiska cybersäkerhetsleverantörer, våra egna insatser på området inom forskarsamhället och näringslivet är fragmenterade och vi har en stor kompetensbrist inom cybersäkerhet i Sverige. Vi behöver alltså samla krafterna inom cybersäkerhetsforskning och innovation och satsa på kompetensutveckling inom området.

EU-kommissionen och EU-parlamentet vill ta ett samlat grepp och genom finansiellt stöd stärka EU:s förmåga och konkurrenskraft inom cybersäkerhet och utveckla unionens kapacitet inom forskning, innovation och kompetens. Svenska forskningsinstitut, företag och myndigheter har möjlighet att söka dessa EU-medel för forsknings- och innovationsprojekt inom cybersäkerhet.

Ett europeiskt kompetenscentrum för cybersäkerhet håller på att inrättas i Bukarest. Kompetenscentrumet kommer att utforma och hantera cybersäkerhetsutlysningar inom EU-programmen Horisont Europa och DIGITAL samt leda ett nätverk av nationella samordningscenter och en europeisk kompetensgemenskap bestående av behovsägare och utförare inom cybersäkerhetsforskning och innovation.

Det svenska nationella samordningscentret (NSC) vid MSB kommer att kunna främja EU-satsningarna i Sverige, knyta kontakter mellan aktörer i branschen och ge stöd vid EU-utlysningar, så att Sverige får förutsättningar att delta i och dra nytta av de EU-finansierade cybersäkerhetsprogrammen. NSC kommer även att kunna förvalta EU-medel för ekonomiskt stöd till framförallt små och medelstora företag.

Genom detta EU-initiativ har Sverige och svenska aktörer möjlighet att placera sig i framkant och stärka förmågan och konkurrenskraften inom cybersäkerhet. Sammantaget kommer denna kraftsamling att kunna bidra till ökad cybersäkerhet i Sverige och i EU.

1 Inledning

1.1 Regeringsuppdraget

Regeringen har uppdragit åt Myndigheten för samhällsskydd och beredskap (MSB) att vidta förberedande åtgärder och lämna förslag på hur ett nationellt samordningscenter för forskning, innovation och tillämpning inom cybersäkerhet[1] ska kunna inrättas vid myndigheten under 2022 (se bilaga 1).

Uppdraget ska genomföras i samverkan med Verket för innovationssystem (Vinnova) och Myndigheten för digital förvaltning (Digg). MSB ska ha en dialog med RISE Research Institutes of Sweden AB och andra aktörer som bedöms vara relevanta.

Uppdraget ska redovisas till Regeringskansliet (Justitiedepartementet) senast den 17 november 2021.

1.2 Bakgrund

Den 28 juni trädde Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 i kraft gällande inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum, nedan kallad CCCN-förordningen[2].

Detta EU-initiativ har sitt ursprung i EU:s cybersäkerhetspaket från den 13 september 2017[3]. Paketet innehåller framförallt tre initiativ för att öka informations- och cybersäkerheten i EU:

1. En EU-reglering som tar ett helhetsgrepp på säkerheten i nätverk och informationssystem för samhällsviktiga tjänster och vissa digitala tjänster, NIS-direktivet[4];
2. Ett ramverk för certifiering av it-säkerhetsprodukter och tjänster samt ett utökat permanent mandat för EU:s cybersäkerhetsorgan ENISA, Cybersäkerhetsakten[5];
3. Ett europeiskt kompetenscentrum för cybersäkerhet, ett nätverk av nationella samordningscentrum och en europeisk kompetensgemenskap för att stimulera forskning och innovation inom cybersäkerhet i EU, CCCN-förordningen.

[1] För en beskrivning av begreppet ”cybersäkerhet”, se begreppslistan i bilaga 2.
[2] Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum
[3] Resilience, Deterrence and Defence: Building strong cybersecurity for the EU - JOIN/2017/0450 final
[4] 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
[5] 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)

Dessa initiativ ingår i EU:s cybersäkerhetsstrategi från 2020 och som identifierar ett antal utmaningar och förslag på åtgärder på EU-nivå[6]. Ytterligare prioriterade områden i strategin är:

- The "Blueprint" recommendation on a coordinated response to large-scale cybersecurity incidents and crises[7] samt the Joint Cyber Unit Recommendation[8];
- The EU 5G Cybersecurity Toolbox for the secure deployment of 5G network infrastructure in the EU[9].

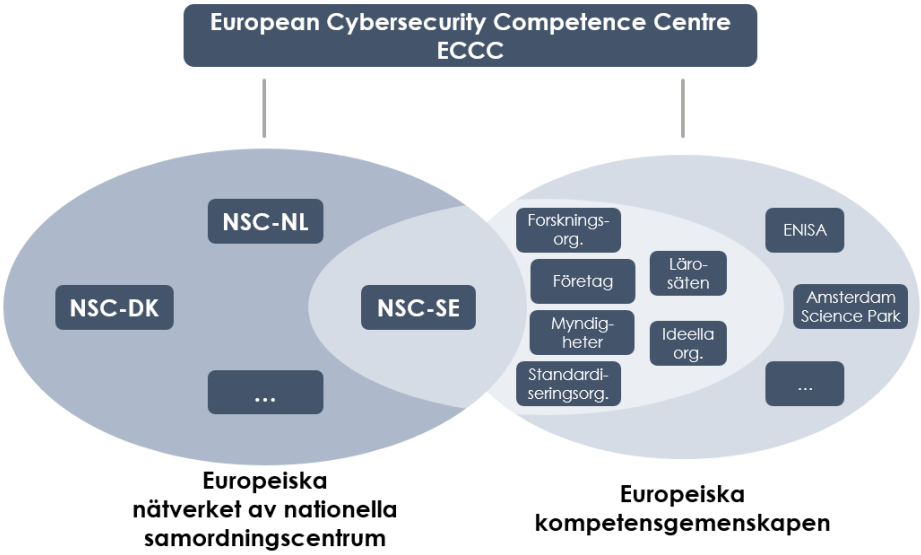
Bakgrunden till det tredje initiativet i EU:s cybersäkerhetspaket är EU:s beroende av icke-europeiska cybersäkerhetsleverantörer och delvis fragmenterade insatser inom forskning och innovation. Det ligger i unionens strategiska intresse att säkerställa att den bibehåller, utvecklar och samlar relevant forskningskapacitet, teknisk kapacitet och kompetens inom cybersäkerhet för att trygga nätverk och informationssystem för samhällsviktiga tjänster och samtidigt tillhandahålla marknadsledande cybersäkerhetsprodukter och tjänster. Små och medelstora företag (SMF) lyfts fram som extra viktiga intressenter, då de kan tillhandahålla spjutspetslösningar inom cybersäkerhet, samtidigt som de SMF som inte har kapacitet att investera i cybersäkerhet är benägna att vara extra sårbara för incidenter.

1.3 EU:s kompetenscentrum för cybersäkerhet, nätverket av nationella samordningscentrum och kompetensgemenskapen

CCCN-förordningen reglerar och beskriver huvudsakligen tre delar i ett ekosystem för cybersäkerhetsforskning, innovation och tillämpning i EU:

- ett europeiskt kompetenscentrum för cybersäkerhet;
- ett nätverk av nationella samordningscentrum;
- en europeisk kompetensgemenskap.

[6] Joint Communication to the European Parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584
[8] Commission Recommendation (EU) 2021/1086 of 23 June 2021 on building a Joint Cyber Unit
[9] Secure 5G deployment in the EU - Implementing the EU toolbox COM/2020/50 final



Figur 1. Ekosystemet i CCCN-förordningen

Uppdraget för EU:s kompetenscentrum och nätverket av nationella samordningscentrum är att stärka EU:s förmåga och konkurrenskraft inom cybersäkerhet genom att utveckla unionens kapacitet inom forskning, innovationer och kompetens.

EU:s kompetenscentrum för cybersäkerhet, eller som det kommer att kallas, ECCC, är ett EU-organ som, när denna redovisning lämnas till regeringen, håller på att inrättas i Bukarest[10]. ECCC styrs av en styrelse med ledamöter från varje medlemsstat. I skrivande stund håller en generaldirektör för ECCC på att rekryteras och förberedelser sker för den fysiska placeringen samt rekrytering av ca 35 medarbetare under 2021-2022. ECCC kommer att vara EU:s huvudorgan för investeringar i cybersäkerhetsforskning, cybersäkerhetsteknik och industriell utveckling av cybersäkerhet samt för genomförande av relevanta projekt och initiativ tillsammans med nätverket av nationella samordningscenter. ECCC kommer att förvalta ekonomiskt stöd till cybersäkerhet från EU-programmen Horisont Europa[11] och DIGITAL (Digitalt Europa)[12]. EU-organet kommer att ta fram strategiska prioriteringar och ett arbetsprogram inom området samt ge expertstöd, utfärda vägledningar, mäkla kunskap och visualisera projekt. ECCC kommer att leda nätverket av nationella samordningscenter och leda arbetsgrupper med registrerade medlemmar i den europeiska kompetensgemenskapen.

Varje medlemsstat ska utnämna ett nationellt samordningscenter, som ska stödja ECCC i sitt uppdrag, bygga upp och samordna den nationella delen av den europeiska kompetensgemenskapen, kunna ge ekonomiskt stöd med EU-medel till tredje part, särskilt små och medelstora företag, främja de europeiska arbetsprogrammen och ge vägledningar

[10] https://cybersecurity-centre.europa.eu/index_en
[11] https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en
[12] https://digital-strategy.ec.europa.eu/en/activities/digital-programme

vid ansökningar samt i stort stimulera forskning, innovation och kompetensutveckling nationellt. Det nationella samordningscentret kommer att delta i nätverket av nationella samordningscenter, som fungerar som ett samlande stöd i ECCC:s uppdrag och är ett forum för utbyte av erfarenheter och samverkan vid nationell tillämpning av CCCN-förordningen.

Kompetensgemenskapen kommer att bestå av en nationell gemenskap som tillsammans med andra medlemsstaters motsvarigheter ingår i en europeisk kompetensgemenskap. Gemenskapen består av behovsägare och utförare av forskning, innovationer, kompetensutveckling och standardisering inom cybersäkerhet. Som medlem i kompetensgemenskapen bidrar organisationen till det uppdrag som ECCC och nätverket av nationella samordningscenter har, bistår med kompetens och rådgivning i arbetsgrupper som leds av ECCC samt stödjer ECCC och det nationella samordningscentret att synliggöra projekt. Kompetensgemenskapen blir en arena för dialog, samverkan och utforskning av möjliga partnerskap.

1.4 EU-programmen för cybersäkerhet

ECCC har i uppdrag att förvalta ekonomiskt stöd till cybersäkerhet från ramprogrammet Horisont Europa och programmet för ett digitalt Europa, DIGITAL, samt bör vara öppet för andra program. Nätverket av nationella samordningscenter ska stödja ECCC att genomföra detta uppdrag.

1.4.1 Horisont Europa

Horisont Europa är EU:s ramprogram för forskning och innovation och tar över efter Horisont 2020[13]. Programmet gäller för perioden 2021-2027. Det är indelat i sex kluster varav kluster 3 om civil säkerhet för samhället inrymmer åtgärder inom cybersäkerhet[14]. De utlysningar som innefattar samfinansiering mellan utförare och medlemsstaten kommer att hanteras av ECCC. Den totala budgeten för åtgärderna inom cybersäkerhet för hela perioden är oklar. För åren 2021-2022 är budgeten ca 135 miljoner euro och innehåller satsningar på metoder för kontinuitet i digitala infrastrukturer, ökad säkerhet i open-source-hårdvara för uppkopplade enheter, AI för ökad cybersäkerhet samt skalbara integritetsskyddande teknologier för europeiska digitala tjänster. När ECCC är inrättat förväntas EU-organet i samarbete med nätverket av nationella samordningscenter att ansvara för utvecklingen och genomförandet av de cybersäkerhetsutlysningar som kräver samfinansiering av medlemsstaterna.

1.4.2 Digitalt Europa (DIGITAL)

Programmet för ett digitalt Europa, eller DIGITAL, är ett nytt EU-program som ska påskynda den digitala transformationen för företag, medborgare och offentlig sektor[15]. Det

[13] https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en
[14] https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en
[15] https://digital-strategy.ec.europa.eu/en/activities/digital-programme

är ett införanderelaterat program och kompletterar Horisont Europa, som huvudsakligen fokuserar på forskning och teknisk utveckling. Även detta program gäller för perioden 2021-2027 och är indelat i fem specifika mål inom storskalig digital kapacitet och infrastrukturuppbyggnad. Den första programperioden 2021-2022 innehåller fyra arbetsprogram; ett huvudprogram med åtgärder inom bl.a. AI[16], digitala färdigheter[17] och en europeisk infrastruktur för kvantkommunikation (EuroQCI)[18], ett arbetsprogram för högpresterande datorsystem[19], ett cybersäkerhetsprogram[20] och ett program för europeiska digitala innovationshubbar (EDIH)[21]. För åtgärder inom det specifika målet för cybersäkerhet och förtroende (mål 3), har DIGITAL en total budget för hela programperioden på 1,6 miljarder euro. Budgeten för arbetsprogrammet för cybersäkerhet 2021-2022 är på 269 miljoner euro. ECCC kommer att ansvara för utvecklingen och genomförandet av arbetsprogrammet för cybersäkerhet i samarbete med nätverket av nationella samordningscenter. Satsningar kommer att ske inom bl.a. testbäddar för cybersäkerhet, sammankopplade SOC:ar (Security Operations Centres), säkerhet inom 5G, stöd till hälso- och sjukvårdssektorn samt stöd för implementeringen av EU-reglering inom cybersäkerhet. DIGITAL tar bland annat över det stöd som tidigare gavs inom EU-programmet CEF Cybersecurity för genomförandet av NIS-direktivet och stöd ges till tillämpningar inom ramen för cybersäkerhetsakten. I detta arbetsprogram sker även en särskild satsning för att stödja inrättandet av nationella samordningscenter samt, efter prövning av EU-kommissionen, en möjlighet för samordningscentren att förvalta EU-medel för stöd till tredje part. Huvudprogrammet innehåller också cybersäkerhetsåtgärder men som inte kommer att hanteras av ECCC. Budgeten för dessa åtgärder uppgår till 222 miljoner euro under programperioden 2021-2022 varav 170 miljoner euro vigs för EuroQCI.

2 Uppgifter för Sveriges nationella samordningscenter

MSB genomför nu förberedande åtgärder för att inrätta Sveriges nationella samordningscenter, fortsättningsvis kallat NSC. Kraven på NSC i CCCN-förordningen innefattar uppgifter kopplade till stöd till ECCC och nätverket av nationella samordningscenter, samordning av kompetensgemenskapen, bidrag med teknisk kompetens till utvecklingen av EU-program, främjande av EU-programmen, vägledning till aktörer vid utlysningar, samt förmågan att förvalta EU-medel för stöd till tredje part.

[16] https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
[17] https://digital-strategy.ec.europa.eu/en/activities/skills-digital-programme
[18] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci
[19] https://digital-strategy.ec.europa.eu/en/policies/high-performance-computing
[20] https://digital-strategy.ec.europa.eu/en/activities/cybersecurity-digital-programme
[21] https://digital-strategy.ec.europa.eu/en/activities/edihs

2.1 Stödja EU:s kompetenscentrum för cybersäkerhet och nätverket av nationella samordningscenter

En av huvuduppgifterna som NSC avser att utveckla är stöd till ECCC gällande dess strategiska uppgifter. Det handlar om att bidra med sakkunskap och samtidigt lyfta fram nationella cybersäkerhetsutmaningar och behov inom olika sektorer. Nedan följer en lista med de strategiska uppgifterna för ECCC och som NSC avser att stödja på olika sätt.

ECCC ska:

- ta fram en agenda som innehåller strategiska rekommendationer för utvecklingen av en europeisk sektor för cybersäkerhet inom näringsliv och forskning;
- fastställa strategiska prioriteringar för sitt arbete med att stärka forskning och innovation inom cybersäkerhet, utveckla kapacitet, stärka kompetens, ta i bruk och använda cybersäkerhetsprodukter, tjänster och processer, stödja marknadsspridningen av lösningar och stödja myndigheter och företag på efterfrågesidan med att införa cybersäkerhetslösningar;
- stödja bland annat små och medelstora företag i cybersäkerhetsbranschen;
- säkerställa synergier med bland annat ENISA;
- på ett effektivt sätt samordna de nationella samordningscentren genom nätverket och få bästa möjliga utbyte av sakkunskap och idéer;
- på begäran av medlemsstaterna tillhandahålla rådgivning inom sitt expertområde;
- underlätta samarbete och utbyte av kunskap mellan medlemmarna i kompetensgemenskapen;
- delta i relevanta konferenser;
- underlätta användning av resultat från forsknings- och innovationsprojekt.

Mycket av stödet från NSC till ECCC och de strategiska diskussionerna kommer att ske i och via nätverket av nationella samordningscenter, som leds av ECCC. Diskussioner pågår med EU-kommissionen om att inrätta en samarbetsgrupp för nätverket och som liknar den strategiska samarbetsgrupp på EU-nivå som finns för genomförandet av NIS-direktivet, se avsnitt 3.3.14.

Enligt CCCN-förordningen ska NSC vara kontaktpunkt på nationell nivå för den svenska delen av kompetensgemenskapen gentemot ECCC och nätverket av nationella samordningscenter. NSC kommer därmed att företräda Sverige i nätverket och gentemot ECCC. Underlag för Sveriges hållning och stöd till ECCC och nätverket av nationella samordningscenter samlar NSC från samordning av den svenska delen av kompetensgemenskapen, NSCs programråd, samverkan med andra relevanta fora och aktörer samt från expertis och erfarenhet inom MSB. Myndigheten kan bland annat bidra med den lägesbild som genereras från incidentrapportering till MSB från statliga myndigheter och NIS-leverantörer, Infosäkkollen[22] och andra flöden och samarbeten

[22] https://www.msb.se/infosakkollen

bidrar till. NSC avser att aktivt bidra i arbetet i nätverket och i de arbetsgrupper som kan komma att skapas.

Utfallet från arbetet på EU-nivå kommer NSC att ta hem och informera om för den svenska delen av kompetensgemenskapen och de myndigheter, organisationer och sammanslutningar som NSC samverkar med i övrigt.

2.2 Bygga upp och samordna den svenska delen av den europeiska kompetensgemenskapen

Som ovan nämndes ska NSC samordna den nationella delen av den europeiska kompetensgemenskapen samt vara kontaktpunkt på nationell nivå för den svenska delen av kompetensgemenskapen gentemot ECCC och nätverket av nationella samordningscenter.

2.2.1 Deltagande i kompetensgemenskapen

En nationell kompetensgemenskap ska bestå av aktörer som å ena sidan verkar inom cybersäkerhet operativt och tekniskt inom industrin (inbegripet små och medelstora företag), akademin och forskningsinstitut, andra ideella organisationer, standardiseringsorganisationer och offentliga verksamheter. CCCN-förordningen anger även att kompetensgemenskapen ska engagera relevanta blivande europeiska digitala innovationshubbar (EDIH). Kompetensgemenskapen ska å andra sidan bestå av behovsägare och kravställare av cybersäkerhetsprodukter och –tjänster. Exempel på viktiga målgrupper är leverantörer av samhällsviktiga och digitala tjänster och regleringsmyndigheterna enligt NIS-förordningen[23], myndigheterna som ingår i Sveriges nationella cybersäkerhetscenter, se avsnitt 3.3.6 och Integritetsskyddsmyndigheten med flera. NSC kommer i enlighet med kraven i CCCN-förordningen att sträva efter en balanserad representation av intressenter i gemenskapen och aktivt stimulera deltagande, särskilt av små och medelstora företag.

Att vara medlem i kompetensgemenskapen innebär att man bidrar i det gemensamma arbetet med att främja cybersäkerhetsforskning och innovation i Sverige och EU. Det kan handla om att:

- delta i arbetsgrupper och aktiviteter beslutade av ECCC:s styrelse och som leds av ECCC;
- genom arbetsgrupperna bidra med kompetens och råd gällande prioriteringar och innehåll i EU:s arbetsprogram;
- stödja ECCC och NSC i att synliggöra vissa EU-finansierade projekt;
- delta i diskussioner och samarbeten inom ramen för den svenska delen av kompetensgemenskapen;
- underlätta för och dela med sig av sin cybersäkerhetskompetens.

[23] Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster

Värdet för medlemmen att delta i kompetensgemenskapen kan vara att:

- få tillgång till en svensk och europeisk arena för dialog, samverkan och möjliga partnerskap;
- få tillgång till information och initiativ från Sverige och EU;
- få information om pågående och kommande utlysningar inom EU
- få möjlighet att lyfta behov och idéer;
- kunna påverka innehållet i EU:s olika arbetsprogram;
- kunna föra behovs- och policy-dialoger med NSC och på EU-nivå.

Ansökan om att få bli medlem i kompetensgemenskapen görs till NSC, som gör en bedömning enligt kriterier som framgår i CCCN-förordningen och som kommer att konkretiseras av ECCC i samarbete med nätverket av NSC. NSC har även möjlighet att sätta ytterligare nationella kriterier. Efter NSC:s bedömning registreras medlemmen av ECCC.

2.2.2 Ett svenskt forum

NSC kommer att inrätta ett forum för den svenska delen av kompetensgemenskapen. I detta forum informerar NSC om aktuellt från EU och Sverige, inhämtar behov och upplevda utmaningar samt uppmuntrar deltagande i de aktiviteter som genereras av ECCC, nätverket av NSC och den europeiska kompetensgemenskapen. Ämnen för information, diskussion eller samarbete kan handla om:

- aktuellt från ECCC, nätverket av nationella samordningscenter och den europeiska kompetensgemenskapen;
- aktuella cybersäkerhetsprogram och utlysningar inom ramen för Horisont Europa och DIGITAL
- aktuella sårbarheter och hot;
- behov av
    - ämnen att beforska
    - innovationer;
    - standarder;
- kompetensbrist och utbildningsbehov;
- testbäddar för cybersäkerhet;
- cybersäkerhets- och kontinuitetsövningar;
- angränsande cybersäkerhetsprogram och utlysningar, från EU, från MSB och från andra svenska aktörer;
- aktuella möjligheter till samarbeten i Sverige och över landgränserna;
- gemensamma möten med NIS samarbetsforum, MSB:s privat-offentliga samverkansforum för NIS-aktörer och MSB:s informationsdelningsnätverk;
- en gemensam katalog som samlar stöd inom cybersäkerhet (rådgivning, revisioner, utbildningar, verktyg m.m.)

Under forumet kommer det finnas möjlighet att sätta upp tematiska undergrupper initierade av NSC eller föreslagna av medlemmarna. Kopplat till forumet kommer NSC att ha en elektronisk medlemsyta. NSC kommer att ta fram riktlinjer för ansökan och deltagande i forumet.

2.2.3 Uppbyggnad

Arbetet med att bygga upp den svenska kompetensgemenskapen kan genomföras på olika sätt. Inledningsvis behöver ställning tas till om NSC ska utföra det själv eller om det kan göras genom att anlita eller samverka med annan aktör. Styrande för detta är bland annat hur innebörden av artikel 6 i CCCN-förordningen ska tolkas. Där ställs två grundkrav på ett nationellt samordningscenter – sakkunskap avseende forskning och teknik respektive kapacitet att effektivt föra en dialog med och samordna arbetet med näringslivet, den offentliga sektorn, den akademiska världen, forskarsamhället och medborgarna, inklusive de myndigheter som utses i enlighet med direktiv (EU) 2016/1148. Båda är en förutsättning för att NSC ska kunna uppfylla sina utpekade uppgifter. Till skillnad mot sakkunskap avseende forskning och teknik, som centret enligt förordningen antingen kan besitta själv eller på annat sätt säkerställa tillgång till, ska ett nationellt samordningscenter ha kapacitet att effektivt föra en dialog med och samordna arbetet med kompetensgemenskapen. Därtill ska NSC enligt artikel 7 samma förordning samordna den svenska delen av kompetensgemenskapen. NSC har en pågående dialog med EU-kommissionen för att säkerställa vilken kompetens och vilket arbete som NSC ska ha internt och vilka uppgifter som kan genomföras genom att anlita eller samverka med externa aktörer.

Flera aktörer arbetar idag med att bygga upp plattformar för samverkan kring innovation och forskning på cybersäkerhetsområdet, bland annat i form av digitala innovationshubbar. Arbetet har kommit olika långt, vissa arbetar nationellt medan andra har regionalt fokus och även inriktningarna kan skilja sig. Som exempel kan nämnas att forskningsinstitutet RISE redan i januari 2020 påbörjade ett arbete med att bygga upp ett nationellt forum i form av en svensk Innovationsnod för cybersäkerhet, se avsnitt 3.3.7. Uppbyggnaden, driften och den vidare utvecklingen finansieras av Vinnova, fram till 30 juni 2024. Vid uppbyggnaden av Innovationsnoden beaktades de krav som diskuterades inom EU avseende de nationella delarna av den europeiska kompetensgemenskapen. Idag har noden ca 90 medlemmar, flertalet är företag inom cybersäkerhetsindustrin. I styrgruppen för noden sitter utöver RISE, även Vinnova och MSB.

Ur ett nationellt perspektiv finns anledning att överväga om NSC vid uppbyggnaden av den svenska kompetensgemenskapen kan dra nytta av det arbete som redan genomförts. Att bygga vidare på redan etablerad samverkan på området skulle vara resurseffektivt och bedöms kunna förenkla för målgrupperna genom att strukturer som, åtminstone delvis, kan uppfattas som parallella undviks. Det skulle även innebära en snabbare etablering av den svenska kompetensgemenskapen än om NSC skulle bygga upp den från grunden.

I det fall CCCN-förordningens regler, inklusive andra överväganden, inte utgör ett hinder för NSC att driva kompetensgemenskapen i samverkan med en eller flera externa aktörer

alternativt genom att anlita externa aktörer för utförande av utpekade uppgifter, kan detta övervägas. Centrala ingångsvärden här är dock att:

- Relationen mellan NSC och samtliga externa aktörer i kompetensgemenskapen efterlever principerna för transparens, likabehandling, proportionalitet, icke-diskriminering samt utformas så att jäv och intressekonflikter motverkas. Ur MSB:s perspektiv bedöms detta inte enbart vara centralt i syfte att uppfylla kraven i CCCN-förordningen i sin roll som NSC. Myndigheten har, utöver de grundläggande krav som ställs på en myndighets verksamhet, även en rad andra åtaganden inom ramen för EU-samverkan där motsvarande krav ställs. I sammanhanget omfattas myndigheten av löpande revision av EU. Sammantaget innebär detta sannolikt att eventuell samverkan eller anlitande av externa aktörer för att driva den svenska kompetensgemenskapen behöver föregås av en offentlig upphandling.
- NSC:s möjligheter till att inneha en aktiv roll vid driften inklusive att kunna utöva styrning av kompetensgemenskapen kan garanteras på ett tillfredsställande sätt. Detta har stor betydelse för att motverka risken för jäv och intressekonflikter och säkerställa att CCCN-förordningens krav uppfylls. Den initiala tolkningen av CCCN-förordningens artiklar och skrivningarna i vägledningen ger att det är NSC som ska styra och inrikta arbetet i kompetensgemenskapen liksom samverka med deltagarna. MSB avser att skapa en fördjupad bild av kraven i dialog med EU-kommissionen.

Om MSB väljer att själv bygga upp och driva kompetensgemenskapen, behöver risken för parallella strukturer för samverkan kring forskning och innovation på cybersäkerhetsområdet beaktas. MSB kommer i ett sådant fall att tydliggöra gränsdragningar och syften för att förenkla för målgrupperna samt så långt möjligt arbeta för att identifiera synergier i syfte att strukturerna ska komplettera varandra snarare än konkurrera. Ett annat alternativ kan vara att NSC inkorporerar och bygger vidare på redan etablerad verksamhet. Förutsättningarna för detta behöver dock utredas närmare.

Som redovisats ovan behöver det praktiska arbetet med att etablera den svenska kompetensgemenskapen föregås av en fördjupad analys avseende vissa frågor. Tolkningen av CCCN-förordningen och EU-kommissionens vägledning för att klargöra frågan om NSC:s, och i så fall i vilken utsträckning, möjlighet att driva kompetensgemenskapen i samverkan med extern aktör alternativt anlita extern aktör för att utföra olika uppgifter, prioriteras i nuläget. Stöd hämtas från kommissionen och hur andra medlemsstater förhåller sig till detta.

2.3 Bidra i utformning av europeiska arbetsprogram

NSC avser i sin roll som kontaktpunkt på nationell nivå att bidra i utformningen av de europeiska arbetsprogram som ECCC ansvarar för, det vill säga cybersäkerhetsprogrammet i DIGITAL och de cybersäkerhetsutlysningar i Horisont Europa som bygger på medfinansiering från medlemsstaterna.

Det är viktigt att de utlysningar som inkluderas i arbetsprogrammen dels syftar till att omhänderta behov som finns i Sverige, och dels att de inriktas så att de kan utföras av svenska aktörer. NSC kommer att inhämta behov och idéer till arbetsprogrammen via kompetensgemenskapen, NSC:s programråd, relevanta samverkansfora och organisationer, se avsnitt 3.3 och från MSB:s sakkunniga inom cybersäkerhet och säkra kommunikationer.

Den medarbetare på NSC-kansliet som innehar rollen som kontaktpunkt på nationell nivå, se avsnitt 3.1, och som företräder NSC gentemot ECCC och nätverket, bereder underlag, planerar och genomför behovsinventeringar och bidrar i programutvecklingen hos ECCC.

2.4 Främja de europeiska cybersäkerhetsprogrammen

För att stärka svenskt deltagande i de europeiska cybersäkerhetsprogrammen, är kännedom om dem viktig. De europeiska finansieringsprogrammen, främst Horisont Europa, kräver ofta samverkan med projektparter från andra medlemsländer vilket inte nationell forsknings- och innovationsfinansiering gör i samma omfattning. Svenska aktörer som söker finansiering står följaktligen inför åtminstone två utmaningar. Den första handlar om att överhuvudtaget ha vetskap om vilka europeiska finansieringsalternativ som finns, i närtid och längre fram i tiden, den andra utmaningen handlar om att hitta potentiella utländska parter att samverka med.

Med anledning av bland annat detta, avser NSC att genomföra åtgärder för att främja de europeiska cybersäkerhetsprogrammen, att göra dem kända lokalt och stimulera deltagande i projekt tillsammans med andra nationella och europiska parter. ”Marknadsföringen” av programmen kommer att ske på ett antal olika sätt.

NSC kommer att utveckla en webbplats, på vilken bland annat information om kommande finansieringsalternativ inom cybersäkerhet från Horisont Europa, DIGITAL och andra källor kommer att publiceras. Detta sker i samverkan mellan informationsansvarig för NSC och NSC:s nationella vägledare, se avsnitt 3.1. Medlemmar i kompetensgemenskapen och andra intresserade aktörer får möjlighet att prenumerera på NSC:s nyhetsbrev. Nyhetsbrevet skickas ut regelbundet, och framförallt när aktuell information om finansieringsalternativ anslås av EU.

EU publicerar ofta sina finansieringsalternativ samlat i omgångar. Vid dessa tillfällen är det betydelsefullt att tidigt nå ut med information, och att kunna svara på frågor. För att möta detta behov kommer NSC att anordna öppna informationsevenemang som kan tematiseras eller riktas mot ett specifikt cybersäkerhetsprogram. NSC kommer inom ramen för samordningen av den svenska kompetensgemenskapen, att informera om de europeiska cybersäkerhetsprogrammen. Utöver egna evenemang och kompetensgemenskapen leder MSB ett stort antal forum och konferenser där information kan delas, t.ex. NIS samarbetsforum, MSB:s privat-offentliga samverkansforum för NIS-aktörer, den årliga NIS-konferensen samt tematiska informationsdelningsnätverk, se avsnitt 3.3.

NSC avser även att använda andra närliggande forum och noder för spridning av information för att främja de europeiska cybersäkerhetsprogrammen, t.ex. RISE innovationsnod för cybersäkerhet, relevanta digitala innovationshubbar och branschorganisationer.

2.5 Ge vägledning till aktörer i Sverige gällande EU:s cybersäkerhetsprogram

Att ansöka till EU-utlysningar kan upplevas som svårt och omständligt och kan medföra en barriär till att vilja delta i utlysningar. En prioriterad roll för NSC är att avlägsna barriärer genom att bland annat ge vägledning till svenska aktörer som söker EU-medel för cybersäkerhetsrelaterade projekt. Vid NSC kommer detta att hanteras av rollen nationell vägledare. Det är vägledarens uppgift att främja, uppmuntra och göra det enklare att delta i nationella och gränsöverskridande projekt och cybersäkerhetsåtgärder som finansieras genom relevanta unionsprogram. Huvudsakliga målgrupper i Sverige är bland annat det civila samhället, näringslivet, särskilt nystartade företag och små och medelstora företag, myndigheter, den akademiska världen och forskarsäten. Det stödjande arbetet kommer att utföras genom enskild rådgivning och i samlande forum. Vidare ingår det i vägledarens uppgift att tillhandahålla praktiskt stöd till aktörer under ansökningsfasen för projekt som förvaltas av ECCC och, efter godkännande från EU-kommissionen, av NSC.

En central förutsättning för vägledaren hos NSC är att regelbundet stämma av med utsedda nationella kontaktpunkter (NCP), t.ex. Vinnova gällande Horisont Europa, DIGG gällande DIGITAL och med andra myndigheter som verkar inom närliggande områden, t.ex. det under 2021 påbörjade arbetet med att utforma ett strategiskt program för att möta och leda i den digitala strukturomvandlingen, se avsnitt 3.3.2.

Utöver direkt vägledning kommer vägledaren att bidra till arbetet med NSC:s främjande roll för de europeiska cybersäkerhetsprogrammen. Det handlar bland annat om att, tillsammans med informationsansvarig för NSC, ordna informationsevenemang, bidra till webbplatsens och nyhetsbrevens innehåll, informera om utbildningsprogram inom cybersäkerhet samt informera om NSC, kompetensgemenskapen och EU-programmen på nationell, regional och lokal nivå, t.ex. i samverkan med Tillväxtverket och relevanta digitala innovationshubbar.

2.6 Främja kompetensutveckling

Det rådet stor brist på kompetens inom cybersäkerhetsområdet[24]. Det gäller såväl grundkompetens och medvetenhet hos medarbetare och ledningsgrupper som spetskompetens för forskning och innovation.

[24] NCSC:s och Polismyndighetens rapport ”Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden”

Deltagande i de europeiska cybersäkerhetsprogrammen stärker svensk cybersäkerhetsrelaterad kompetens. Det är dock angeläget att Sverige stärker kompetensen på bredden och djupet genom utbildning.

Utbildningar erbjuds inom olika aspekter av cybersäkerhet och på olika nivåer och de sträcker sig från tillämpade yrkesutbildningar till akademiska utbildningar på forskarnivå. Därutöver genomförs utbildningsinsatser av företag och myndigheter.

Inom ramen för MSB:s utbildningsprogram inom informations- och cybersäkerhet gav regeringen 2019 MSB i uppdrag att genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor[25]. Mot bakgrund i nämnda utbildningsinsats erbjuder MSB ett flertal kurser som vänder sig till personer som arbetar med eller direkt påverkas av cybersäkerhet inom offentlig sektor.[26]

NSC kommer att främja insatser som syftar till kompetensutveckling inom cybersäkerhet. Det kan handla om visualisering av behov och utbildningar, att stödja incitament för ökad kompetensutveckling eller att tillhandahålla rådgivning om behov inom området.

2.7 Skapa synergier med policyutveckling i Sverige

Behovsinventering, diskussioner och samverkan som sker med fokus på cybersäkerhetsforskning och innovation kommer att ge värdefulla ingångsvärden till policyutvecklingen i Sverige. Det handlar om t.ex. utvecklingen av den nationella informations- och cybersäkerhetsstrategin, nationella kraftsamlingar inom digitalisering, forskningsstrategier på olika nivåer i landet och kompetensförsörjningsstrategier. NSC avser att engagera sig i relevanta policyutvecklingsfora och bidra med den kunskap och erfarenhet som kommer med NSC-uppdraget. NSC kan också dra nytta av MSB:s samlade expertis från myndighetens uppdrag att stödja och samordna arbetet med samhällets informations- och cybersäkerhet och att analysera och bedöma omvärldsutvecklingen inom området.

2.8 Uppföljning och användning av EU-finansierade projekt

En central uppgift för NSC är att följa upp och synliggöra relevanta resultat av det arbete som bedrivs inom nätverket, gemenskapen och EU:s kompetenscentrum på nationell, regional eller lokal nivå. Därutöver kommer NSC även att verka för att resultaten från forsknings- och innovationsprojekt också kommer till användning hos svenska aktörer.

Synliggörandet av genomförda projekt kommer åtminstone att baseras på sammanställningar av pågående och avslutade projektresultat finansierade inom ramen för ECCC:s verksamhetsområde. Särskilt fokus bör läggas på det svenska deltagandet i EU-programmen i förhållande till andra medlemsstater.

Nyckeltal som t.ex. antal ansökningar med svenskt deltagande, finansierade projekt med svenskt deltagande, det svenska deltagandets ekonomiska värde relativt andra länder samt

[25] Ju2019/03057/SSK
[26] https://www.informationssakerhet.se/kompetensutveckling/kurser-msb/

antal organisationer som använder resultat från genomförda projekt, är angelägna att utveckla. Det är dock för tidigt att säga vilka nyckeltal ECCC kommer att utveckla och dela med NSC, och vilka nyckeltal NSC avser att utveckla.

MSB gör bedömningen att den uppföljande förmågan för NSC kommer att vara beroende av vilken projektrelaterad information som tillgängliggörs av ECCC. I den vidare utvecklingen av ECCC:s verksamhet bör därför MSB framhålla vikten av informationsdelning gällande ansökningar och finansierade projekt. ECCC kommer att vidareutveckla den cybersäkerhetsatlas som EU-kommissionen har tagit fram och som presenterar forskningsinstitut och andra aktörer inom cybersäkerhet[27]. Där finns en potential att också synliggöra öppna resultat som har genererats från EU-programmen inom området.

MSB har vana av att koppla forskningsresultat till nyttor för skilda samhällsaktörer. Myndigheten har i sitt ordinarie uppdrag uppgiften att beställa, kvalitetssäkra och förmedla forskning som finansieras med en del av anslaget 2:4 Krisberedskap. NSC kommer också att kunna nyttja den överblick som ges nationellt och i EU för att stimulera aktörer att visa intresse för, testa och nyttja lösningar som har tagits fram genom EU-programmen.

NSC kommer att synliggöra de utfall som genereras genom de kanaler som NSC etablerar, dvs. digitala kanaler, informationsevenemang, samordningen av den svenska kompetensgemenskapen och kopplingen till övriga samverkansgränssnitt, se avsnitt 3.3.

2.9 Om EU-finansiering till tredje part

I CCCN-förordningen ges möjligheten[28] till NSC att förvalta och tillhandahålla viss EU-finansiering till tredje part. Även om det är möjligt att bli utnämnd till och agera som NSC utan att uppfylla kraven i CCCN-förordningen för att kunna förmedla finansiering till tredje part, finns det en uttalad önskan från EU-kommissionens sida att de nationella samordningscentren etablerar sådan förmåga. Förmedlingen av medel bidrar till kompetenscentrets, kompetensgemenskapens, nätverkens och de nationella samordningscentrens förmåga att fullgöra uppdraget och uppnå de mål som fastställs i CCCN-förordningen. Ur ett svenskt perspektiv underlättas möjligheterna att ge ett effektivt stöd till relevanta svenska aktörer inom näringsliv (särskilt små och medelstora företag), akademin och offentlig sektor. Nyttjandegraden av EU-finansiering hos svenska aktörer har, i jämförelse med aktörer i många andra medlemsstater, ofta varit förhållandevis låg. NSC bedöms, genom att förenkla tillgången till medel från de stora EU-programmen Horisont Europa och DIGITAL, därför kunna bidra till att stärka konkurrenskraften inom cybersäkerhetsområdet på nationell nivå.

[27] https://cybersecurity-atlas.ec.europa.eu/

[28] Artikel 6 par 6: ” Ett nationellt samordningscentrum får när som helst begära ett erkännande av att det har kapacitet att förvalta medel för att fullgöra uppdraget och uppnå de mål som fastställs i denna förordning, i enlighet med förordning (EU) 2021/695 och (EU) 2021/694. Kommissionen ska inom tre månader från begäran bedöma huruvida det nationella samordningscentrumet har sådan kapacitet och ska utfärda ett beslut.”

Särskilt utlysningarna från cybersäkerhetsprogrammet i DIGITAL är av intresse ur ett NSC-perspektiv[29]. Ett av de uttalade syftena är att stödja implementeringen av EU-reglering och politiska initiativ såsom EU:s cybersäkerhetsstrategi, NIS-direktivet, cybersäkerhetsakten, CCCN-förordningen med flera. Här ges möjlighet att ansöka om medel för etableringen av NSC med upp till en miljon euro fördelat på två år givet att motsvarande summa tillhandahålls av en annan part. NSC kan i anslutning till denna utlysning ansöka om ytterligare en miljon euro för förmedling till tredje part för att bland annat sprida den senaste cybersäkerhetstekniken. Som ytterligare exempel på utlysningar inom DIGITAL med särskild koppling till NSC:s verksamhet är den som tar sikte på att stärka kompetensgemenskapen för cybersäkerhet respektive den som innebär förmedling av medel till tredje part rörande testning och certifiering i enlighet med målsättningarna i cyberssäkerhetsakten.

En förutsättning för att kunna förmedla EU-finansiering till tredje part är att en medlemsstat eller dess utpekade NSC begär att EU-kommissionen yttrar sig över förmågan hos aktuell NSC att förmedla medel. En sådan begäran kan göras när som helst och innebär att kommissionen gör en bedömning av samordningscentrets kapacitet när det gäller att förvalta medel för att fullgöra uppdraget och uppnå de mål som fastställs i CCCN-förordningen. Kommissionen ska avge sitt yttrande inom tre månader från att begäran inkommer. Ett positivt yttrande beaktas som ett beslut om godkännande av att samordningscentret har den nödvändiga kapaciteten. Ett eventuellt negativt yttrande ska vara motiverat samt ange vilka krav som inte är uppfyllda. Efter att bristerna åtgärdats kan en ny begäran lämnas in tillsammans med kompletterande information.

Ledning för vad som krävs för att kunna utgöra ett nationellt samordningscenter inklusive anses ha förmåga att förmedla medel till tredje part, kan hämtas från den vägledning samt det ansökningsformulär EU-kommissionen har tagit fram till de blivande nationella samordningscentren[30]. Ansökningsformuläret ska användas i samband med begäran om yttrande över förmågan att förmedla medel till tredje part och det är därför först vid detta tillfälle som en medlemsstat redovisar hur det utpekade samordningscentret uppfyller kraven som ställs på rollen som NSC. Något motsvarande krav på att redovisa förmåga ställs inte när en medlemsstat endast utnämner sitt nationella samordningscenter.

2.9.1 Krav som ställs på MSB

För att MSB i rollen som NSC ska kunna förmedla medel till tredje part behöver följande redovisas i samband med att en begäran om kommissionens yttrande lämnas in:

1. att MSB inte befinner sig i en sådan uteslutningssituation som avses i artikel 136 i budgetförordningen[31], exempelvis är försatt i konkurs;

[29] https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital
[30] https://digital-strategy.ec.europa.eu/en/news/european-cybersecurity-competence-centre-and-network-commission-issues-guidelines-evaluation
[31] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU, Euratom) 2018/1046 av den 18 juli 2018 om finansiella regler för unionens allmänna budget, om ändring av förordningarna (EU) nr 1296/2013, (EU) nr 1301/2013, (EU) nr 1303/2013, (EU) nr 1304/2013, (EU) nr 1309/2013, (EU) nr

2. att MSB är identifierad som juridisk person och vem som är rättslig företrädare;
3. hur MSB:s organisation och arbete förhåller sig till uppfyllandet av de uppgifter som NSC har;
4. att MSB har tillräcklig finansiell kapacitet för uppdraget;
5. att MSB har tillräcklig kapacitet avseende personal knuten till NSC, inte bara avseende antal utan även kompetens och erfarenhet;
6. att MSB har förmåga att ge ekonomiskt stöd till tredje part genom att ha regler, rutiner och arbetssätt på plats för hantering av medel och att dessa uppfyller principerna om proportionalitet, sund ekonomisk förvaltning, likabehandling och icke-diskriminering, garanterar öppenhet i processen och motverkar intressekonflikter;
7. att MSB har ett robust regelverk för riskhantering och intern kontroll;
8. att MSB har kapacitet att samordna arbetet på nationell nivå.

Det arbete som har gjorts hittills med att analysera de olika kraven som ställs indikerar att MSB redan i nuläget uppfyller flera av ovan nämnda krav. Eftersom myndigheten i andra sammanhang redan har beviljats EU-medel har MSB redan sedan tidigare redovisat punkterna 1 och 2.

Kravet i punkten 4 om finansiell kapacitet är också redan uppfyllt eftersom det är tillräckligt att MSB tillhör offentlig sektor.

När det gäller punkterna 6 och 7 om förmåga att ge ekonomiskt stöd respektive ha ett robust regelverk för riskhantering och intern kontroll har myndigheten redan sedan tidigare utvärderats i flera delar (sk ”pillar assessment”) inför att MSB fick ansvaret för EU:s civila kris- och konflikthanteringslager (CSDP Warehouse II). Av de nio pelare som en aktör granskas på och som bekräftar dess förmåga att hantera EU-medel, har MSB sedan 2018 fått godkänt i fyra av dessa, dvs. det interna kontrollsystemet, redovisningssystem, oberoende extern revision samt upphandlingar.[32] Under 2020 utvidgades utvärderingen på MSB:s initiativ till att innefatta ytterligare tre pelare, dvs uteslutning från tillgång till finansiering, offentliggörande av information om mottagare, samt skydd för enskilda med hänsyn till personuppgiftshanteringen, vilka även de bl.a. tar sikte på sådan förmåga som myndigheten nu behöver ha för att kunna uppfylla sitt uppdrag som nationellt samordningscenter och förmedla medel till tredje part. Utvärderingen genomförs av extern revisionsbyrå och kommer att redovisas för kommissionen under november 2021.

De två pelare som MSB ännu inte har granskats på är tillhandahållande av finansiering med EU-medel i form av bidrag, samt finansieringsinstrument.

MSB har en dialog med EU-kommissionen gällande huruvida den genomförda utvärderingen kan användas som underlag även när yttrande begärs av kommissionen om

1316/2013, (EU) nr 223/2014, (EU) nr 283/2014 och beslut nr 541/2014/EU samt om upphävande av förordning (EU, Euratom) nr 966/2012

[32] MSB 2016-03610-27, Pillar Assessment-Final Report

förmågan hos NSC att förmedla medel till tredje part i enlighet med CCCN-förordningen. MSB har även inlett en inventering av mallar och annat stöd från kommissionen som kan användas vid den närmare utformningen av regler, rutiner och arbetssätt inom ramen för NSC:s verksamhet.

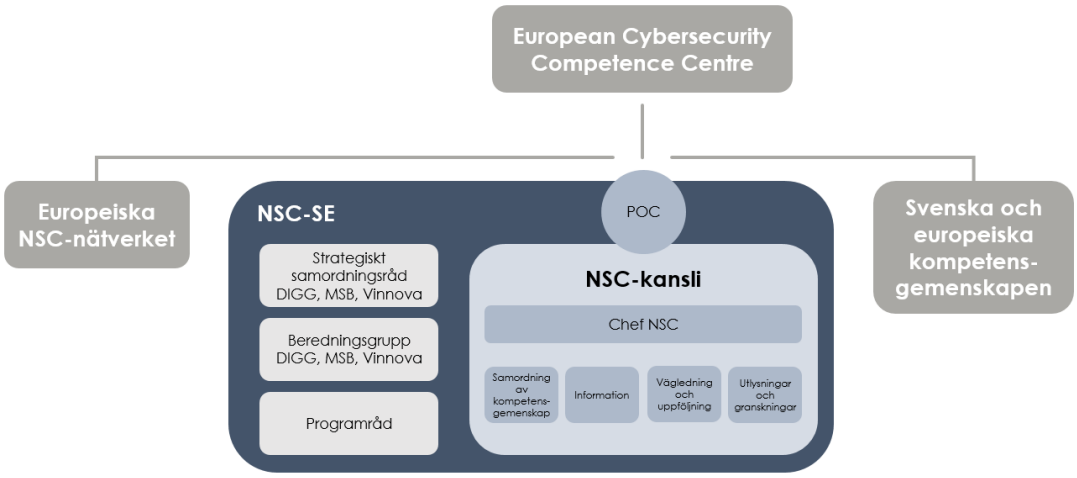
När det gäller punkten 3, 5 och 8 om organisation, personal och samordning pågår arbete och planering. För närmare redogörelse hänvisas till avsnitt 3.1 respektive 2.2 i denna uppdragsredovisning.

Myndighetens preliminära bedömning är att förmågan att uppfylla många av kraven för att kunna förmedla medel till tredje part i stora delar redan har byggts upp för att möta tidigare EU-relaterade uppgifter. Målsättningen är att komplettera redan existerande förmåga och säkerställa att MSB i rollen som NSC uppfyller kraven för att få förmedla medel till tredje part under första kvartalet 2022. Detta skulle innebära att kommissionens svar på en begäran på yttrande om förmåga att förmedla medel till tredje part skulle komma i tid för att möjliggöra att NSC hinner ansöka om medel både för egen utveckling och för förmedling till tredje part från cybersäkerhetsprogrammet i DIGITAL. En sådan ansökan behöver vara inlämnad senast under fjärde kvartalet 2022.

3 Styrning, organisation, resursbehov och samverkan

3.1 Styrning och organisation

Styrningen av NSC ska genomföras av en chef för NSC-kansliet. Därutöver ska det finnas ett strategiskt samordningsråd, en beredningsgrupp och ett programråd. NSC kommer att inrättas på MSB med ett arbetande kansli som stöd för NSC:s verksamhet.



Figur 2. Styrnings- och organisationsstruktur NSC

Det strategiska samordningsrådet ska bestå av myndighetscheferna för DIGG, MSB och Vinnova. Dessa myndigheter har alla en samordnande roll gällande EU-programmen Horisont Europa respektive DIGITAL och har i övrigt angränsande roller gällande samhällets digitalisering. Rådet ska ledas av myndighetschefen för MSB och ska träffas två

gånger per år. Det strategiska samordningsrådets huvudsakliga roll ska vara att ge råd gällande inriktning och utveckling av verksamheten vid NSC. I det ligger att ge råd om NSC:s årsprogram inklusive centrets prioriteringar för året samt de strategiska frågor som centret ska driva i EU. Frågor gällande finansiella satsningar från respektive myndighet ska inte behandlas i detta råd.

För att bereda frågor och förbereda underlag till NSC:s strategiska samordningsråd ska det finnas en beredningsgrupp. Beredningsgruppen ska bestå av utsedda handläggare från DIGG, MSB/NSC-kansliet och Vinnova. Utöver förberedelser för rådet ska gruppen genomföra regelbundna och händelsestyrda avstämningar gällande frågor av gemensamt intresse och som avser informationsutbyte, ömsesidigt stöd och gemensamma insatser.

Utöver styrningen av och den strategiska rådgivningen till NSC ska det finnas ett programråd som fungerar som en referensgrupp till NSC. Programrådet ska kunna ge råd till NSC om inriktningar, prioriteringar och innehåll i arbetsprogram samt kunna ge återkoppling på utkast till texter och tjänster från NSC. Programrådet ska bestå av representanter från offentliga sektorn, näringslivet och forskarsamfundet, både från behovssidan och från utförarsidan. Representanten ska utses baserat på sakkompetens och kunna delta aktivt och självständigt i sin egen kapacitet som sakkunnig. Representanten ska inte företräda sin organisations intressen utan ska kunna inta ett samhällsperspektiv i sin rådgivande funktion.

Till stöd för NSC:s verksamhet kommer ett bemannat kansli att sättas upp på MSB och som är indelat i följande fem huvudområden:

- Kontaktpunkt på nationell nivå (POC – Point of Contact) gentemot ECCC, NCC Network och den europeiska kompetensgemenskapen som leds av ECCC;
- Utveckling och samordning av den svenska delen av den europeiska kompetensgemenskapen;
- Information för att ”marknadsföra” de forskningsprogram och utlysningar som är aktuella inom Horisont Europa och DIGITAL;
- Vägledning och uppföljning gällande cybersäkerhetsarbetsprogram;
- Genomförande av utlysningar och granskningar av ansökningar.

MSB kommer att utse en chef för NSC. Chefen ska leda det dagliga arbetet vid kansliet.

3.2 Resursbehov

Inrättandet av ett nationellt samordningscenter, som är ett ofinansierat uppdrag, kommer att medföra nya uppgifter för MSB. Ju mer NSC kan stödja det svenska forskarsamhället, näringslivet och den offentliga sektorn, desto större effekt kommer denna EU-satsning att få för Sveriges förmåga och konkurrenskraft inom cybersäkerhet. Nedan följer vilka typer av resurser som kommer att behövas de närmaste två åren:

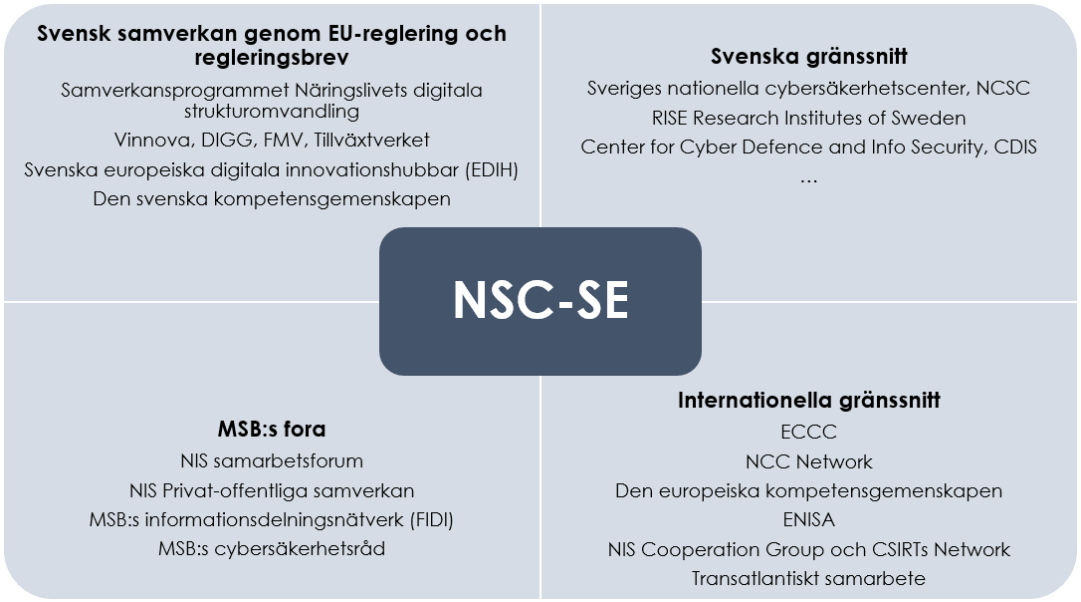
- Sex medarbetare på heltid;
- Personella resurser från MSB:s övriga verksamhet på begäran;

- Konsultkostnader för utveckling av webbplats, medlemsyta för kompetensgemenskapen samt kompetensdatabas;
- Marknadsföring, kampanjer;
- Konferenser, informationsmöten och tematiska seminarier;
- Samordning av kompetensgemenskapen inklusive forum och arbetsgrupper;
- Resor i Sverige och i EU.

MSB avser att återkomma med kostnadsberäkningar i samband med myndighetens budgetunderlag.

3.3 Samverkansgränssnitt

Genom CCCN-förordningen är en samverkansstruktur redan etablerad. Förutom samverkan med ECCC, nätverket av nationella samordningscenter och genom Kompetensgemenskapen, som är formaliserad med medlemskap, se avsnitt 2.2, ser MSB ytterligare samverkansgränssnitt som kommer att kunna ge mervärden för forskning, innovation och kapacitetsutveckling inom cybersäkerhet. Nedan presenteras några exempel på samverkansgränssnitt, som MSB har eller kommer att utveckla i rollen som NSC.



Figur 3. Samverkansgränssnitt

3.3.1 Samverkan med regeringskansliet, Vinnova och andra aktörer gällande regeringens samverkansprogram Näringslivets digitala strukturomvandling

I MSB:s uppdrag att stödja och samordna arbetet med samhällets informations- och cybersäkerhet och i en kommande roll som nationellt samordningscenter, samverkar myndigheten med regeringskansliet, Vinnova, andra myndigheter och näringslivet

avseende regeringens samverkansprogram Näringslivets digitala strukturomvandling[33]. MSB bidrar genom uppdrag i regleringsbrevet i detta arbete och deltar i arbetsgruppen Avancerad digitalisering – forskning, kunskap och tillämpning, ledd av Teknikföretagen. Gruppen diskuterar behov, utmaningar och konsekvenser och tar fram förslag på åtgärder inom fokusområdet.

Inom ramen för denna nationella samverkan, leder Vinnova arbetet kring att skapa en kraftsamling med andra myndigheter i syfte att stärka Sveriges digitala förmåga, konkurrenskraft och innovationssystem för ekologisk, social och ekonomisk hållbarhet[34]. Visionen för kraftsamlingen är ett hållbart digitaliserat Sverige år 2030. En viktig del i denna utveckling är att skapa robusta och säkra digitala system som möjliggör innovation inom olika tillämpningsområden. En kraftsamling förutsätter ett myndighetsgemensamt kansli för en effektiv samverkan och koordinering mellan myndigheter i strategisk samverkan med näringsliv, offentlig sektor, akademi och civilsamhället, inte minst när det gäller Sveriges deltagande i EU:s program och policyprocesser. Nya och gemensamma arbetssätt och att dela kunskap och lärande mellan myndigheter, över sektorsgränser och inom olika delområden behöver utvecklas och tillämpas för en framgångsrik nationell kraftsamling för att möta och leda i den digitala strukturomvandlingen. Denna kraftsamling är en föreslagen och prioriterad insats från samverkansprogrammet Näringslivets digitala strukturomvandling och erfarenheter från regeringens samverkansprogram är av stort värde i arbetet. I det arbetet deltar MSB i dialoger om samverkansstrukturer samt bidrar med expertis med målet att informations- och cybersäkerhet vägs in som en naturlig och tidig del i digitaliseringen.

3.3.2 Samverkan med Vinnova avseende Horisont Europa

Vinnova och MSB delar på ansvaret för samordningen av den del av Horisont Europa[35] som omfattar Civil säkerhet för samhället inklusive cybersäkerhet (kluster 3), se avsnitt 1.4.1. Vinnova företräder med stöd av MSB regeringen med experter i den europeiska programkommittén för Horisont Europa avseende kluster 3. Vinnova har vidare en utsedd nationell kontaktperson (NCP) och MSB bistår med en biträdande NCP. Deras uppgifter är att ge vägledning till aktörer som vill delta i Horisont Europa. Framtida arbetsprogram inom Horisont Europa och som avser samfinansierade cybersäkerhetsprogram kommer att hanteras av ECCC och nätverket av nationella samordningscenter. Detta betyder att det kommer att finnas behov av samverkan mellan NSC-kansliet, MSB och Vinnova både avseende det europeiska arbetsprogrammets utveckling såväl som vägledning till aktörer genom NCP-funktionen.

[33] https://www.regeringen.se/regeringens-politik/regeringens-strategiska-samverkansprogram/samverkansprogrammet-naringslivets-digitala-strukturomvandling/
[34] https://www.vinnova.se/publikationer/kraftsamling-for-ett-hallbart-digitaliserat-sverige/
[35] För mer information om Horisont Europa; https://www.vinnova.se/m/horisont-europa/

3.3.3 Samverkan med DIGG

Myndigheten för digital förvaltning, DIGG, har regeringens uppdrag att ansvara för samordning av programmet för ett digitalt Europa (DIGITAL) för perioden 2021-2027[36]. DIGG redovisade i juli ett förslag på hur en långsiktig samverkansstruktur ska se ut.[37] MSB deltog i det arbetet och deltar i den fortsatta utvecklingen av samverkansstrukturen.

Samverkansstrukturen enligt DIGG:s förslag bygger bl.a. på en kärna av myndigheter som samverkar på programnivå samt en tematisk indelning i kluster. Ett av klustren kallas cybersäkerhet. Cybersäkerhetsrelaterade utlysningar i DIGITAL är huvudsakligen omhändertagna i ett separat arbetsprogram och som hanteras av ECCC och nätverket av nationella samordningscenter, se avsnitt 1.4.2. MSB föreslår tillsammans med DIGG att klustret för cybersäkerhet motsvaras av det arbete som bedrivs vid NSC.

Cybersäkerhet dyker även upp i andra arbetsprogram under DIGITAL, så som programmet som innehåller satsningar på EuroQCI, Quantum Communications Infrastructure. Detta område ligger idag utanför mandatet för ECCC och nätverket av nationella samordningscenter. På nationellt plan berör frågan dock MSB gällande uppdraget att tillhandahålla säkra kommunikationer, Rymdstyrelsen gällande satellitdelen och PTS som har ett samlat ansvar inom området elektronisk kommunikation. Förslag om ett kluster för EuroQCI ligger på bordet hos DIGG och ett samarbete mellan berörda myndigheter pågår nu för att samordna arbetet med den nationella delen av EuroQCI.

Sammantaget föreslår MSB och DIGG gemensamt att NSC-kansliet leder kluster Cybersäkerhet, att MSB deltar i kluster EuroQCI och att både NSC-kansliet och MSB deltar i den horisontella samverkan på programnivå.

Inom uppdraget att etablera en förvaltningsgemensam infrastruktur för informationsutbyte (FDII)[38] finns en etablerad samverkan mellan MSB och DIGG inom, främst, området informationssäkerhet. DIGG och MSB har även en bredare samverkan etablerad där myndigheterna regelbundet möts för att informera varandra om pågående aktiviteter. Dessa båda samverkansformer och -forum skiljer sig till innehåll och syfte jämfört med den samverkan som har etablerats med kring DIGITAL. MSB och DIGG delar uppfattningen att samverkan utifrån NSC:s styrning bör hållas skild från generell samverkan och samverkan inom ramen för FDII. I den mån koordinering bör ske svarar myndigheterna för att denna sker internt inom respektive myndighet.

3.3.4 Samverkan med FMV avseende cybersäkerhetscertifiering

FMV har regeringens uppdrag att utgöra myndighet för cybersäkerhetscertifiering i Sverige[39]. Verksamheten är indelad i en inspektion för cybersäkerhetscertifiering (ICC) och ett certifieringsorgan för it-säkerhet (CSEC). ICC genomför uppgifter som följer av EU:s cybersäkerhetsakt, bland annat tillsyn över efterlevnaden av certifieringar enligt det

[36] Uppdrag att ansvara för samordning av programmet för ett digitalt Europa, I2021/01008
[37] Förslag till långsiktig samverkansstruktur för DIGITAL, DIGG Dnr. 2021-642
[38] Uppdrag att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte, I2019/03306/DF, I2019/01036/DF (delvis),I2019/01361/DF (delvis), I2019/02220/DF
[39] https://www.fmv.se/aktuellt--press/aktuella-handelser/myndigheten-for-cybersakerhetscertifiering/

europeiska ramverket för cybersäkerhetscertifiering, samt samverkan med nationella och internationella aktörer på området. NSC kommer att främja genomförandet av det europeiska ramverket för cybersäkerhetscertifiering i Sverige och avser att söka samverkan med FMV i frågan.

3.3.5 Samverkan med Tillväxtverket och Europeiska digitala innovationshubbar (EDIH)

Tillväxtverket arbetar för att stärka små och medelstora företags förmåga att ta tillvara digitaliseringens möjligheter. I det arbetet finns ett etablerat samarbete mellan MSB och Tillväxtverket, som menar att MSB är en viktig samarbetspart för att höja kompetens och förmåga inom cybersäkerhet, för att kunna ta tillvara på digitaliseringen på ett säkert och hållbart sätt.

Tillväxtverket har regeringens uppdrag att samordna de svenska kandidaterna till Europeiska digitala innovationshubbar, EDIH, totalt 15 st. varav tre till sex kommer att väljas ut av EU-kommissionen[40]. EDIH:s uppdrag är att stödja små och medelstora företags och offentliga organisationers digitala transformation och erbjuda tjänster inom områdena test och validering, utbildning och kompetensuppbyggnad, stöd för att hitta finansiering samt nätverk och ekosystem för innovation. I CCCN-förordningen anges att samverkan ska ske mellan EDIH, EU:s kompetenscentrum och nätverket av nationella samordningscenter. Vidare anges i förordningen att NSC ska etablera en samordning med relevanta EDIH gällande sitt NSC-uppdrag för att kunna erhålla EU-medel från DIGITAL för inrättandet av det nationella samordningscentret. I dessa sammanhang ska samverkan ske mellan NSC, Tillväxtverket och de svenska EDIH. NSC och Tillväxtverket kan till exempel gemensamt vända sig till de svenska EDIH för att inhämta behov samt informera om kommande cybersäkerhetsutlysningar inom DIGITAL och Horisont Europa.

3.3.6 Samverkan med det nationella cybersäkerhetscentret (NCSC)

I det nationella cybersäkerhetscentret, NCSC, i vilket MSB ingår, samverkar sju myndigheter[41] med särskilt ansvar för samhällets informations- och cybersäkerhet med det övergripande syftet att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot[42]. Verksamheten byggs upp successivt fram till 2025. En central del av NCSC:s uppdrag är privat-offentlig samverkan. Regeringen har även uttryckt att samverkan inom ramen för NCSC ska utvecklas inom bland annat kunskaps-, kompetens- och informationsutbyte samt dialog med aktörer inom forsknings-, kunskaps- och kompetensuppbyggnad. NSC ska följa uppbyggnaden av verksamheten i NCSC och där det är möjligt etablera samverkan för att utbyta information om utmaningar och behov

[40] Uppdrag att lämna stöd till de regionala digitaliseringskoordinatorerna samt att samordna och koordinera digitala innovationshubbar, I2021/00794.

[41] De ingående myndigheterna i NCSC är Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Post- och telestyrelsen och Säkerhetspolisen.

[42] https://www.cfcs.se/

gällande samhällets cybersäkerhet. Genom att MSB är en del av NCSC säkerställs en nära samverkan mellan de två centren.

3.3.7 Samverkan med RISE

MSB samverkar med RISE Research Institutes of Sweden AB genom forskningsprojekt inom cybersäkerhet samt kunskaps- och erfarenhetsutbyten gällande teknikområden och förebyggande stöd till samhället. Ett exempel på förebyggande stöd är tillhandahållande av testbäddar för cybersäkerhet. MSB och Försvarsmakten finansierar sedan 2008 en test- och övningsbädd inom cybersäkerhet, CRATE - Cyber Range and Training Environment, som utvecklas och drivs av FOI. RISE har i år inrättat en motsvarande Cyber Range med fokus test och träning. MSB, FOI och RISE genomför kunskaps- och erfarenhetsutbyten inom detta område och utforskar möjliga synergier.

Avseende uppbyggnaden och samordningen av den svenska delen av den europeiska kompetensgemenskapen, har MSB en dialog med bland andra RISE, som sedan januari 2020 driver den svenska innovationsnoden för cybersäkerhet[43]. Syftet med innovationsnoden är att sammanföra industri, akademi och offentlig sektor för att initiera framförallt innovation men även forskning inom cybersäkerhet samt att stärka Sveriges förmåga att vinna medel från forskningsprogrammen inom EU. Noden har ett antal tematiska arbetsgrupper för att diskutera behov och uppslag till innovationsprojekt samt arrangerar ”matchmaking”- aktiviteter för aktörer som vill bilda konsortier till utlysningsansökningar. Noden är medlemsdriven och bygger successivt upp en kompetensdatabas baserad på medlemmarnas profiler. MSB ingår som tidigare nämnts i styrgruppen för och är medlem i Noden.

3.3.8 Samverkan med CDIS

Centrum för cyberförsvar och informationssäkerhet (CDIS) bedriver sedan 2020 forskning och utbildning inom cybersäkerhetsområdet[44]. Idag ingår KTH, Försvarsmakten och Försvarshögskolan som parter, och det finns en ömsesidig intention att inom kort inlemma MSB, FRA och FOI. Centrumbildningen förväntas därefter fortsatt expandera genom anslutning av ytterligare myndigheter, högskolor och företag. MSB och CDIS har ett flertal kontaktpunkter, såsom gemensamma forskningsprojekt, planering av svenskt deltagande i the European Cyber Security Challenge, och svensk-amerikanskt forskningsutbyte inom cybersäkerhetsområdet. CDIS och NSC förväntas ha påtagliga kontaktytor. NSC kommer att kunna stödja CDIS med europeiska kontakter och kunskap om europeisk forsknings- och utbildningsorganisation och -finansiering inom cybersäkerhetsområdet. CDIS kan fungera som expertstöd för NSC inom specifika forsknings- och utbildningsområden inom CCCN. NSC och CDIS kan samverka för att stärka Sveriges deltagande i utformningen av den europeiska cybersäkerhetsforsknings- och utbildningsagendan.

[43] https://cybernode.se/
[44] https://www.kth.se/sv/cdis/center-for-cyber-defense-and-information-security-1.946971

3.3.9 Samverkan med NIS Samarbetsforum

CCCN-förordningen pekar särskilt på behovet av att stärka cybersäkerheten för samhällsviktiga tjänster inom de sektorer som omfattas av NIS-direktivet. Sektorerna består av energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvattenförsörjning och digital infrastruktur samt vissa digitala tjänster såsom molntjänster, digitala marknadsplatser och sökmotorer. I samband med den pågående uppdateringen av NIS-direktivet väntas antalet sektorer utökas. MSB leder NIS Samarbetsforum, som samlar regleringsmyndigheterna för leverantörerna av samhällsviktiga tjänster inom de aktuella sektorerna[45]. Forumet samarbetar kring utformning av föreskrifter, tillsynssamordning, samt utbyter erfarenheter och diskuterar cybersäkerhetsutmaningar. NSC ska samverka med NIS Samarbetsforum för att inhämta utmaningar och behov gällande cybersäkerhet för våra samhällsviktiga tjänster samt informera om aktuella EU-program och utlysningar som vänder sig till NIS-aktörerna.

3.3.10 Samverkan med MSB:s privat-offentliga samverkansforum för NIS-aktörer

Som en del i en satsning på att stärka tillämpningen av NIS-regleringen i Sverige, inrättade MSB nyligen ett privat-offentligt samverkansforum på NIS-området. I forumet ingår bransch- och verksamhetsföreträdare för leverantörer av samhällsviktiga och digitala tjänster. De representerar behovsägare och kravställare av cybersäkerhetsprodukter och -tjänster för att möta kraven i NIS-regleringen. I forumet lyfts behov och utmaningar för leverantörer av samhällsviktiga och digitala tjänster regelbundet, vilket kan bidra till NSC:s verksamhet, men forumet kan även vara relevant för att sprida information om aktuella EU-program och utlysningar, som de deltagande organisationerna kan sprida vidare till sina medlemsföretag.

3.3.11 Samverkan med MSB:s informationsdelningsnätverk inom cybersäkerhet

MSB leder ett antal tematiska informationsdelningsnätverk (FIDI) inom cybersäkerhet och som syftar till att utbyta information om erfarenheter, hot, sårbarheter, utmaningar och behov[46]. Nätverken samlar företrädare för företag och myndigheter inom t.ex. ICS/SCADA, bank- och finans, hälso- och sjukvård respektive it-drift. Dessa nätverk är viktiga behovsägare gällande vad som behöver beforskas och utvecklas för ökad cybersäkerhet. MSB uppdaterar dessa nätverk gällande utvecklingen av NSC och avser att samverka med dem när NSC är på plats.

3.3.12 Samverkan med MSB:s cybersäkerhetsråd

MSB leder cybersäkerhetsrådet, ett privat-offentligt samverkansforum bestående av etablerade och kompetenta personer från både näringslivet och offentlig sektor och som bidrar med övergripande strategiska råd till MSB:s arbete inom informations- och cybersäkerhet. Cybersäkerhetsrådet bidrar med information om utvecklingstrender inom området och synpunkter på inriktning, prioritering och genomförande av MSB:s

[45] För mer information om NIS: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/
[46] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/samverkan-inom-informationssakerhet/

verksamhet. Rådet bidrar även med kvalitetssäkring och till att sprida information om MSB:s arbete på området i omvärlden. Utifrån detta kan cybersäkerhetsrådet bidra till NSC:s strategiska arbete samt att sprida information om verksamheten i sina nätverk.

3.3.13 Samverkan med ENISA

MSB har väl upparbetade relationer med EU:s cybersäkerhetsorgan ENISA[47], i MSB:s övergripande uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet och i rollen som nationell kontaktpunkt för NIS-direktivet. ENISA har som EU:s expertorgan inom cybersäkerhet en särskilt utpekad rådgivande roll gällande genomförandet av CCCN-förordningen. I det arbetet följer ENISA utvecklingen och tar fram kartläggningar och vägledningar som stöd i arbetet med att bygga upp ekosystemet för att effektivisera europeisk forskning, innovation och kapacitetsutveckling inom cybersäkerhet. ENISA och MSB har genomfört ett antal möten gällande erfarenheter, frågeställningar och rekommendationer och har därutöver regelbundna avstämningar om status och vägen framåt. ENISA kommer fortsatt att vara en viktig samverkanspart för NSC, som en neutral part som utifrån kan agera diskussionspart och ge stöd.

3.3.14 Samverkan med NIS Cooperation Group och CSIRTs Network

MSB är Sveriges nationella kontaktpunkt gällande NIS-direktivets tillämpning samt driver den nationella CSIRT-enheten CERT-SE[48]. Inom ramen för dessa två roller företräder MSB Sverige i två EU-fora. Den strategiska samarbetsgruppen samlar medlemsstaternas nationella kontaktpunkter och verkar för en harmoniserad tillämpning av NIS-direktivet[49]. CSIRT-nätverket samlar de nationella CSIRT-enheterna för utbyte av information om sårbarheter och hot och för operativt samarbete vid gränsöverskridande incidenter[50]. Dessa båda grupper diskuterar utmaningar och behov på strategisk respektive teknisk nivå och ger värdefull kunskap om vilka cybersäkerhetssatsningar som behövs inom forskning och innovation.

3.3.15 Transatlantiskt samarbete

Sverige har ett forsknings- och utvecklingsavtal med USA, som MSB och Department of Homeland Security (DHS) förvaltar och administrerar[51]. MSB har i och med DHS-avtalet väl upparbetade kontakter i USA med aktörer, både myndigheter och forskningsmiljöer, som verkar inom cybersäkerhet. MSB har också vana av att sätta upp och även finansiera forsknings- och utvecklingsprojekt med forskare från Sverige och USA. Den transatlantiska samordningen på MSB har därmed även kontakter i den amerikanska forskarvärlden, som NSC eventuellt kan nyttja inom ramen för de krav som gäller för tredje land enligt villkoren i EU-programmen.

[47] https://www.enisa.europa.eu/
[48] https://www.cert.se/
[49] https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group
[50] https://csirtsnetwork.eu/
[51] https://www.msb.se/sv/om-msb/internationella-samarbeten/usa-och-kanada/

4 Kommande steg

Enligt CCCN-förordningen ska respektive medlemsstat utnämna den enhet som ska vara landets nationella samordningscenter senast den 29 december 2021. Medlemsstaten ska underrätta styrelsen för ECCC om den aktuella enheten. Styrelsen ska i sin tur förteckna den aktuella enheten som nationellt samordningscenter senast tre månader efter anmälan och ECCC ska offentliggöra förteckningen över utsedda nationella samordningscenter.

Under tiden förbereder MSB för ansökan till EU-kommissionen om att förvalta EU-medel för stöd till tredje part.

MSB har som mål att inviga Sveriges nationella samordningscenter under andra kvartalet 2022.

Bilaga 1: Regeringens uppdrag till MSB

Regeringen

Regeringsbeslut **II:9**

2021-09-02
Ju2021/03097

Justitiedepartementet

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad

Uppdrag till Myndigheten för samhällsskydd och beredskap att vidta förberedelser för att bli nationellt samordningscenter kopplat till det europeiska kompetenscentret för cybersäkerhet

Regeringens beslut

Regeringen uppdrar åt Myndigheten för samhällsskydd och beredskap (MSB) att vidta förberedande åtgärder och lämna förslag på hur ett nationellt samordningscenter för forskning, innovation och tillämpning inom cybersäkerhet ska kunna inrättas vid myndigheten under 2022.

Det nationella samordningscentret ska kunna utföra de uppgifter som regleras i Europaparlamentets och rådets förordning (EU) (2021/887) av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum. Uppdraget ska genomföras i samverkan med Verket för innovationssystem (Vinnova) och Myndigheten för digital förvaltning (Digg). MSB ska ha en dialog med RISE Research Institutes of Sweden AB och andra aktörer som bedöms vara relevanta.

MSB ska löpande hålla Regeringskansliet (Justitiedepartementet) informerat om uppdragets genomförande. Uppdraget ska redovisas till Regeringskansliet (Justitiedepartementet) senast den 17 november 2021.

Närmare om uppdraget

I uppdraget ingår att lämna förslag om

- inbördes ansvar och roller för MSB, Vinnova och Digg i ett nationellt samordningscenter,
- hur verksamheten vid centret kan ledas och organiseras,

Telefonväxel: 08-405 10 00
Fax: 08-20 27 34
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Herkulesgatan 17
E-post: ju.registrator@regeringskansliet.se

- hur nödvändig kapacitet att förvalta EU-finansiering säkerställs,
- hur relevant EU-finansiering kan nyttjas och följas upp,
- hur den nationella kompetensgemenskapen ska byggas upp, bl.a. i relation till det nationella cybersäkerhetscentret, och
- en långsiktig samverkansstruktur för berörda myndigheter och aktörer, såväl nationella som internationella.

MSB ska i uppdragets genomförande samverka med Vinnova i syfte att tillvarata och dra nytta av Vinnovas roll i det svenska innovationssystemet, t.ex. myndighetens förmåga och vana vid att samla forsknings-, utvecklings- och innovationsaktörer i tvärsektoriell bemärkelse samt erfarenheter och ansvar i EU-program. MSB ska även samverka med Digg utifrån myndighetens ansvar att samordna och stödja den förvaltningsgemensamma digitaliseringen liksom ansvaret för samordningen av programmet för ett digitalt Europa (DIGITAL) för perioden 2021–2027. Genomförandet av åtgärder och hanteringen av medel inom ramen för programmets specifika mål om cybersäkerhet och förtroende ska genomföras genom det europeiska kompetenscentret för cybersäkerhet (ECCC) och nätverket av nationella samordningscenter.

Skälen för regeringens beslut

Europaparlamentets och rådets förordning (2021/887) av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum, trädde i kraft den 28 juni 2021. Enligt förordningen ska ECCC bl.a. fastställa strategiska rekommendationer för forskning, innovation och tillämpning inom cybersäkerhet. En kompetensgemenskap ska också bildas för att föra samman de viktigaste intressenterna inom teknisk, industriell, akademisk och forskningsrelaterad kapacitet inom cybersäkerhet i unionen. De nationella samordningscentren ska bl.a. fungera som kontaktpunkt på nationell nivå för kompetensgemenskapen för att stödja ECCC. Senast den 29 december 2021 ska medlemsstaterna nominera ett nationellt samordningscenter.

MSB har i uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet. Myndigheten är nationell kontaktpunkt enligt 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). MSB ingår även i det

2 (3)

nationella cybersäkerhetscentret tillsammans med Försvarsmakten, Försvarets radioanstalt och Säkerhetspolisen. MSB har också teknisk expertis inom cybersäkerhet och finansierar forskning inom området.

På regeringens vägnar

Mikael Damberg

Carolina Sandö

Kopia till

Statsrådsberedningen/SAM och EUKANSLI
Finansdepartementet/BA
Näringsdepartementet/N EIN
Infrastrukturdepartementet/ESD
Myndigheten för digital förvaltning
Verket för innovationssystem

3 (3)

Bilaga 2: Uppdragets genomförande

Detta regeringsuppdrag har MSB genomfört i samverkan med Vinnova och DIGG.

Med Vinnova har MSB framförallt behandlat frågor om styrning, organisation, samverkan samt utveckling av kompetensgemenskapen.

Med DIGG har MSB framförallt behandlat frågor om styrning, organisation samt samverkan.

MSB har med Vinnova och DIGG genomfört workshops och veckovisa avstämningsmöten, texter har författats av MSB och skickats till Vinnova och DIGG för återkoppling och texter har författats av Vinnova respektive DIGG som bidrag till återrapporteringen till regeringen.

Dialoger har under regeringsuppdraget förts med RISE, Tillväxtverket, PTS, Energimyndigheten, Rymdstyrelsen, Sweden ICT, ISACA Sweden, CDIS, Justitiedepartementet, NIS samarbetsforum, EU-kommissionen, Concordia, finska NESA och NCSC-FI samt ett urval av andra relevanta aktörer.

MSB har med RISE haft täta dialoger gällande förhållandet mellan den kommande kompetensgemenskapen och den innovationsnod för cybersäkerhet som RISE inrättade i januari 2020. Övriga samverkansgränssnitt har också diskuterats, t.ex. testbäddar för cybersäkerhet (CRATE och RISE Cyber Range).

Vinnova, DIGG, RISE, Tillväxtverket, Energimyndigheten och Luleå tekniska universitet har beretts möjlighet att ge återkoppling på utkastet till redovisningen av regeringsuppdraget.

Bilaga 3: Begreppslista

CCCN	EU:s kompetenscentrum för cybersäkerhet och nätverket av nationella samordningscentrum
CCCN-förordningen	Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum
Cybersäkerhet	All verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra personer som berörs av cyberhot (från CCCN-förordningen)
Cyberhot	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 (från CCCN-förordningen)
ECCC	EU:s kompetenscentrum för cybersäkerhet
EDIH	Europeisk digital innovationshub
NCC	National Coordination Centre
NIS	Network and Information Security
NSC	Nationellt samordningscenter
SMF	Små och medelstora företag

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984