Redovisning av regeringsuppdrag FÖ2025/00388

Nationell operativ plan för hantering av storskalig cybersäkerhetsincident och kris

NATIONELLT CYBERSÄKERHETSCENTER

En del av FRA

Nationellt cybersäkerhetscenter, NCSC, är sedan 2024 en del av Försvarets radioanstalt, FRA.

NCSC har lett arbetet med att ta fram en nationell operativ plan för hantering av storskalig cybersäkerhetsincident och cyberkris.

FRA fick regeringsuppdraget i februari 2025 och uppdraget redovisades 1 december 2025.

Förord

En allt snabbare digitalisering samt ett försämrat säkerhetspolitiskt läge, i kombination med att cyberhotet ökat både sett till omfattning och komplexitet, innebär att kraven på Sveriges förmåga att säkra, skydda och stärka samhällets funktioner även i cyberdomänen höjts.

Digitaliseringen har fört med sig enorma möjligheter såsom snabbare innovation, effektivare myndigheter, nya affärsmodeller. Men den har också fört med sig sårbarheter. Vi har sett hur cyberhoten vuxit i omfattning, komplexitet och tempo. Kriminella nätverk använder cyberangrepp för utpressning och finansiell vinning. Statliga aktörer testar vår motståndskraft via påverkansoperationer, där cyberattacker används för att underminera förtroendet för institutioner och vårt demokratiska samhälle.

En storskalig cybersäkerhetsincident eller cyberkris skulle ha stor påverkan på det svenska samhället. Även mindre incidenter kan få omfattande nationella konsekvenser. En nationell operativ plan för hantering av storskaliga cybersäkerhetsincidenter och kriser utgör därför en viktig del i arbetet att stärka vår nationella digitala motståndskraft och Sveriges samlade förmåga att effektivt kunna hantera incidenter och kriser.

Planens utgångspunkt är att Sveriges förmåga att hantera allvarliga cybersäkerhets-incidenter kräver nära samverkan och informationsdelning mellan ansvariga myndigheter, Regeringskansliet, drabbade och berörda verksamhetsutövare, med beaktande av den nationella kris- och beredskapsstrukturen. Motsvarande planer utarbetas nu av alla EU-länder vilket möjliggör gemensam situationsmedvetenhet och tidig varning vid gränsöverskridande hot.

Cyberkrishanteringsplanen har utformats för att kunna utgöra en första basplatta för att utveckla det nationella cyberkrishanteringsarbetet i samarbete med företag, myndigheter och andra intressenter. Det pågår just nu en större omorganisering av ansvar och uppdrag på cybersäkerhetsområdet i Sverige. Jag ser därför fram emot att involvera en bredare krets av nationella berörda myndigheter och verksamhetsutövare i kommande uppdatering av denna plan för att spegla de nya ansvarsförhållandena.

Jag vill rikta ett stort tack till alla myndigheter och organisationer som deltagit i framtagningen av planen och bidragit med viktiga underlag.

Denna plan blir en möjlighet att stegvis vidareutveckla det nationella arbetet med att stärka det svenska samhällets förmåga att hantera storskaliga cybersäkerhetsincidenter och kriser. Ett Sverige med en hög nivå av cybersäkerhet bygger vi inte var för sig, det gör vi tillsammans.

John Billow,
chef, Nationellt cybersäkerhetscenter, en del av FRA

Innehåll

1. En nationell cyberkrishanteringsplan

Enligt artikel 9.4 i NIS 2-direktivet[1] ska alla medlemsstater i Europeiska Unionen (EU) anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och cyberkriser (cyberkrishanteringsplanen). Mot denna bakgrund gav regeringen den 27 februari 2025 Försvarets radioanstalt (FRA) i uppdrag att utarbeta en sådan plan (Fö2025/00388). I och med denna redovisning är regeringsuppdraget slutfört.

Cyberkrishanteringsplanen har utformats för att kunna utgöra en grundplatta för fortsatt utveckling av det nationella cyberkrishanteringsarbetet i samarbete med företag, myndigheter och andra intressenter.

Planens utformning som grundplatta har anammats då det är Sveriges första nationella operativa cyberkrishanteringsplan. I nuläget sker även stora förändringar i det nationella cybersäkerhetsarbetet. Bland annat ska NIS 2-direktivet implementeras och det finns det ett förslag om att inrätta en ny funktion för operativ krishantering i den finansiella sektorn.[2] Den 20 november 2025 gav regeringen FRA och Myndigheten för samhällsskydd och beredskap (MSB) i uppdrag att förbereda överföringen av informations- och cybersäkerhetsverksamheten som idag bedrivs vid MSB, i enlighet med förslagen i utredningen Samlade förmågor för ökad cybersäkerhet (SOU 2025:79). Uppdraget ska genomföras så att verksamhetens uppgifter kan integreras i Nationellt cybersäkerhetscenter (NCSC) den 1 juli 2026 och innebär att FRA då får rollen som cyberkrishanteringsmyndighet (CKHM).

Cyberkrishanteringsplanen syftar av denna anledning i första hand till att tydliggöra ansvar och uppgifter kopplat till nationell operativ incidenthantering. Planens primära målgrupp är de aktörer som är direkt involverade i nationell operativ incidenthantering inom ramen för verksamheten som bedrivs och koordineras av NCSC. Förutom NCSC inkluderar dessa CKHM och de av regeringen utpekade så kallade. samverkansmyndigheterna[3]: Försvarets materielverk (FMV), Försvarsmakten, MSB, Polismyndigheten, Post-och telestyrelsen (PTS) och Säkerhetspolisen.

Vid framtagandet av planen har FRA beaktat MSB:s tidigare förslag till nationell plan för hantering av cybersäkerhetsincidenter och kriser.[4] FRA har även i tre omgångar inhämtat synpunkter på cyberkrishanteringsplanen från samverkansmyndigheterna, Energimyndigheten, Finansinspektionen (FI), Sveriges Kommuner och Regioner (SKR) och Svenskt Näringsliv.

Arbetet med att uppdatera cyberkrishanteringsplanen kommer att påbörjas skyndsamt. I detta arbete kommer en bredare krets av nationella berörda myndigheter och

[1] Europaparlamentets och rådets direktiv (EU) 2022/2055 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 (NIS 2-direktivet).

[2] Se En ny funktion för operativ krishantering i den finansiella sektorn (utkast till lagrådsremiss), Regeringskansliet, Fi2025/01510.

[3] § förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt.

[4] Sveriges cyberkrishanteringsplan – förslag till nationell plan för hantering av cybersäkerhetsincidenter och kriser – åtgärder för en samlad hantering, MSB:s dnr 2023-17571-4. 4.

verksamhetsutövare kunna involveras. Likaså kommer den uppdaterade planen kunna ta höjd för ökad komplexitet och ytterligare scenarier än vad som omständigheterna medger i denna första version och bygga vidare på kopplingen till det nationella kris- och beredskapsramverket. Det möjliggör även för bredare samordning med EU-arbetets utveckling på området.

1.1 Utgångspunkter

Vid betydande cybersäkerhetsincident, med potential att eskalera till en storskalig cybersäkerhetsincident, har politiska beslutsfattare tidskritiska behov av information och underlag. Löpande informationsdelning och samverkan med Regeringskansliet utgör därför en betydelsefull del av cyberkrishanteringsplanen.

Likaså är samverkan och informationsdelning mellan NCSC, samverkansmyndigheterna, drabbade eller berörda myndigheter och verksamhetsutövare avgörande för att stärka de nationella förutsättningarna att begränsa konsekvenserna av betydande cybersäkerhetsincidenter. Av denna anledning utgör samverkansstrukturen en viktig del av planen.

De verksamhetsmoment som ingår i nationell operativ incidenthantering ska kunna utföras under snäva tidsförhållanden och i krissituationer. Tidigare upparbetade arbetssätt är ofta enklare att tillämpa även under mer utmanande förhållanden. Av denna anledning efterliknar cyberkrishanteringsplanens nationella operativa hantering av storskaliga cybersäkerhetsincidenter och cyberkriser dess motsvarighet för cybersäkerhetsincidenter av lägre allvarlighetsgrad. .

Cyberkrishanteringsplanen utgår från de rekommendationer till medlemsstater som anges i EU:s så kallade Cyberplan.[5] För att cyberkrishanteringsplanen ska vara interoperabel med EU:s cyberkrishanteringsstruktur används EU:s definitioner av incidenttyper (se sidan 10). Av samma skäl tillämpar cyberkrishanteringsplanen Cyberplanens definition av vad som utgör teknisk och operativ nivå. Detta innebär att nationell CSIRT (*Computer Security Incident Response Team*) anses utföra nationell incidenthantering på teknisk nivå, medan CKHM och NCSC agerar och utför nationell incidenthantering på operativ nivå.

Cyberkrishanteringsplanen förutsätter att cybersäkerhetsincidenter i någon aspekt hanteras på teknisk nivåoch utgår därför från att nationell CSIRT vanligtvis är den nationella funktion som först uppmärksammas på en nationell incident. Nationell CSIRT är därför även vanligtvis den funktion som gör en initial bedömning av incidentens allvarlighetsgrad och, om incidenten är tillräckligt allvarlig, informerar NCSC om att det kan finnas behov av att aktivera nationell operativ incidenthantering.

Cyberkrishanteringsplanen förhåller sig dock neutral till hur en incident kommer till NCSC:s eller nationell CSIRT:s kännedom. Planen tar sålunda höjd för att information om incidenter kan inkomma på olika sätt, och inte enbart genom formell incidentrapportering till nationell CSIRT.

[5] Rådets rekommendation av den 6 juni 2025 om en EU-plan för hantering av cyberkriser (C/2025/3445).

Storskaliga cybersäkerhetsincidenter och cyberkriser kan vara resultat av incidenter som eskalerat i allvarlighetsgrad över tid. För att förstå om en incident föranleder aktivering av nationell operativ incidenthantering eller inte, beskriver planen även nationell operativ hantering av incidenter av lägre allvarlighetsgrad än enbart storskaliga cybersäkerhetsincidenter och cyberkriser.

Nationell operativ incidenthantering och de verksamhetsmoment som ingår i denna utförs inom ramen för NCSC:s verksamhet. Denna verksamhet innefattar samarbete mellan NCSC och samverkansmyndigheterna i enlighet med förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvaretsradioanstalt (NCSC-förordningen). För mer om detta samt NCSC:s roll och ansvar se appendix 4.

Enligt artikel 16.2 i NIS 2-direktivet ska det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) bland annat bestå av företrädare för medlemsstaternas cyberkrishanteringsmyndigheter. CKHM representerar sålunda Sverige i detta forum. CKHM:s uppgifter och ansvarsområden på nationell nivå anges däremot inte i NIS 2-direktivet, utan ska enligt direktivet anges i cyberkrishanteringsplanen. För CKHM:s uppgifter och ansvarsområden inom ramen för planen, se avsnitt 2 fas 2, 3, och 4.

Cyberkrishanteringsplanen antar ett myndighetsneutralt perspektiv vad gäller nationell CSIRT och CKHM. Det innebär att cyberkrishanteringsplanen inte tillskriver dessa funktioner någon uttalad myndighetsbehörighet. Detta görs för att cyberkrishanterings-planen ska kunna användas oavsett vilken myndighet som har dessa roller.

Som nämndes ovan kommer rollen som CKHM övergå till FRA den 1 juli 2026. Med anledning av detta kan delar av planen därefter behöva uppdateras för att reflektera förändrade ansvarsförhållanden.

Vidare utgår cyberkrishanteringsplanen från att NCSC enbart klassificerar en storskalig cybersäkerhetsincident från ett nationellt perspektiv, och mer specifikt om Sverige drabbats av en incident som orsakar störningar som är så omfattande att Sverige inte kan hantera dessa.

Om en annan EU-medlemsstat drabbats av motsvarande incident från ett nationellt perspektiv utgår cyberkrishanteringsplanen från att den drabbade medlemsstaten gör denna klassificering.

Det framgår varken av NIS 2-direktivet eller av Cyberplanen vilken myndighet eller vilket organ som klassificerar om det inträffat en storskalig cybersäkerhetsincident eller om en cyberkris brutit ut. Av Cyberplanen framgår dock att CSIRT-nätverket rekommenderas att ge EU-CyCLONe råd om en observerad cybersäkerhetsincident kan betraktas som en potentiell eller pågående storskalig cybersäkerhetsincident. Cyberkrishanteringsplanen utgår därför från antagandet att det inom ramen för EU-CyCLONe görs en klassificering huruvida minst två EU-medlemsstater drabbats av en incident som har en betydande påverkan på dem, och därmed utgör en storskalig cybersäkerhetsincident, alternativt om en cyberkris brutit ut. För definitioner av olika incidenttyper se sidan 10.

I planen anges NCSC, snarare än CKHM, klassificera incidenter från ett nationellt perspektiv. Det första skälet till detta är att CKHM formellt övertar ansvaret för hantering av storskaliga cybersäkerhetsincidenter och kriser först *efter* att en

incident klassificerats som en storskalig cybersäkerhetsincident från ett nationellt perspektiv. Eftersom denna klassificering görs när NCSC fortfarande har ansvar för nationell hantering är det därför lämpligt att NCSC även gör klassificeringen. Det andra skälet är att det blir tydligare om samma funktion klassificerar incidenter från ett nationellt perspektiv i samtliga faser av cyberkrishanteringsplanen..

För att cyberkrishanteringsplanen ska vara flexibel och fungera i en övergångsperiod går den inte in i detalj på hur varje verksamhetsmoment utförs. Istället beskriver planen på ett övergripande sätt de verksamhetsmoment som ska genomföras inom ramen för nationell operativ incidenthantering, och av vem.

Cyberkrishanteringsplanen ska övas både nationellt och inom ramen för EU:s unions-övergripande övningar för storskaliga cybersäkerhetsincidenter och cyberkriser. Cyberkrishanteringsplanen ska även uppdateras över tid, i takt med att planen används och utvärderas. För mer om övningsverksamheten se appendix 3.9.

1.1.1 Cyberkrishantering i den nationella ramen för krishantering

Cyberkrishanteringsplanen syftar till att stärka den nationella operativa incident-hanteringen av cyberaspekten av allvarliga cybersäkerhetsincidenter. Efterföljande störningar av dessa incidenter hanteras däremot inom ramen för den bredare kris- och beredskapsstrukturen och av de sektorer som drabbats av incidenten enligt ansvarsprincipen.

För att gemensamt verka för att stärka de nationella förutsättningarna att begränsa konsekvenserna av betydande cybersäkerhetsincidenter krävs nära samverkan mellan NCSC, samverkansmyndigheterna, och den nationella kris- och beredskapsstrukturen, inklusive sektorsansvariga myndigheter. Denna samverkan utgör alltså en viktig del av cyberkrishanteringsplanen. Planen beskriver därför på ett övergripande sätt i fas 2 och 3 hur formerna för cyberkrishantering integreras i den allmänna nationella ramen för krishantering samt kanaler för informationsutbyte.

1.1.2 Avgränsningar

Detaljerna kring hantering av cybersäkerhetsincidenter som utgör säkerhetsskydds-incidenter eller information om incidenter som innehåller säkerhetsskyddsklassificerad information, exempelvis säkerhets- och försvarsunderrättelser, hanteras i särskild ordning mellan berörda myndigheter. Av denna anledning lämnas denna hantering utanför cyberkrishanteringsplanen.

Slutligen finns det enligt nätkoderna[6] möjlighet att låta cyberkrishanteringsplanen även utgöra en nationell plan för hantering av cyberkriser som avser gränsöverskridande elflöden. Denna första cyberkrishanteringsplan avser dock att inte utgöra en sådan nationell plan. Cyberkrishanteringsplanens utformning medger dock möjligheten att inkorporera denna aspekt i en uppdaterad version av planen.

[6] Kommissionens delegerade förordning (EU) 2024/1366 av den 11 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden (nätkoderna).

Incidentkategorier och ansvar nationell incidenthantering

Incidentkategorier	Definition	Vem klassificerar	Ansvar nationell operativ incidenthantering
Betydande incident	”En incident som: a) har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten, b) har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.”[7]	N/A	N/A
Betydande incident med potential att eskalera till en storskalig cyber-säkerhetsincident	Enligt definitionen av betydande incident och storskalig cybersäkerhetsincident	NCSC	NCSC Se fas 2
Storskalig cyber-säkerhetsincident	”En incident som orsakar störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater.”[8]	NCSC klassificerar från nationellt perspektiv (om incident inträffat som är så omfattande att Sverige inte kan hantera dess störningar) Annan EU-medlemsstat klassificerar från sitt nationella perspektiv (om incident inträffat som är så omfattande att medlemsstaten inte kan hantera dess störningar) EU-CyCLONe klassificerar från ett unionsperspektiv (om en incident inträffat som har en betydande påverkan på minst två medlemsstater)	CKHM Se fas 3
Cyberkris	”En storskalig cybersäkerhetsincident som eskalerat till en fullt utvecklad kris som hindrar den inre marknaden från att fungera korrekt eller som allvarligt hotar den allmänna tryggheten och säkerheten för entiteter eller medborgare i flera medlemsstater eller i unionen som helhet.”[9]	EU-CyCLONe klassificerar	CKHM Se fas 3

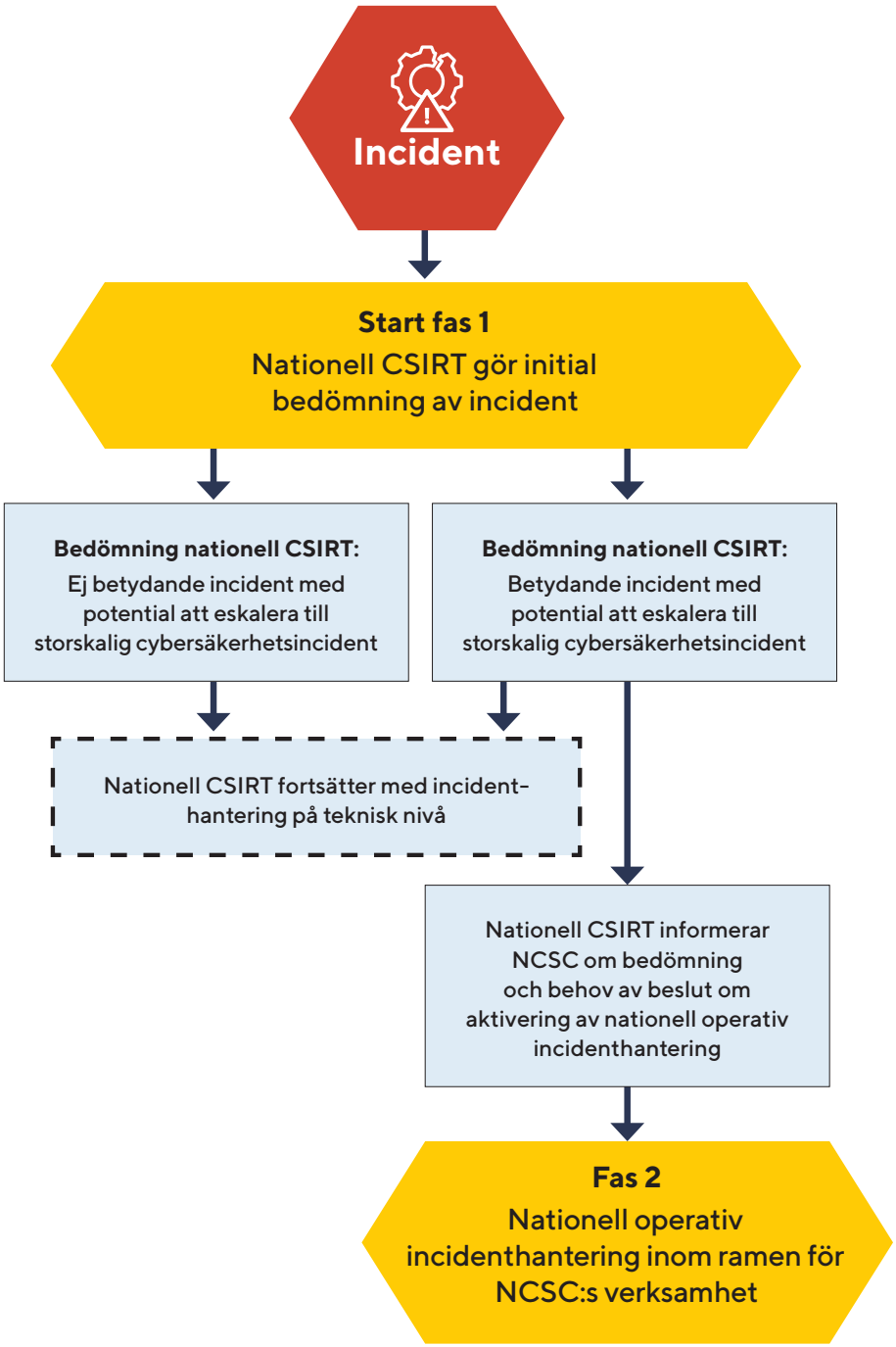
[7] Artikel 23.3 NIS 2-direktivet.

[8] Artikel 6.7 NIS 2-direktivet.

[9] Artikel 7d Cyberplanen.

2. Nationell operativ plan för storskalig cybersäkerhetsincident och cyberkris

Fas 1: Detektion och klassificering



2.1 Fas 1: Detektion och initial bedömning av allvarlighetsgrad

När en incident kommer till nationell CSIRT:s kännedom görs en initial bedömning av incidentens allvarlighetsgrad. Mer specifikt bedömer nationell CSIRT om incidenten utgör en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident eller ej.

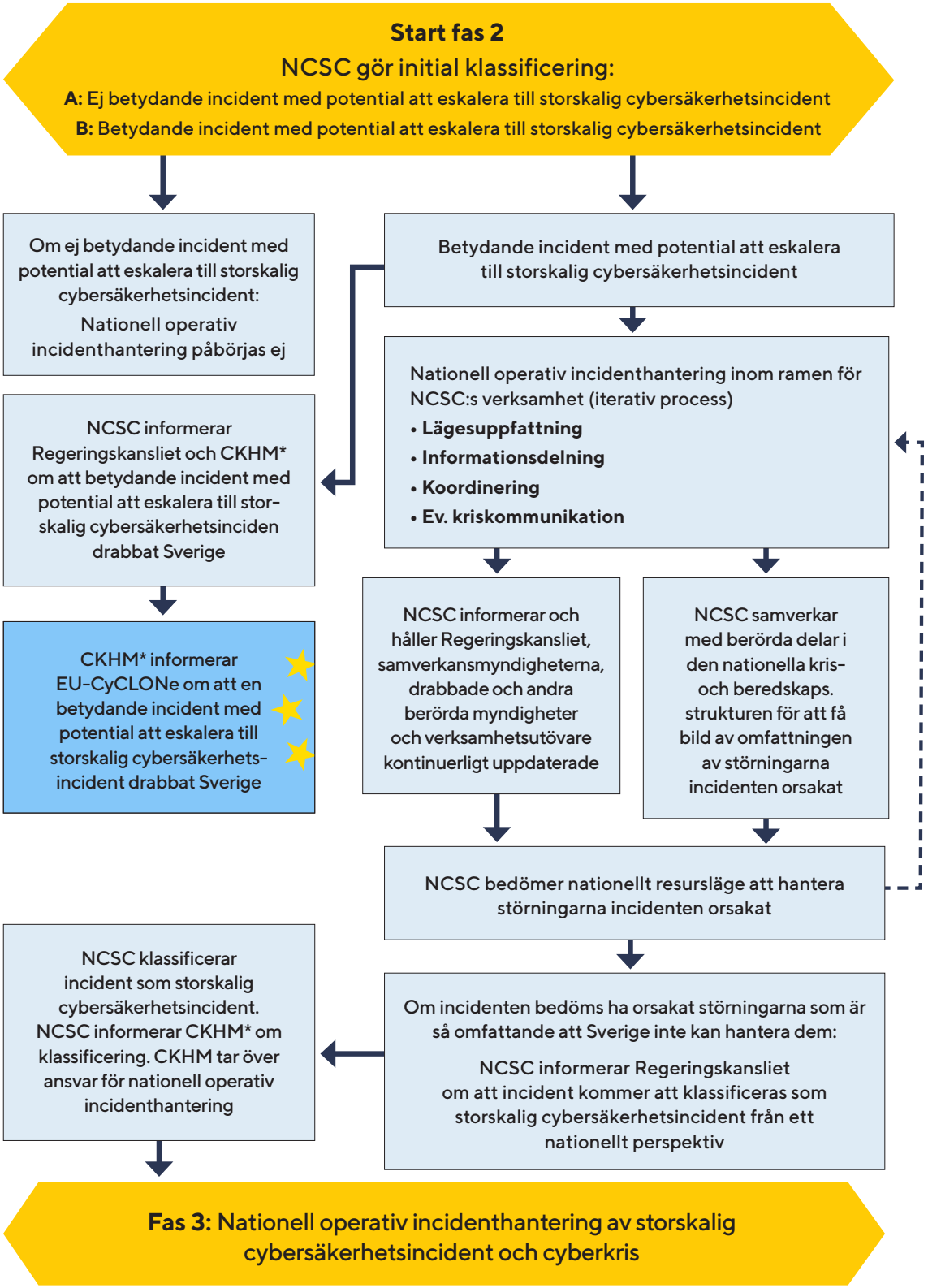
Om nationell CSIRT bedömer att incidenten utgör en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident föranleder detta att nationell CSIRT informerar NCSC. Genom att informera NCSC om bedömningen så påtalar nationell CSIRT att det kan finnas behov av beslut om att aktivera nationell operativ incidenthantering inom ramen för NCSC:s verksamhet (se fas 2).

Om nationell CSIRT bedömer att incidenten inte utgör en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident men kräver hantering på teknisk nivå genomför nationell CSIRT denna enligt ordinarie rutin.

Eskalerar en incident som tidigare bedömts inte utgöra en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident, blir den föremål för en ny bedömning. Bedömer nationell CSIRT då att incidenten utgör en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident informeras NCSC (se fas 2).

Om incidenten fortsatt kräver hantering på teknisk nivå genomför nationell CSIRT denna enligt ordinarie rutin.

Fas 2: Nationell operativ incidenthantering av betydande incident med potential att eskalera till storskalig cybersäkerhetsincident



* CKHM = Cyberkrishanteringsmyndighet

2.2 Fas 2: Klassificering och nationell operativ incidenthantering av betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident

2.2.1 Initial incidentklassificering på operativ nivå av NCSC

Efter att NCSC informerats om CSIRT:s initiala bedömning att en incident inträffat som utgör åtminstone en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident gör NCSC en egen incidentklassificering. NCSC kan även klassificera incidenter som inkommit på annat sätt än via nationell CSIRT.

Antingen klassificerar NCSC att incidenten

a. inte utgör en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident, eller
b. utgör en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident

Anses incidenten inte utgöra en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident påbörjas inte nationell operativ incidenthantering inom ramen för NCSC:s verksamhet. I sådana fall informerar NCSC nationell CSIRT att man gjort en annan bedömning.

Anser NCSC att incidenten utgör en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident informeras Regeringskansliet och CKHM om klassificeringen och att nationell operativ incidenthantering inom ramen för NCSC:s verksamhet påbörjats.

CKHM informerar i sin tur resten av EU-CyCLONe om att Sverige drabbats av en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident.

2.2.2 NCSC ansvarar för nationell operativ incidenthantering

NCSC ansvarar för nationell operativ incidenthantering av betydande incidenter med potential att eskalera till storskaliga cybersäkerhetsincidenter. Verksamhetsmomenten som ingår i nationell operativ incidenthantering utförs kontinuerligt inom ramen för NCSC:s verksamhet allt eftersom incidenten utvecklas och ny information inkommer.

Regeringskansliet, samverkansmyndigheterna, drabbade och berörda myndigheter och verksamhetsutövare hålls kontinuerligt uppdaterade om incidenten och dess utveckling. Beroende på incidentens natur och efterföljande störningar som den orsakar kan berörda myndigheter innefatta exempelvis myndigheter i den nationella kris- och beredskapsskapsstrukturen och sektorsansvariga myndigheter. Likaså kan berörda verksamhetsutövare innefatta flertalet olika slags verksamhetsutövare som på olika sätt berörs av incidenten.

I genomförandet av de olika verksamhetsmomenten som utgör nationell operativ incidenthantering samarbetar NCSC med samverkansmyndigheterna enligt vad som anges i NCSC-förordningen.

Verksamhetsmomenten som ingår i nationell operativ incidenthantering innefattar:

- **Informationsdelning:** NCSC, samverkansmyndigheterna, drabbade och berörda myndigheter och verksamhetsutövare delar aktuell information om incidenten, dess konsekvenser, hur man kan skydda sig, vidta åtgärder för att minimera negativa följder, samt återgå till normalläge.

  Nationellt delas relevant information till berörda delar av kris- och beredskapsstrukturen samt till sedan tidigare etablerade sektorspecifika och andra forum för samverkan. Om inget relevant forum finns etablerat kan NCSC etablera ett tillfälligt forum för en specifik incident.

  Information delas även internationellt till olika nätverk kopplat till cybersäkerhet och incidenthantering som Sverige deltar i.

- **Lägesuppfattning:** Baserat på informationsdelning och andra källor sammanställs tillgänglig information kontinuerligt och resulterar i en bredare analys av incidenten, som vid behov ger förslag på åtgärder som bör vidtas. Analysen resulterar i en fördjupad rapport som redogör för vad som hänt och nuvarande incidentstatus.

  Rapporten delas med Regeringskansliet, samverkansmyndigheterna, samt drabbade och berörda myndigheter och verksamhetsutövare. Rapporteringsfrekvensen beror primärt på incidentutvecklingen och hur prioriterat informationsbehovet är hos mottagarna.

- **Koordinering:** NCSC, samverkansmyndigheterna, drabbade och berörda myndigheter och verksamhetsutövare genomför incidentkoordinering. Detta innefattar att kommunicera kring och samordna information, resurser och kompetenser på nationell nivå.

  Utöver detta så koordinerar NCSC med den bredare kris- och beredskapsstrukturen i syfte att följderna av störningarna ska bli så begränsade som möjligt. NCSC deltar i nationella samverkanskonferenser som anordnas av den nationella kris- och beredskapsstrukturen för att utbyta information om incidenten, dess konsekvenser och vilka åtgärder som vidtas. Denna samverkan säkerställer att relevant information utbyts mellan NCSC och de som hanterar de uppkomna störningarna som incidenten orsakat eller på annat sätt berörs av incidenten.

- **Eventuell kriskommunikation:** Vid behov samordnar NCSC kommunikation kring incidenten med samverkansmyndigheterna, drabbade och berörda myndigheter och verksamhetsutövare. Respektive myndighet och verksamhetsutövare bestämmer själva huruvida de vill använda gemensamt framtagna talepunkter. Syftet med att koordinera kriskommunikation är att ge allmänhet och media saklig, korrekt och enhetlig information om incidenten och motverka felaktig ryktesspridning. Innan NCSC förmedlar framtagna talepunkter till allmänheten och media informeras Regeringskansliet om vad dessa innefattar.

- **Nationellt resursläge:** Samverkan med den bredare nationella kris- och beredskapsstrukturen ger också NCSC en förståelse för omfattningen av störningarna som incidenten orsakat. Baserat på denna uppfattning gör NCSC en bedömning av det nationella resursläget och möjligheterna att hantera incidentens konsekvenser.

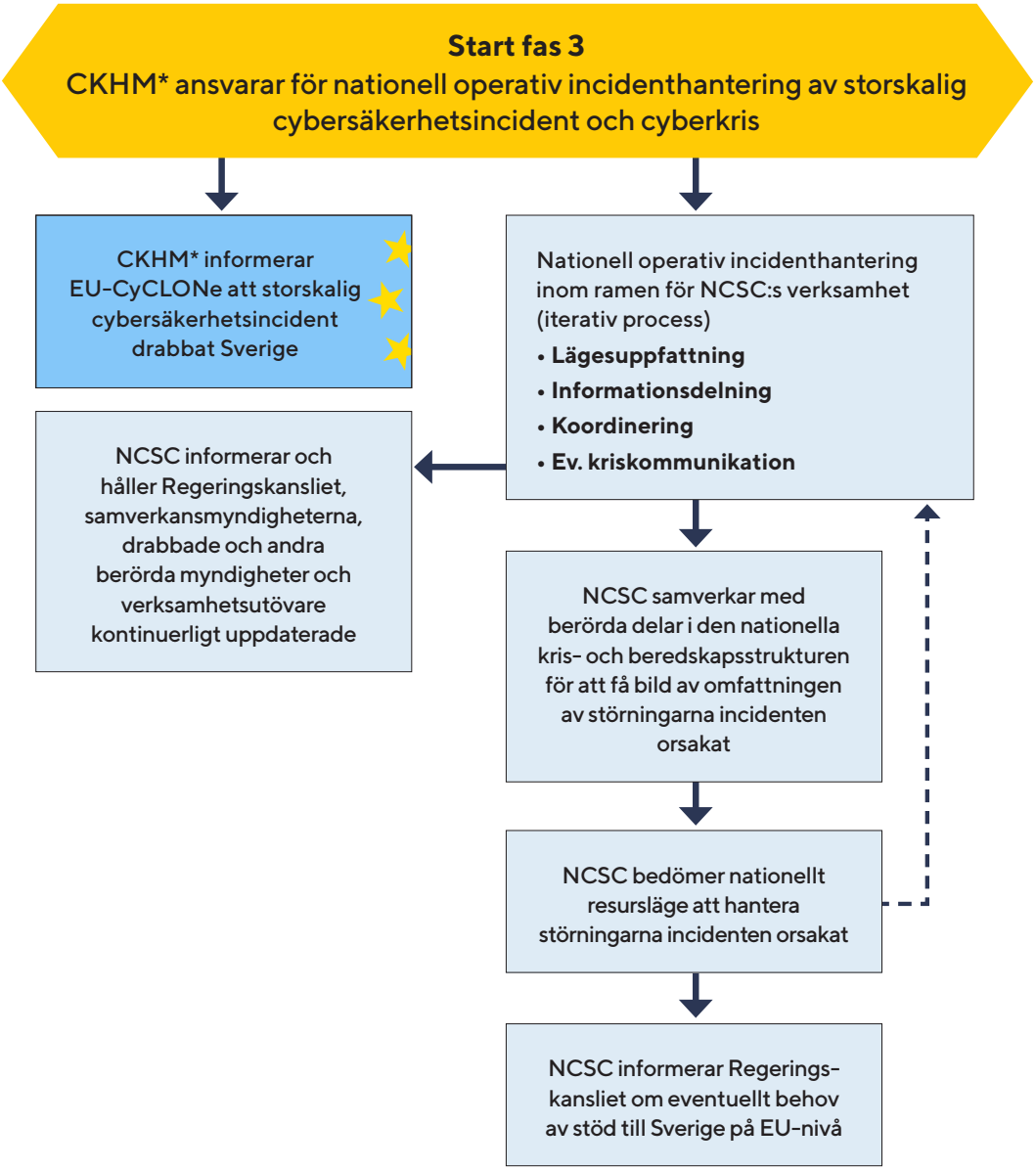
  Bedömningen utgör i sin tur ett nytt ingångsvärde för den kontinuerligt pågående nationella operativa incidenthanteringen och de verksamhetsmoment som genomförs inom ramen för denna.

  En bedömning av nationellt resursläge krävs för att NCSC ska kunna avgöra huruvida kraven för en storskalig cybersäkerhetsincident från ett nationellt perspektiv är uppfyllda. Detta eftersom en storskalig cybersäkerhetsincident från ett nationellt perspektiv definieras som en incident som orsakar störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem. Av denna anledning är en bedömning möjlig först efter närmare samverkan mellan NCSC och berörda parter i den nationella kris- och beredskapsstrukturen.

- **Om aktuellt: Klassificering av storskalig cybersäkerhetsincident**
  Bedömer NCSC att Sverige inte kan hantera de störningar som incidenten har orsakat så är kriterierna för en storskalig cybersäkerhetsincident från ett nationellt perspektiv uppfyllda. NCSC informerar Regeringskansliet om att man planerar att klassificera incidenten som en storskalig cybersäkerhetsincident. Efter att Regeringskansliet informerats klassificerar NCSC incidenten som en storskalig cybersäkerhetsincident och informerar CKHM om detta. I och med klassificeringen tar CKHM över ansvaret för den nationella hanteringen.

  Om incidenten fortsatt kräver hantering på teknisk nivå genomför nationell CSIRT denna enligt ordinarie rutin.

Fas 3: Nationell operativ incidenthantering av storskaliga cybersäkerhets-incidenter och cyberkriser



* CKHM = Cyberkrishanteringsmyndighet

2.3 Fas 3: Klassificering och nationell operativ incidenthantering av storskalig cybersäkerhetsincident och cyberkris

2.3.1 Klassificering

När någon av nedanstående fyra incidentklassificeringar gjorts påbörjas nationell operativ incidenthantering av storskalig cybersäkerhetsincident eller cyberkris inom ramen för NCSC:s verksamhet:

1. NCSC klassificerar incident som storskalig cybersäkerhetsincident från ett nationellt perspektiv (sker i fas 2),
2. En annan EU-medlemsstat klassificerar en incident som storskalig cyber-säkerhetsincident från sitt nationella perspektiv,
3. EU-CyCLONe klassificerar en incident som storskalig cybersäkerhetsincident om en incident inträffat som har en betydande påverkan på minst två EU-medlemsstater, eller
4. EU-CyCLONe klassificerar att en cyberkris brutit ut

Om Sverige utsatts för en storskalig cybersäkerhetsincident från ett nationellt perspektiv informerar CKHM resten av EU-CyCLONe.

Om en annan EU-medlemsstat bedömer att de drabbats av en storskalig cyber-säkerhetsincident från ett nationellt perspektiv kan medlemsstaten informera EU-CyCLONe. CKHM nås först av denna information via sina företrädare i EU-CyCLONe. CKHM informerar i sin tur Regeringskansliet och NCSC.

Incidentrapportering från EU-medlemsstater ger EU-CyCLONe ett samlat informations-läge som möjliggör för EU-CyCLONe att bedöma och klassificera huruvida en incident som har en betydande påverkan på minst två EU-medlemsstater har inträffat, och därmed utgör en storskalig cybersäkerhetsincident. CKHM nås först av denna information via sina företrädare i EU-CyCLONe. CKHM informerar i sin tur Regeringskansliet och NCSC om detta.

EU-CyCLONes samlade informationsläge möjliggör även för EU-CyCLONe att bedöma om en cyberkris – det vill säga att ”en storskalig cybersäkerhetsincident som eskalerat till en fullt utvecklad kris inträffat som hindrar den inre marknaden från att fungera korrekt eller som allvarligt hotar den allmänna tryggheten och säkerheten för entiteter eller medborgare i flera medlemsstater eller i unionen som helhet” - inträffat. CKHM nås först av denna information via sina företrädare i EU-CyCLONe. CKHM informerar i sin tur Regeringskansliet och NCSC om detta.

2.3.2 Nationell operativ incidenthantering påbörjas oavsett om Sverige drabbats eller inte

Nationell operativ hantering av storskalig cybersäkerhetsincident och cyberkris inom ramen för NCSC:s verksamhet påbörjas oavsett om det är Sverige eller någon eller några andra EU-medlemsstater som direkt drabbats.

Anledningen till detta är att NCSC behöver förstå hur den storskaliga cybersäkerhets-incidenten eller cyberkrisens direkta eller indirekta spridningseffekter påverkar eller kan komma att påverka Sverige.

Detta kan vara fallet i tre scenarier:

1. om annan EU-medlemsstat har drabbats av en storskalig cybersäkerhetsincident från ett nationellt perspektiv,
2. om EU-CyCLONe bedömer att en incident inträffat som har betydande påverkan på minst två medlemsstater (varav ingen är Sverige) och därmed uppfyller kriterierna för en storskalig cybersäkerhetsincident, eller
3. om EU-CyCLONe bedömer att en cyberkris brutit ut, det vill säga att "en storskalig cybersäkerhetsincident som eskalerat till en fullt utvecklad kris inträffat som hindrar den inre marknaden från att fungera korrekt eller som allvarligt hotar den allmänna tryggheten och säkerheten för entiteter eller medborgare i flera medlemsstater" (men inte Sverige).

2.3.3 CKHM ansvarar för nationell hantering

CKHM ansvarar för den nationella hanteringen av storskaliga cybersäkerhetsincidenter och cyberkriser.

Verksamhetsmomenten som ingår i nationell operativ incidenthantering utförs inom ramen för NCSC:s verksamhet, och kontinuerligt, allt eftersom incidenten utvecklas och ny information inkommer. För att underlätta operativ incidenthantering är dessa i stort detsamma som genomförs i händelse av en betydande incident med potential att eskalera till en storskalig cybersäkerhetsincident.

Regeringskansliet, samverkansmyndigheterna, drabbade och berörda myndigheter och verksamhetsutövare hålls kontinuerligt uppdaterade om incidenten och dess utveckling. Beroende på incidentens natur och efterföljande störningar som den orsakar kan berörda myndigheter innefatta exempelvis myndigheter i den nationella kris- och beredskapsskapsstrukturen och sektorsansvariga myndigheter. Likaså kan berörda verksamhetsutövare innefatta flertalet olika slags verksamhetsutövare som på olika sätt berörs av incidenten.

I genomförandet av de olika verksamhetsmomenten som utgör nationell operativ incidenthantering samarbetar NCSC med samverkansmyndigheterna enligt vad som anges i NCSC-förordningen.

Verksamhetsmomenten som ingår i nationell operativ incidenthantering innefattar:

- **Informationsdelning:** NCSC, samverkansmyndigheterna, drabbade och berörda myndigheter och verksamhetsutövare delar aktuell information om incidenten, dess konsekvenser, samt hur man kan skydda sig, vidta åtgärder för att minimera negativa följder, samt återgå till normalläge.

  Nationellt delas relevant information till berörda delar av kris- och beredskapsstrukturen samt till sedan tidigare etablerade sektorspecifika och andra forum för samverkan. Om inget relevant forum finns etablerat kan NCSC etablera ett tillfälligt forum för en specifik incident.

  Information delas även internationellt till olika nätverk kopplat till cybersäkerhet och incidenthantering som Sverige deltar i.

- **Lägesuppfattning:** Baserat på informationsdelning och andra källor sammanställs tillgänglig information kontinuerligt och resulterar i en bredare analys av incidenten, som vid behov ger förslag på åtgärder som bör vidtas. Analysen resulterar i en fördjupad rapport som redogör för vad som hänt och nuvarande incidentstatus.

  Rapporten delas med Regeringskansliet, samverkansmyndigheterna, samt drabbade och berörda myndigheter och verksamhetsutövare. Rapporteringsfrekvensen beror primärt på incidentutvecklingen och hur prioriterat informationsbehovet är hos mottagarna.

- **Koordinering:** NCSC, samverkansmyndigheterna, drabbade och berörda myndigheter och verksamhetsutövare genomför incidentkoordinering. Detta innefattar att kommunicera kring och samordna information, resurser och kompetenser på nationell nivå.

  Utöver detta så koordinerar NCSC med den bredare kris- och beredskapsstrukturen i syfte att följderna av störningarna ska bli så begränsad som möjligt. NCSC deltar då i nationella samverkanskonferenser som anordnas av den nationella kris- och beredskapsstrukturen för att utbyta information om incidenten, dess konsekvenser och vilka åtgärder som vidtas. Denna samverkan säkerställer att relevant information utbyts mellan NCSC och de som hanterar de uppkomna störningarna som incidenten orsakat eller på annat sätt berörs av incidenten.

- **Eventuell kriskommunikation:** Vid behov samordnar NCSC kommunikation kring incidenten med samverkansmyndigheterna, drabbade och berörda myndigheter och verksamhetsutövare. Respektive myndighet och verksamhetsutövare bestämmer om de vill använda gemensamt framtagna talepunkter. Syftet med att koordinera kriskommunikation är att ge allmänhet och media saklig, korrekt och enhetlig information om incidenten och motverka ryktesspridning. Innan NCSC förmedlar framtagna talepunkter till allmänheten och media informeras Regeringskansliet om vad dessa innefattar.

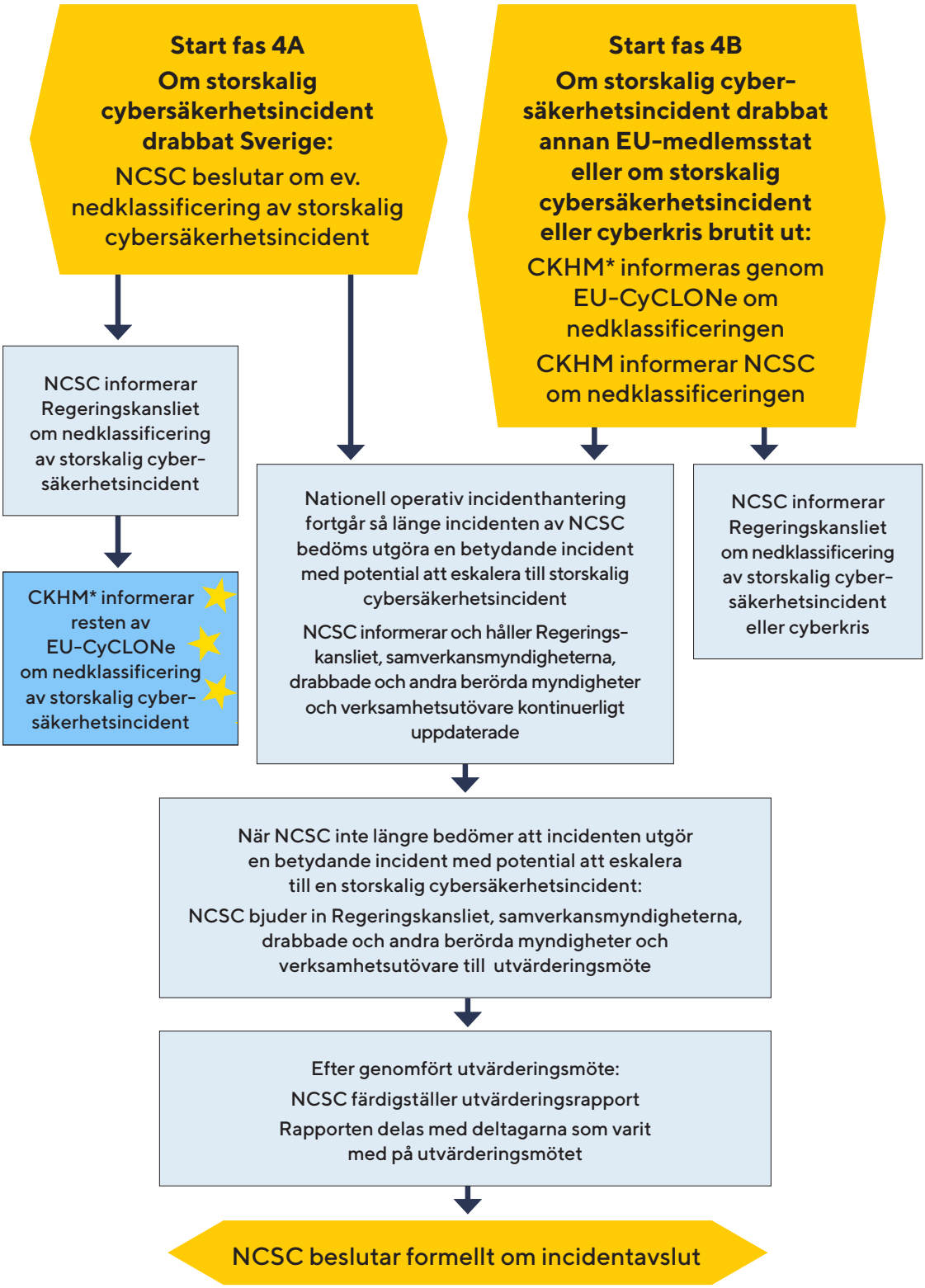
- **Nationellt resursläge:** Samverkan med den bredare nationella kris- och beredskapsstrukturen ger också NCSC en förståelse för omfattningen av störningarna som incidenten orsakat. Baserat på detta gör NCSC en bedömning av det nationella resursläget att hantera incidentens konsekvenser.

  Bedömningen utgör i sin tur ett nytt ingångsvärde för den kontinuerligt pågående nationella operativa incidenthanteringen och de verksamhetsmoment som genomförs inom ramen för denna.

  Anser NCSC att Sverige har behov av att få stöd från EU för att hantera störningarna som incidenten orsakat informeras Regeringskansliet.

Om incidenten fortsatt kräver hantering på teknisk nivå genomför nationell CSIRT denna enligt ordinarie rutin.

Fas 4: Nedklassificering av storskalig cybersäkerhetsincident eller cyberkris samt incidentavslut



* CKHM = Cyberkrishanteringsmyndighet

2.4 Fas 4: Nedklassificering av storskalig cybersäkerhetsincident eller cyberkris samt incidentavslut

2.4.1 Nedklassificering

Nedklassificering av storskalig cybersäkerhetsincident eller cyberkris kan ske på fyra olika sätt:

1. NCSC fattar beslut om nedklassificering av storskalig cybersäkerhetsincident när en incident som NCSC tidigare klassificerat som denna incidenttyp från ett nationellt perspektiv inte längre anses uppfylla dessa incidentkriterier. NCSC informerar Regeringskansliet och CKHM om nedklassificeringen. CKHM informerar resten av EU-CyCLONe om detsamma.
2. En annan EU-medlemsstat fattar beslut om nedklassificering av storskalig cybersäkerhetsincident när en incident som medlemsstaten tidigare klassificerat som denna incidenttyp från ett nationellt perspektiv inte längre anses uppfylla dessa incidentkriterier. EU-medlemsstaten meddelar EU-CyCLONe om nedklassificeringen. CKHM nås först av denna information via sina företrädare i EU-CyCLONe. CKHM informerar Regeringskansliet och NCSC om nedklassificeringen.
3. EU-CyCLONe fattar beslut om nedklassificering av storskalig cybersäkerhetsincident när en incident som EU-CyCLONe tidigare klassificerat som denna incidenttyp, med anledning av bedömningen att en incident inträffat som har en betydande påverkan på minst två medlemsstater, inte längre anses uppfylla dessa incidentkriterier. CKHM nås först av denna information via sina företrädare i EU-CyCLONe. CKHM informerar sedan Regeringskansliet och NCSC om nedklassificeringen.
4. EU-CyCLONe fattar beslut om nedklassificering av cyberkris när en incident som EU-CyCLONe tidigare klassificerat som denna incidenttyp inte längre anses uppfylla dessa incidentkriterier. CKHM nås först av denna information via sina företrädare i EU-CyCLONe. CKHM informerar sedan Regeringskansliet och NCSC om nedklassificeringen.

2.4.2 Fortsatt nationell operativ incidenthantering efter nedklassificering

Nationell operativ incidenthantering fortsätter så länge NCSC bedömer att incidenten fortfarande utgör en betydande incident med potential att eskalera till storskalig cybersäkerhetsincident.

2.4.3 Avslut nationell operativ incidenthantering

När NCSC bedömer att incidenten inte längre utgör en betydande incident med potential att eskalera till storskalig cybersäkerhetsincident så nedklassificerar NCSC incidenten. Efter denna nedklassificering avslutas nationell operativ incidenthantering inom ramen för NCSC:s verksamhet.

Om incidenten fortsatt kräver hantering på teknisk nivå genomför nationell CSIRT denna enligt ordinarie rutin.

2.4.4 Utvärdering

Efter att nationell operativ incidenthantering avslutats bjuder NCSC in Regeringskansliet, samverkansmyndigheterna, drabbade och andra berörda myndigheter och verksamhetsutövare till ett utvärderingsmöte. Mötet syftar till att dra lärdomar från incidenthanteringen som kan hjälpa NCSC och andra drabbade eller berörda myndigheter och verksamhetsutövare att ha bättre förutsättningar att hantera incidenter av motsvarande allvarlighetsgrad i framtiden. Efter att utvärderingsmötet genomförts sammanställs en utvärderingsrapport av NCSC där viktiga lärdomar redogörs för. Rapporten delas i första hand med de som deltagit i utvärderingsmötet.

2.4.5 Incidentavslut

Efter sammanställningen av utvärderingsrapporten fattar NCSC formellt beslut om incidentavslut.

Om incidenten fortsatt kräver hantering på teknisk nivå så utför nationell CSIRT detta enligt ordinarie rutin.

3. Appendix

3.1 Uppdraget

Regeringen gav den 27 februari 2025, FRA i uppdrag att utarbeta en nationell operativ plan för hantering av storskaliga cybersäkerhetsincidenter och cyberkriser (Fö2025/00388). I uppdragets genomförande ska FRA föra dialog med MSB. MSB ska bistå FRA med de uppgifter och underlag som behövs för genomförandet av uppdraget.

Den operativa planen ska tas fram med utgångspunkt i artikel 9.4b-f i NIS 2-direktivet. Planen ska särskilt beskriva berörda myndigheters ansvarsområden inom cyberkrishantering samt redogöra för nationella beredskapsåtgärder och förfaranden för cyberkrishantering vid cybersäkerhetsincidenter och cyberkriser. I detta ingår även att redogöra för samverkansförfaranden mellan relevanta myndigheter samt övriga verksamhetsutövare vid hantering av storskaliga cybersäkerhetsincidenter och cyberkriser. Vidare ska planen innehålla en beskrivning av berörda offentliga och privata intressenter och berörd infrastruktur.

Vid uppdragets genomförande ska FRA utgå från nationell lagstiftning, bland annat. säkerhetsskyddsregelverket, och beakta relevanta bestämmelser om hantering av storskaliga cybersäkerhetsincidenter och cyberkriser i andra EU-rättsakter.

FRA ska inhämta synpunkter om bland annat vilka nationella beredskapsåtgärder och förfaranden som bör etableras för cyberkrishanteringen från FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen. FRA ska även inhämta synpunkter från övriga relevanta myndigheter, exempelvis Finansinspektionen och Energimyndigheten, näringslivet och Sveriges Kommuner och Regioner. FRA ska senast 1 december 2025 lämna en redovisning av uppdraget till Regeringskansliet (Försvarsdepartementet).

3.2 Informations- och cybersäkerhetsverksamhet förs över till FRA

Regeringen beslutade den 20 november 2025 att ge FRA och MSB i uppdrag att förbereda överföring av informations- och cybersäkerhetsverksamhet som idag bedrivs vid MSB till FRA (Fö2025/01703, Fö2025/01704). Beslutet bygger på slutsatserna i utredningen *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79), som pekar på behovet av en mer samlad och kraftfull struktur för att skydda Sverige mot cyberhot. Övergången av verksamhet ska genomföras och integreras i NCSC den 1 juli 2026.

Regeringens beslut innebär bland annat att följande uppgifter som regleras i förordningen (2008:1002) med instruktion för MSB ska föras över till FRA:

- Ansvaret för att stödja och samordna arbetet med samhällets informations- och cybersäkerhet samt analysera och bedöma omvärldsutvecklingen.
- Rapporteringsskyldigheten till regeringen på informations- och cybersäkerhetsområdet.

- Uppdraget att ha en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera cybersäkerhetsincidenter.

- MSB:s uppdrag att utgöra nationellt samordningscenter (NCC-SE) enligt artikel 6 CCCN-förordningen.[10]

MSB har ansvaret för informations- och cybersäkerhetsarbetet i den nationella beredskapsstrukturen. För statliga myndigheter regleras detta i förordningen om statliga myndigheters beredskap. Beslutet innebär att ansvaret för incidentrapporteringsfunktionen enligt regleringen överförs till FRA. Därtill får FRA i uppdrag att ansvara för föreskrifter för beredskapsmyndigheternas arbete med informationssäkerhet.

Beslutet innebär även att FRA utses till CSIRT-enhet, gemensam kontaktpunkt och CKHM.

Vidare innebär beslutet bland annat att FRA får ett utökat uppdrag inom arbetet med samhällets informations- och cybersäkerhet. De nya uppgifterna ska verksamhetsmässigt utföras av NCSC.

3.3 Rättsliga krav på cyberkrishanteringsplanen

De rättsliga kraven på den nationella planen framgår huvudsakligen av NIS 2-direktivet.

I artikel 9.4 NIS 2-direktivet anges att planen särskilt ska innehålla följande:

a. Målen för nationella beredskapsåtgärder och beredskapsverksamhetsutövare.
b. Cyberkrishanteringsmyndigheternas uppgifter och ansvarsområden.
c. Cyberkrishanteringsförfaranden, inbegripet deras integrering i den allmänna nationella ramen för krishantering och kanaler för informationsutbyte.
d. Nationella beredskapsåtgärder**,** inbegripet övningar och utbildningsverksamhet.
e. Berörda offentliga och privata intressenter och berörd infrastruktur.
f. Nationella förfaranden och arrangemang mellan relevanta nationella myndigheter och organ för att säkerställa att medlemsstaten på ett ändamålsenligt sätt kan delta i och stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser på unionsnivå.

Utöver bestämmelserna i NIS 2-direktivet finns det även bestämmelser som direkt rör den nationella planen och CKHM i de så kallade. nätkoderna. Nätkoderna innehåller sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden. Syftet med nätkoderna är att komplettera bestämmelserna i NIS 2-direktivet när gränsöverskridande elflöden berörs.

[10] 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.

Nätkoderna innehåller bland annat krav på CKHM att ingå i ett särskilt samordningsforum.[11] Vidare finns det en möjlighet att låta den nationella planen även utgöra nationell plan för hantering av cyberkriser som avser gränsöverskridande elflöden. För det fall den nationella planen även utgör en sådan plan tillkommer det vissa uttryckliga krav på planen i nätkoderna.

3.4 Roller och ansvar i nationell incidenthantering

3.4.1 Nationell CSIRT

Enligt artikel 10 i NIS 2-direktivet ska varje medlemsstat utse eller inrätta en eller flera CSIRT-enheter. CSIRT-enheternas uppgifter regleras främst i artikel 11 i NIS 2-direktivet.

I artikel 11.3 anges att CSIRT-enhetens uppgifter är följande:

a. Övervakning och analys av cyberhot, sårbarheter och incidenter på nationell nivå och, på begäran, tillhandahållande av stöd till berörda väsentliga och viktiga entiteter avseende realtidsövervakning eller nära realtidsövervakning av deras nätverks- och informationssystem.

b. Tillhandahållande av tidiga varningar, larm, meddelanden och spridning av information till väsentliga och viktiga entiteter samt till behöriga myndigheter och andra relevanta intressenter om cyberhot, sårbarheter och incidenter, om möjligt i nära realtid.

c. Vidtagande av åtgärder till följd av incidenter och, i tillämpliga fall, tillhandahållande av stöd till de berörda väsentliga och viktiga entiteterna. Nationella beredskapsåtgärder, inbegripet övningar och utbildningsverksamhet.

d. Insamling och analys av forensiska uppgifter och tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet när det gäller cybersäkerhet.

e. Tillhandahållande, på begäran av den väsentliga eller viktiga entiteten, av en proaktiv skanning av den berörda entitetens nätverks- och informationssystem i syfte att upptäcka sårbarheter med en potentiellt betydande påverkan.Nationella förfaranden och arrangemang mellan relevanta nationella myndigheter och organ för att säkerställa att medlemsstaten på ett ändamålsenligt sätt kan delta i och stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser på unionsnivå.

f. Deltagande i CSIRT-nätverket och ömsesidigt bistånd i enlighet med deras kapacitet och befogenheter till andra medlemmar i CSIRT-nätverket på deras begäran.

g. I tillämpliga fall, fungera som processamordnare för den samordnade delgivningen av information om sårbarheter enligt artikel 12.1.

h. Bidrag till införandet av säkra verktyg för informationsutbyte enligt artikel 10.3. CSIRT-enheterna får utföra en proaktiv, icke-inkräktande skanning av väsentliga och viktiga entiteters allmänt tillgängliga nätverks- och informationssystem. Sådan skanning ska utföras för att upptäcka sårbara eller osäkert konfigurerade nätverks- och informationssystem och informera de berörda enheterna. Sådan skanning får inte ha någon negativ inverkan på hur entiteternas tjänster fungerar. När CSIRT-enheten utför dessa uppgifter får den prioritera särskilda uppgifter på grundval av en riskbaserad metod.

[11] Artikel 40 nätkoderna.

Av artikel 11.4 framgår därutöver att CSIRT-enheterna ska upprätta samarbetsförbindelser med relevanta intressenter inom den privata sektorn i syfte att uppnå målen för detta direktiv. För att främja ett sådant samarbete ska CSIRT-enheterna verka för antagande och användning av gemensamma eller standardiserade metoder, klassificeringssystem och taxanomier när det gäller förfaranden för incidenthantering samt samordnad delgivning av information om sårbarheter enligt artikel 12.1.

Av artikel 12 i direktivet framgår vidare att varje medlemsstat ska utse en av sina CSIRT-enheter till samordnare för den samordnade delgivningen av information om sårbarheter. Den CSIRT-enhet som utsetts till samordnare ska fungera som en betrodd mellanhand och vid behov underlätta interaktionen mellan den som rapporterar en sårbarhet och tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller tjänsterna. Uppgiften som samordnare innefattar att ha förmågan att ta emot anonyma sårbarhetsrapporter och agera på dessa samt säkerställa anonymiteten för den som rapporterat sårbarheten.

Det CSIRT-nätverk som CSIRT-enheterna ska medverka i enligt artikel 11.3 f beskrivs i artikel 15 i NIS 2-direktivet. Där framgår att nätverket ska ha ett omfattande uppdrag att möjliggöra delning av relevant information mellan de nationella CSIRT-enheterna samt utgöra ett forum för samarbete mellan de nationella enheterna vid incidenter.

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.

3.4.2 Cyberkrishanteringsmyndigheten

Av artikel 9 i NIS 2-direktivet framgår att varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och cyberkriser. Enligt artikel 16.2 i direktivet ska EU-CyCLONe bland annat bestå av företrädare för medlemsstaternas cyberkrishanteringsmyndigheter.

CKHM:s uppgifter och ansvarsområden på nationell nivå anges inte i NIS 2-direktivet. I stället ska medlemsstaterna enligt artikel 9.4 i direktivet anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och cyberkriser där mål och villkor för hanteringen av sådana situationer fastställs. Enligt artikel 9.4 b ska denna plan särskilt innehålla en beskrivning av CKHM:s uppgifter och ansvarsområden; dessa framgår av beskrivningen i avsnitt 2 av fas 2, 3, och 4 av cyberkrishanteringsplanen.

3.4.3 NCSC

Från och med den 1 november 2024 finns NCSC vid FRA som har ansvaret för att leda centret. Enligt 4 a § förordningen (2007:937) med instruktion för Försvarets radioanstalt har NCSC till uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra cybersäkerhetsincidenter.

NCSC-förordningen (2025:237) innehåller kompletterande bestämmelser om den verksamhet som ska bedrivas av NCSC.

Av 2 § förordningen framgår att NCSC ska utgöra en nationell plattform för samverkan och informationsutbyte mellan verksamhetsutövare, såväl privata som offentliga, i frågor som rör cybersäkerhet. Centret ska också vara en kontaktpunkt för sådana frågor.

Enligt 3 § i samma förordning ska NCSC särskilt

1. bidra till att samordna och harmonisera det nationella cybersäkerhetsarbetet,
2. lämna råd och stöd till privata och offentliga verksamhetsutövare i frågor om hot, sårbarheter och risker med koppling till cybersäkerhet,
3. lämna råd och stöd till privata och offentliga verksamhetsutövare vid cybersäkerhetsincidenter,
4. genomföra utbildningar, övningar och andra kompetenshöjande insatser inom cybersäkerhetsområdet,
5. till privata och offentliga verksamhetsutövare ta fram samlade lägesbilder av antagonistiska cyberhot och andra cybersäkerhetsincidenter,
6. bistå Regeringskansliet (Försvarsdepartementet) med samlade lägesbilder som bland annat innehåller bedömningar av hotnivån,
7. vara en kontaktpunkt gentemot motsvarande funktioner i internationella sammanhang och utveckla samarbetet och informationsutbytet med dessa,
8. rapportera till regeringen om förhållanden på cybersäkerhetsområdet som kan leda till behov av åtgärder samt lämna förslag på sådana åtgärder, och
9. informera regeringen om relevanta förhållanden vid ett sådant hot eller annan incident som avses i 5 § andra stycket.

Vidare anges i 4 § att FRA ska organisera, leda och planera verksamheten som bedrivs inom ramen för NCSC. FRA ska i den verksamhet som bedrivs inom ramen för NCSC samverka med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen (de så kallade samverkansmyndigheterna).

Av 5 § NCSC-förordningen framgår att samverkansmyndigheterna, inom ramen för sina respektive befintliga ansvarsområden, löpande ska bistå NCSC med kunskap, kompetens och information. NCSC ska löpande bistå samverkansmyndigheterna med kunskap och information.

Vid ett antagonistiskt cyberhot eller annan it-incident som har vållat eller som kan antas ha potential att vålla betydande skada ska NCSC och samverkansmyndigheterna utbyta kunskap, kompetens och information i syfte att förbättra samordningen mellan myndigheterna och bidra till att effektivisera myndigheternas arbete med att hantera cyberhotet eller incidenten.

3.5 Cyberplanen, CSIRT-nätverket och EU-CyCLONe

3.5.1 Cyberplanen

I Cyberplanen fastställs unionens ram för cyberkrishantering inom ramen för EU:s övergripande beredskap för storskaliga cybersäkerhetsincidenter och cyberkriser som uppstår till följd av sådana incidenter, oavsett vilken sektor eller enhet som berörs. Ramen återspeglar både medlemsstaternas och unionens institutioners, organs och byråers (unionsentiteters) roller inom ramen för deras respektive befogenheter.

Av Cyberplanen framgår att medlemsstaterna har huvudansvaret för hanteringen av cybersäkerhetsincidenter och cyberkriser. Cybersäkerhetsincidenternas potentiella gränsöverskridande och sektorsövergripande karaktär kräver emellertid att medlemsstaterna och de berörda unionsentiteterna samarbetar på teknisk, operativ och politisk nivå för att effektivt samordna sig i hela unionen.

Hur Cyberplanen skiljer mellan teknisk, operativ och politisk nivå, samt vilka de olika organ som är involverade i cyberkrishantering på nationell nivå och EU-nivå illustreras av grafiken nedan.[12] Av denna framgår att på teknisk nivå samverkar nationell CSIRT med CSIRT-nätverket, medan CKHM samverkar med EU-CyCLONe på operativ nivå.

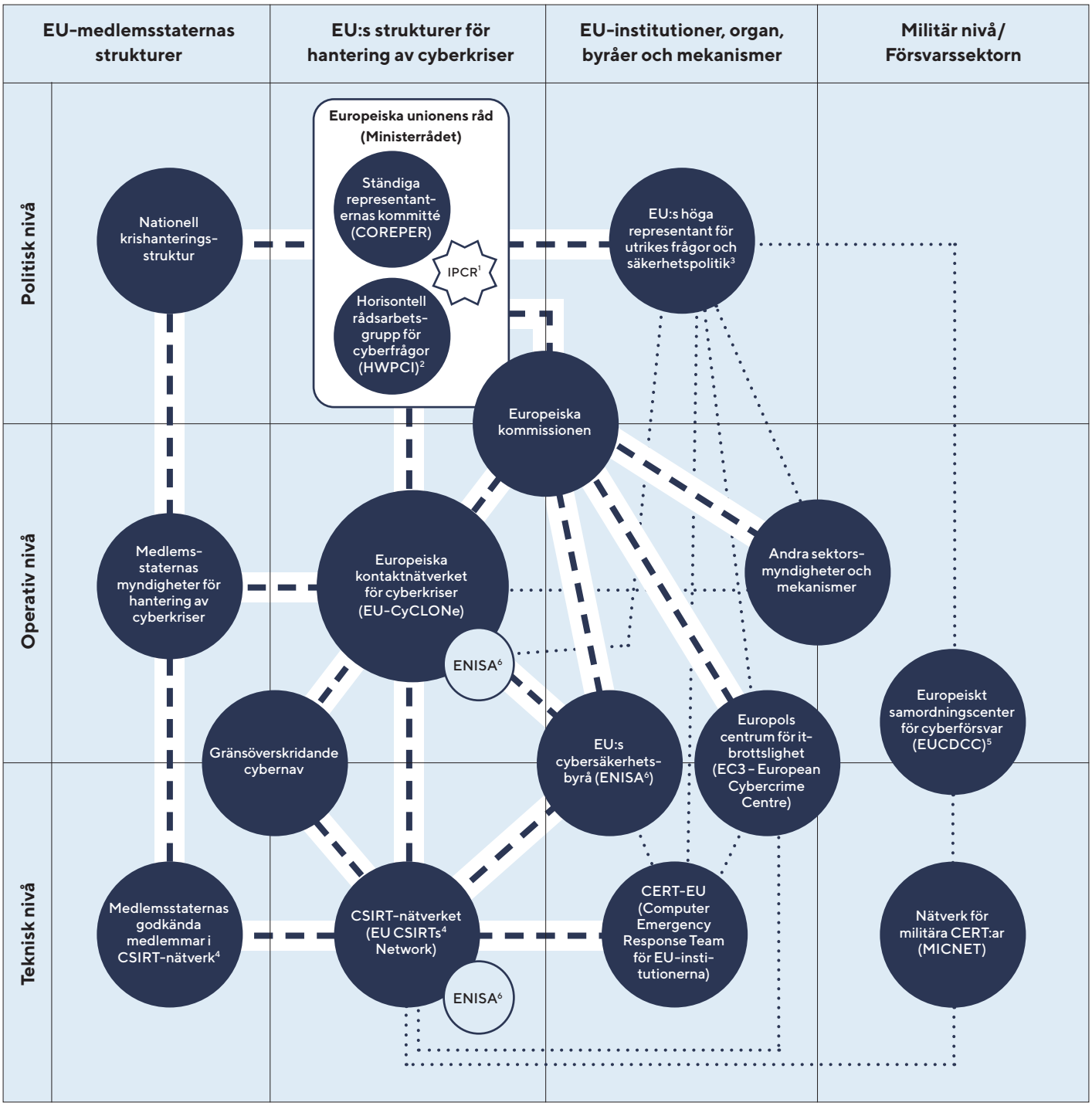
Vid cybersäkerhetsincidenter och cybersäkerhetshot samarbetar medlemsstaterna och utbyter frivilligt och regelbundet information inom CSIRT-nätverket och EU-CyCLONe, i enlighet med nätverkens standardiserade tillvägagångssätt.

3.5.2 CSIRT-nätverket

Nationell CSIRT samverkar i CSIRT-nätverket somhar följande uppgifter:[13]

- Bidrar till att skapa förtroende och tillit och främjar ett snabbt operativt samarbete mellan medlemsstaterna.
- Är det främsta nätverket för utbyte av relevant information om incidenter, tillbud, cyberhot, risker och sårbarheter.
- På begäran av en medlem som kan påverkas av en incident utbyter och diskuterar nätverket information om den incidenten och relaterade cyberhot.
- Nätverket kan också underlätta samordnade insatser för att hantera en incident som har identifierats inom en begärande medlems jurisdiktion.
- Bistår medlemsstaterna med hanteringen av gränsöverskridande incidenter och undersöker ytterligare samarbetsformer, inbegripet ömsesidigt bistånd.
- Får information från medlemsstaterna om deras framställningar till EU-cybersäkerhetsreserven.

[13] Bilaga II s.15 Cyberplanen.



Samarbete vid storskaliga incidenter eller cyberkriser

Andra informationsutbyten och samarbeten

1. Integrerad politisk krishanteringsmekanism (IPCR)
2. Horizontal Working Party on Cyber Issues
3. Med stöd av Europeiska utrikestjänsten (EEAS – European External Action Service)
4. CSIRT = Computer Security Incident Response Team
5. EUCDCC och gränsöverskridande cybernav håller på att etableras
6. EU:s cybersäkerhetsbyrå (ENISA – European Union Agency for Cybersecurity)

3.5.3 EU-CyCLONe

EU-CyCLONe är ett nätverk för samordning av hanteringen av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser på operativ nivå, även vid sektorsövergripande storskaliga cybersäkerhetsincidenter och cyberkriser.

EU-CyCLONe[14]

- Stöder en samordnad hantering av storskaliga cybersäkerhetsincidenter och cyberkriser på operativ nivå.
- Säkerställer ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer.
- Samordnar hanteringen av storskaliga cybersäkerhetsincidenter och cyberkriser och ger stöd till beslutsfattande på politisk nivå i samband med sådana incidenter och cyberkriser.
- Bedömer konsekvenserna och effekterna av relevanta storskaliga cybersäkerhetsincidenter och cyberkriser och föreslår möjliga begränsningsåtgärder.
- Diskuterar, på begäran av en berörd medlemsstat, nationella planer för hantering av storskaliga nationella cybersäkerhetsincidenter och cyberkriser.
- Utarbetar tillsammans med Enisa och kommissionen mallen för att underlätta inlämning av framställningar om stöd från EU-cybersäkerhetsreserven.
- Får information från medlemsstaterna om deras begäranden till EU-cybersäkerhetsreserven.
- Får information om en potentiell eller pågående storskalig cybersäkerhetsincident från de gränsöverskridande cybernaven eller CSIRT-nätverket.

3.6 FRA och samverkansmyndigheterna

3.6.1 Ansvarsprincipen

Regeringen fastslår i den nationella strategin för cybersäkerhet 2025–2029 att ansvarsprincipen gäller även på cyberområdet. Vid en cybersäkerhetsincident kan en krissituation uppstå som konsekvens och ansvarsprincipen därmed bli tillämplig inom den offentliga förvaltningen. Principen innebär att den som i normala fall ansvarar för en verksamhet, till exempel en statlig myndighet eller kommun, också har detta ansvar under en krissituation. Vid storskaliga cybersäkerhetsincidenter och cyberkriser ska dock en eller flera behöriga CKHMs ansvara för nationell hantering.

[14] Bilaga II s. 21 cyberplanen.

Nedan beskrivs FRA:s och samverkansmyndigheternas ansvarsområden med koppling till incidenthantering och cybersäkerhet.

3.6.1.1 Försvarets radioanstalt

FRA är Sveriges expertmyndighet för teknisk informations- och cybersäkerhet. Myndigheten får efter begäran lämna stöd till statliga myndigheter och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Inom ramen för sitt underrättelseuppdrag bedriver FRA signalspaning.

Inom FRA finns hög teknisk kompetens inom informationssäkerhetsområdet som gör det möjligt för myndigheten att genomföra kvalificerade it-säkerhetsanalyser och ge annat tekniskt stöd. Mer konkret innebär detta att FRA efter begäran kan stödja både statliga myndigheter och enskilda verksamhetsutövare med tekniskt stöd för att stärka säkerheten i deras it-system. FRA utför bland annat avancerade säkerhetsgranskningar för att upptäcka brister eller intrång i en myndighets eller ett företags it-system. FRA tillhandahåller också ett varningssystem som med hjälp av myndighetens höga tekniska kompetens och tillgång till underrättelseinformation kan upptäcka avancerade it-angrepp som normalt inte fångas av kommersiella skyddssystem.

FRA har även till uppdrag att stödja insatser vid nationella kriser med it-inslag. Informations- och cybersäkerhetsarbetet hos FRA har ett nära samarbete med underrättelsearbetet där FRA kartlägger de mest kvalificerade statliga hotaktörerna.

Från och med den 1 november 2024 finns NCSC inom FRA. FRA ansvarar för att leda arbetet inom ramen för NCSC. Se appendix 3.4 där NCSC:s uppdrag beskrivs närmare.

3.6.1.2 Försvarets materielverk

FMV har idag endast en stödjande roll i NCSC och deltar inte i verksamheten relaterad till hanteringen av cybersäkerhetsincidenter. FMV:s samverkan i NCSC utgår från de uppdrag och verksamheter myndigheten har inom cybersäkerhetsområdet. Detta inkluderar uppdraget att vara tillsynsmyndighet inom cybersäkerhetscertifiering (ICC), certifieringsorgan för cybersäkerhetscertifiering (CSEC), fullfölja åtaganden i rollen som nationell industrisäkerhetsmyndighet och andra åtaganden som faller inom myndighetens materielförsörjningsuppdrag. Myndigheten har idag inget uppdrag som omfattar en aktiv roll inom cyberkrishantering men kan bistå vid hantering i de fall myndighetens kompetens efterfrågas eller bedöms nödvändig.

3.6.1.3 Försvarsmakten

Försvarsmaktens huvuduppgift är att försvara Sverige och allierade stater mot ett väpnat angrepp med utgångspunkt i det kollektiva försvaret inom Nato. Försvarsmakten har också uppgiften att leda och bedriva militär underrättelse- och säkerhetstjänst. Försvarsmakten inhämtar information om cyberhot inom ramen för sin underrättelse- och säkerhetstjänst.

Försvarsmaktens cyberförsvar ingår som en integrerad del av det militära försvaret och bidrar genom att i samtliga konfliktnivåer kunna avskräcka och förneka en motståndare att i eller genom cyberdomänen påverka det militära försvarets förmåga att mobilisera, möta ett väpnat angrepp, upprätthålla den territoriella integriteten eller värna Sveriges suveräna rättigheter. För att uppnå detta har cyberförsvaret förmåga att försvara kritisk infrastruktur som Försvarsmakten är beroende av och att vidta åtgärder inom cyberdomänen för att bidra till att totalförsvaret och det kollektiva försvaret inom Nato som helhet är krigsavhållande.

Cyberförsvaret har förmåga att genomföra offensiva och defensiva cyberoperationer samt att upptäcka, identifiera och avvärja hot mot digitala informationssystem och elektroniska kommunikationstjänster. Den offensiva cyberförmågan kan nyttjas för att upprätthålla egen handlingsfrihet samt påverka motståndarens handlingsfrihet.

Försvarsmakten är också en av de myndigheter som utövar tillsyn och utfärdar föreskrifter enligt säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955), bland annat vad gäller informationssäkerhet. Vidare samverkar Försvarsmakten med FRA, inom NCSC, tillsammans med övriga samverkansmyndigheter med uppgift att utveckla och stärka Sveriges förmåga för att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter.

3.6.1.4 MSB/Myndigheten för civilt försvar

MSB ska enligt sin instruktion stödja berörda myndigheters samordning av åtgärder vid en kris eller vid höjd beredskap. MSB ska se till att berörda aktörer under sådana förhållanden, när det gäller krishantering och civilt försvar, får tillfälle att 1) samordna åtgärder, 2) samordna information till allmänhet och medier, 3) effektivt använda samhällets samlade resurser och internationella förstärkningsresurser, och 4) samordna stödet till centrala, regionala och lokala organ i fråga om information och lägesbilder.

Myndigheten ska också bistå Regeringskansliet med underlag och information av betydelse för myndighetens ansvarsområde i samband med allvarliga olyckor och kriser samt under höjd beredskap. Myndigheten ska även utifrån en nationell riskbild upprätthålla beredskap med stödresurser för att kunna bistå i samband med allvarliga olyckor och kriser och vid höjd beredskap. MSB ska även kunna prioritera och fördela tillgängliga förstärkningsresurser enligt 6 kap. 8 a § lagen (2003:778) om skydd mot olyckor.

MSB har som särskild uppgift att arbeta för att kommunikationen i systemet på nationell nivå samordnas och kan användas som ett strategiskt verktyg i hanteringen av samhällsstörningar i fredstid och under höjd beredskap.

MSB:s arbete med att upprätthålla nationell beredskap innebär att det dygnet runt finns en snabb och effektiv initiering av samhällets samlade hantering av olika samhällsstörningar och hantering av förfrågningar om stöd från EU och internationella aktörer. Vid myndigheten sker en kontinuerlig omvärldsbevakning och myndigheten håller regeringen och Regeringskansliet informerade om läget i landet.

MSB stödjer samordningen vid samhällsstörningar genom att vara en pådrivande kraft i att få till stånd den nödvändiga samordningen mellan berörda myndigheter. Utgångspunkten är lägesbildsarbetet med analyser av konsekvenser för samhället som helhet och behov av åtgärder utifrån ett samlat nationellt perspektiv. MSB identifierar gemensamma utmaningar och ser till att ansvariga myndigheter samverkar för att samordna sina åtgärder. MSB verkar också för att tillgängliga resurser används effektivt där de behövs mest. MSB tar fram förslag om hur resurserna bör prioriteras och kan också mäkla resurser mellan verksamhetsutövare, underlätta för aktörer att ge och ta emot stöd.

MSB har rollen som nationell CKHM, nationell kontaktpunkt enligt NIS1-, NIS 2- och CER-direktiven, samt utgöra CSIRT-enhet tills 1 juli 2026, då dessa roller övergår till FRA.

MSB byter den 1 januari 2026 namn till Myndigheten för civilt försvar (MCF) roll är att leda, inrikta och samordna det civila försvaret. I detta ingår att leda och skapa handlingskraft i den samlade civila hanteringen av krig och kriser nationellt för att det civila och militära försvaret ska vara samordnat. Myndigheten hanterar kriser både nationellt och internationellt och som allierade i krig.

I rollen som sektorsansvarig myndighet för beredskapssektorn Räddningstjänst håller myndigheten samman förberedelserna för att vid krig kunna skydda befolkningen och därmed upprätthålla försvarsviljan. MCF bidrar även till att räddningstjänsten fungerar i vardagen, vid kriser och olyckor, och ytterst i krig. Myndighetens verksamhet ska bidra till att uppfylla målet för civilt försvar och det övergripande målet för totalförsvaret samt målen för skydd mot olyckor och krisberedskap.

3.6.1.5 Post- och telestyrelsen

PTS har ett samlat ansvar för områdena elektronisk kommunikation och post. PTS är beredskapsmyndighet och sektorsansvarig myndighet för beredskapssektorn elektroniska kommunikationer och post. Myndigheten verkar för att elektroniska kommunikationsnät och -tjänster är tillförlitliga, det vill säga robusta, säkra och tillgängliga samt att sektorn har en god förmåga att kunna hantera fredstida kriser, höjd beredskap och krig. Myndigheten är tillsynsansvarig för leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur och för leverantörer av digitala tjänster. PTS pekas enligt regeringsbeslut ut som tillsynsansvarig myndighet för fem sektorer under NIS 2-direktivet och den kommande cybersäkerhetslagen. PTS är även tillsynsansvarig för enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet inom områdena elektronisk kommunikation och post.

3.6.1.6 Säkerhetspolisen

Säkerhetspolisen är Sveriges nationella säkerhetstjänst och bedriver i den egenskapen underrättelse- och säkerhetsarbete. Myndigheten bedriver även polisverksamhet.

Som säkerhetstjänst arbetar Säkerhetspolisen för att höja säkerhetsnivån i det egna landet. Detta görs dels genom att avslöja och reducera säkerhetshot som riktas mot landet och dess skyddsvärda verksamheter, dels genom att reducera sårbarheter i dessa verksamheter. Säkerhetspolisen bedriver även vägledning, rådgivning och tillsyn, samt ger i vissa fall tekniskt stöd, för att säkerställa att verksamhetsutövarna efterlever säkerhetsskyddslagstiftningens krav.

Säkerhetspolisen kan inleda en förundersökning om dataintrång, eller välja att överta en sådan utredning från Polismyndigheten i fall angreppet avser säkerhetskänslig verksamhet eller har utförts av aktörer som myndigheten har i uppdrag att följa, så som främmande makt (verksamhetsområde kontraspionage) eller terroristorganisationer (verksamhetsområde kontraterror).

Verksamhetsutövare ska enligt säkerhetsskyddsregelverket skyndsamt anmäla till Säkerhetspolisen om det finns skäl att anta att en säkerhetsskyddsklassificerad uppgift otillåtet har röjts, det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet, eller verksamhetsutövaren får kännedom eller misstanke om någon annan för denne allvarlig säkerhetshotande verksamhet.

I händelse av bland annat en sådan anmälan får Säkerhetspolisen lämna tekniskt stöd, och under vissa förutsättningar vägledning, inom säkerhetsskydd till den drabbade verksamhetsutövaren. Säkerhetspolisen är däremot skyldig att på begäran lämna rådgivning inom säkerhetsskydd till Regeringskansliet, riksdagen och dess myndigheter (exempelvis Riksbanken) samt till Justitiekanslern.

Säkerhetspolisen är en av samverkansmyndigheterna och ska löpande bistå NCSC med kunskap, kompetens och information. Vid ett antagonistiskt cyberhot eller annan it-incident som har vållat eller som kan antas ha potential att vålla betydande skada ska Säkerhetspolisen utbyta kunskap, kompetens och information med det NCSC i syfte att förbättra samordningen mellan myndigheterna och bidra till att effektivisera myndigheternas samarbete med att hantera cyberhotet eller incidenten.

3.6.1.7 Polismyndigheten

Till Polismyndighetens uppgifter hör bland andra att upptäcka, förebygga och förhindra brottslig verksamhet samt att utreda och beivra brott som hör under allmänt åtal. Samtliga dessa uppgifter förutsätter att polisen ges bästa möjliga information om ett inträffat angrepp för att kunna välja relevanta och effektiva åtgärder. Ett förstärkt informationsutbyte från nationella myndigheter under NCSC-paraplyet i den operativa delen att utreda det brottsliga angreppet skulle avsevärt kunna förbättra förutsättningarna att komma framåt i en brottsutredning.

Polismyndigheten arbetar även inom ramen för uppgifterna att upptäcka, förebygga och förhindra brottslig verksamhet med underrättelseverksamhet. Även för denna verksamhet finns behov av möjligheten att ta del av information om angreppet från andra nationella myndigheter. Genom att också samverka med relevanta utländska tjänster kan polisen bidra till skapandet av en överblick över skadlig infrastruktur för att därefter kunna ingripa mot den genom exempelvis ett förverkandeförfarande. Det internationella samarbetet är av stor vikt för att nå ett sådant nedtagande av skadlig infrastruktur och det är här viktigt att Sverige kan bidra på ett reciprokt sätt i förhållande till utländska tjänster.

3.7 Berörda nationella offentliga och privata intressenter

Förutom Regeringskansliet, FRA och samverkansmyndigheterna finns ett stort antal andra berörda nationella offentliga och privata intressenter. Nedan redogörs för ett urval av dessa.

3.7.1 Beredskapsmyndigheter och sektorsansvariga myndigheter

Beredskapsmyndigheter är myndigheter med ansvar inom en eller flera viktiga samhällsfunktioner och vars verksamhet har särskild betydelse för samhällets krisberedskap och totalförsvaret. Myndigheterna ska ha god förmåga att motstå hot och risker, förebygga sårbarheter, hantera fredstida krissituationer och genomföra sina uppgifter vid höjd beredskap. Beredskapsmyndigheterna ska varje jämt årtal lämna en sammanfattande redovisning (risk- och sårbarhetsbedömning) till Regeringskansliet och MSB. För varje beredskapssektor finns en sektorsansvarig beredskapsmyndighet som leder arbetet med att samordna åtgärder både inför och vid fredstida krissituationer och höjd beredskap.[15]

3.7.1.1 Riksbanken

Riksbanken har ett ansvar för att allmänheten ska kunna göra betalningar i såväl krissituationer som inträffar under fredstid som i en situation där höjd beredskap råder. Riksbankslagen ger Riksbanken ansvar, uppgifter och mandat som ska bidra till en successiv förstärkning av den samlade förmågan att upprätthålla allmänhetens betalningar under fredstida krissituationer och höjd beredskap. I praktiken innebär ansvaret att Riksbanken har en samordnande, kravställande och övervakande roll. Som en del i Riksbankens krisförebyggande arbete analyserar och övervakar Riksbanken cyberrisker i det finansiella systemet. Dessutom koordinerar Riksbanken cybersäkerhetstester inom svensk finansiell sektor.

I utkast till lagrådsremiss *En ny funktion för operativ krishantering i den finansiella sektorn*[16] föreslås att det införs en ny funktion för operativ krishantering som ska hantera allvarliga driftsstörningar i det finansiella systemet. I utkastet föreslås att Riksbanken ska få ansvaret att leda krishanteringsfunktionen. Utöver Riksbanken ska Finansinspektionen, Riksgäldskontoret och vissa företag i den finansiella sektorn ingå i funktionen. Riksbanken ska även få bjuda in andra verksamhetsutövare som har kunskaper eller resurser som är av betydelse för funktionen att medverka i dess verksamhet. Lagändringarna föreslås träda i kraft den 1 juli 2026.

[15] I bilaga 1 och bilaga 2 till beredskapsförordningen framgår vilka myndigheter som är beredskapsmyndigheter respektive sektorsansvariga myndigheter.

[16] En ny funktion för operativ krishantering i den finansiella sektorn (utkast till lagrådsremiss), Regeringskansliet, Fi2025/01510.

3.7.1.2 Försäkringskassan

Försäkringskassan är beredskapsmyndighet och sektorsansvarig myndighet för beredskapssektorn ekonomisk säkerhet. För att Försäkringskassans verksamhet ska fungera vid en särskild allvarlig störning eller incident finns rutiner och reservförfaranden för att eventuella avbrott inte ska påverka viktiga samhällsfunktioner. Försäkringskassan deltar även i samverkansfora med syfte att förebygga störningar i betalningssystemen och att stärka stabiliteten i finanssektorn.

3.7.1.3 Finansinspektionen

Finansinspektionen (FI) ska arbeta för att det finansiella systemet är stabilt och ansvarar bland annat för tillsynen, regelgivningen, tillståndsprövningen och registreringen som rör finansiella marknader och finansiella företag. FI är även beredskapsmyndighet och sektorsansvarig myndighet för beredskapssektorn finansiella tjänster, enligt beredskapsförordningen.

FI ska ha en god förmåga att motstå hot och risker, förebygga sårbarheter, hantera fredstida krissituationer och genomföra sina uppgifter vid höjd beredskap. Majoriteten av de samhällsviktiga finansiella tjänsterna tillhandahålls av de finansiella företagen. En viktig del av FI:s arbete är därför att verka för att de finansiella företag som är berörda, utvecklar sina förmågor så att de kan motstå hot och risker inför och vid fredstida krissituationer och höjd beredskap.

Slutligen är FI ansvarig tillsynsmyndighet för DORA-förordningen[17] gällande digital operativ motståndskraft i finanssektorn. Det innebär bland annat att finansiella institut ska hantera risker inom informations- och kommunikationsteknologi (IKT) och rapportera in allvarliga IKT-relaterade incidenter till FI. FI granskar de inrapporterade incidenterna och bedömer om det finns behov av eskalering, förtydliganden eller vidare tillsynsaktivitet. De inrapporterade allvarliga IKT-relaterade incidenterna skickas automatiskt vidare till de europeiska tillsynsmyndigheterna och till Riksbanken. FI är även svensk kontaktpunkt i *European Systemic Cyber Incident Coordination Framework (EU-SCICF),* vilket är ett ramverk för koordinering av systemiska gränsöverskridande cyberincidenter i finanssektorn.

3.7.1.4 Skatteverket

Skatteverket är beredskapsmyndighet och sektorsansvarig beredskapsmyndighet för beredskapssektorn försörjning av grunddata. Uppdraget omfattar grunddata för personer, företag, fastighetsinformation, geografisk information och positionsdata. Detta är uppgifter inom den offentliga förvaltningen som är viktiga i samhället även under höjd beredskap och vid fredstida kriser. Skatteverket är även beredskapsmyndighet inom beredskapssektorn ekonomisk säkerhet som ansvarar för att in- och utbetalningar ska fungera.

[17] Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

3.7.1.5 Socialstyrelsen

Socialstyrelsen är beredskapsmyndighet och sektorsansvarig beredskapsmyndighet i beredskapssektorn hälsa, vård och omsorg. Till uppgifterna hör även att driva på arbetet inom beredskapssektorn, stödja de övriga beredskapsmyndigheterna samt verka för att uppgifter och roller inom beredskapssektorn tydliggörs.

3.7.1.6 Livsmedelsverket

Livsmedelsverket är beredskapsmyndighet och sektorsansvarig beredskapsmyndighet för beredskapssektorn livsmedelsförsörjning och dricksvatten. Myndigheten har en krisledningsfunktion som snabbt ska kunna aktiveras vid bland annat krissituationer och som har i uppdrag att samordnar myndighetens hantering av händelsen.

3.7.1.7 Trafikverket

Trafikverket är beredskapsmyndighet och sektorsansvarig beredskapsmyndighet för beredskapssektorn transporter. Transporter, inklusive en fungerande transport-infrastruktur, är av särskild betydelse för krisberedskap och totalförsvaret eftersom transporter behöver fungera i fredstid såväl som i allvarlig kris och i krig. Myndigheten ska utveckla och vidmakthålla den övergripande landsomfattande infrastrukturen i transportsystemet.

3.7.1.8 Länsstyrelser och civilområden

Länsstyrelser är beredskapsmyndigheter och har även ett regionalt geografiskt områdesansvar, vilket bland annat innebär att de har ett särskilt ansvar för samordning regionalt. Landets 21 länsstyrelser är indelade i sex civilområden med varsin civil-områdesansvarig länsstyrelse som bland annat ska se till att det civila försvaret inom civilområdet får en enhetlig inriktning. Vid fredstida krissituationer som berör flera län inom civilområdet ska den civilområdesansvariga länsstyrelsen också ha förmåga att utgöra en gemensam funktion för stöd till länsstyrelsernas hantering av krisen.

3.7.1.9 Energimyndigheten

Energimyndigheten har ett särskilt ansvar inom både beredskap och sektorssamordning för energiförsörjning i Sverige, vilket innebär ett strategiskt och operativt ansvar för att samordna och stärka Sveriges förmåga att hantera störningar och kriser inom energisystemet. Som beredskapsmyndighet ska Energimyndigheten säkerställa att verksamheter inom energiförsörjning fungerar även vid kris, höjd beredskap och krig. I rollen som sektorsansvarig myndighet leder Energimyndigheten arbetet inom beredskapssektorn energiförsörjning, ansvarar för att samordna aktörer, utveckla gemensamma hot- och riskanalyser, och ta framinriktningsdokument som styr sektorns arbete. Myndigheten har en krisledningsfunktion för samordning och arbetar för effektiv krishantering.

Inom det nationella cyberkrishanteringssystemet är Energimyndighetens roll framförallt att kontrollera efterlevnaden av informationssäkerhet för att på så sätt förebygga cyberincidenter och kriser. Energimyndigheten är ansvarig tillsynsmyndighet inom energisektorn. Tillsynsansvaret innebär en kontrollerande funktion där Energimyndigheten övervakar och utvärderar de leverantörer av samhällsviktiga tjänster som omfattas inom energisektorn.

Energimyndigheten har även en roll inom den cyberkrishantering som följer av nätkoderna. Energimyndigheten är behörig myndighet enligt nätkoderna i Sverige (18 § första stycket 1 förordningen [2025:784] med instruktion för Statens energimyndighet).

3.7.1.10 Sveriges Kommuner och Regioner

Sveriges kommuner och regioner (SKR) har ingen formell roll i den nationella beredskapsstrukturen, men fungerar som en central arena för kommuner och regioner att samverka och utbyta erfarenheter. SKR:s uppdrag är att bidra till att stärka medlemmars förmåga inom cyber- och informationssäkerhet och att verka för välfungerande samverkansstrukturer. SKR:s verkan även för medlemmarnas förmågehöjande arbete samt kan driva operativa frågor när det behövs. När gemensamma insatser och samordnade åtgärder krävs är SKR en naturlig partner för kommuner och regioner.

3.7.2 Övriga berörda myndigheter, organisationer och verksamhetsutövare

3.7.2.1 Inspektionen för vård och omsorg

Inspektionen för vård och omsorgs (IVO) roll inom det nationella cyberkrishanteringssystemet har fokus på förebyggande åtgärder inom sektorn för hälso- och sjukvård. I enlighet med NIS-direktivet, som är implementerat genom lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, har IVO tilldelats ett specifikt tillsynsansvar. Denna ansvarsroll innebär aktiv övervakning och utvärdering av hur väl leverantörer av samhällsviktiga digitala tjänster inom hälso- och sjukvårdssektorn efterlever säkerhetskraven.

IVO:s uppdrag omfattar tre huvudområden:

- att identifiera och registrera de leverantörer som faller under NIS-lagstiftningen
- att ta emot och hantera incidentrapporter från dessa leverantörer
- att bedriva en regelbunden tillsyn över deras arbete med informationssäkerhet

Genom denna tillsynsverksamhet bidrar IVO till att minska risken för incidenter och att begränsa de skador som eventuella incidenter kan orsaka, både genom att säkerställa att leverantörerna har adekvata förebyggande säkerhetsåtgärder på plats och genom att analysera och dra lärdomar från inträffade störningar. IVO:s roll innefattar även representation av Sverige i europeiska och internationella nätverk inom NIS-området.

3.7.2.2 Integritetsskyddsmyndigheten

Integritetsskyddsmyndigheten (IMY) arbetar för att skydda personuppgifter, så att de hanteras korrekt och inte hamnar i orätta händer. IMY tar varje år emot en stor mängd personuppgiftsincidentrapporter och klagomål som ofta beror på brister i organisationens informations- och cybersäkerhet. IMY kan inleda tillsyn för att utreda eventuella brister inom informations- och cybersäkerhet. Om det är brister i säkerheten för personuppgifter kan IMY meddela sanktionsavgift som en korrigerande befogenhet. IMY ger vägledning samt föreläser och utbildar inom området, ibland tillsammans med bland annat krisberedskapsmyndigheter, för att höja nivån på informations- och cybersäkerhet hos offentliga och privata organisationer.

3.7.2.3 Myndigheten för psykologiskt försvar

Myndigheten för psykologiskt försvar (MPF) ska i fredstid och vid höjd beredskap leda arbetet med att samordna och utveckla myndigheters och andra verksamhetsutövares verksamhet inom Sveriges psykologiska försvar. MPF ska bland annat identifiera, analysera och kunna lämna stöd i bemötandet av otillbörlig informationspåverkan och annan vilseledande information som riktas mot Sverige eller svenska intressen. Myndigheten följer i det operativa arbetet utländska antagonistiska verksamhetsutövare och påverkansaktiviteter i informationsmiljön som kan riktas mot Sverige. I arbetet ingår även att identifiera kognitiva effekter av påverkansaktiviteter, bland annat inom cyberområdet, som riktas mot Sverige. MPF:s uppdrag omfattar dock inte cyber eller informationssäkerhet, eller följdverkningar av cybersäkerhetsincidenter i sig.

3.7.2.4 Transportstyrelsen

Transportstyrelsen är ansvarig myndighet inom transportsektorn för tillsyn av säkerhetsskydd, cybersäkerhet och NIS. Tillsynsansvaret omfattar samtliga trafikslag (luft, sjö, järnväg och väg). Myndigheten är beredskapsmyndighet i beredskapssektorn Transporter med huvuduppgift att svara för regelgivning, tillståndsprövning och tillsyn inom transportområdet. Verksamheten ska särskilt inriktas på att bidra till ett internationellt konkurrenskraftigt, miljöanpassat och säkert transportsystem. Transportstyrelsens tillsyn ska utövas över järnvägs-, tunnelbane- och spårvägssystemen, över den civila sjöfarten (särskilt sjösäkerheten, sjöfartsskyddet och hamnskyddet), över den civila luftfarten (särskilt flygsäkerheten och luftfartsskyddet) och inom vägtransportsystemet. Transportstyrelsen ska särskilt ansvara för frågor om krav på infrastruktur, fordon, fartyg och luftfartyg, kompetenskrav och behörigheter, krav på infrastrukturförvaltare, trafikorganisatörer och trafikföretag, trafikregler, nyttjande av infrastruktur, anläggningar och service, villkor för marknadstillträde och konkurrensvillkor, och villkor för resenärer och de som köper godstransporttjänster. Vidare ska Transportstyrelsen svara för register över järnvägsfordon, luftfartygs- och inskrivningsregistret, fartygs- och sjömansregistret, registrering av avtal om båtbyggnadsförskott, vägtrafikregistret, och databasen över olyckor och personskador i trafiken.

3.7.2.5 Svenska kraftnät

Svenska kraftnät är ett statligt affärsverk som är systemansvarig myndighet för kraftsystemet i Sverige och som förvaltar och utvecklar Sveriges transmissionsnät för el. I rollen som systemansvarig myndighet ansvarar Svenska kraftnät för kraftsystemets driftsäkerhet och att det i varje ögonblick är balans mellan den el som produceras och den el som förbrukas. Svenska kraftnät är också Sveriges elberedskapsmyndighet. Det innebär att affärsverket arbetar för att elförsörjningen ska ha beredskap för extrema händelser som kan innebära svåra påfrestningar på samhället. Svenska kraftnät ser till att beredskapshöjande åtgärder genomförs, att det finns utbildad personal och att det finns resurser för kommunikation och reparation eller annan felavhjälpning.

Svenska kraftnäts krishanteringsorganisation och i förekommande fall tjänsteman i beredskap (TiB) lämnar vidare lägesbild och information till två sektorsansvariga beredskapsmyndigheter: Energimyndigheten och PTS. På förfrågan lämnar myndigheten också lägesbild till regeringen, MSB, länsstyrelser och civilområdesansvariga länsstyrelser.

3.7.2.6 Privata verksamhetsutövaret

Privata verksamhetsutövare inom näringslivet är viktiga för att bidra till att minska konsekvenserna av cybersäkerhetsincidenter och för att använda samhällets resurser effektivt. En väl fungerande privat-offentlig samverkan är en viktig förutsättning för Sveriges digitala motståndskraft.

Privata cybersäkerhetsverksamhetsutövare på den svenska marknaden utför tjänster inom incidentrapportering och kan vid begäran erbjuda stöd och återhämtningsåtgärder för att återgå till normal drift. Flera privata verksamhetsutövare erbjuder egenutvecklade CSIRT:s eller Security Operations Center (SOC). Dessa detektions- och responsplattformar bestående av cybersäkerhetsexperter övervakar och analyserar nätverksaktivitet för att upptäcka och reagera på cyberhot.

3.7.2.7 Svenskt Näringsliv

Svenskt Näringsliv samverkar med 49 arbetsgivar- och branschorganisationer och är den gemensamma rösten för 60 000 företag med nästan två miljoner medarbetare. Svenskt Näringslivs uppgift är verka för ett bättre företagsklimat i Sverige och att tala för alla företag och branscher, även de som ännu inte finns men som Svenskt Näringsliv anser kan uppstå omförutsättningarna är de rätta.

3.8 Infrastruktur, tjänster och övrigt stöd

Nedan beskrivs vilken infrastruktur, vilka tjänster och vilket övrigt stöd som CKHM och andra verksamhetsutövare kan använda för att underlätta hanteringen av en särskilt allvarlig cybersäkerhetsincident.

Upptäckt, hantering, övning och lärande av cybersäkerhetsincidenter sker med stöd av olika typer av infrastruktur och tjänster. För att säkerställa tillräcklig kapacitet är det centralt att funktionaliteten hos denna infrastruktur och tjänster är tillräckligt robust att de fungerar även under förhållanden där de är utsatta för cybersäkerhetsincidenter. Nyttjandet av infrastrukturerna och tjänsterna ställer även krav på användarna.

3.8.1 Incidentrapportering

Incidentrapportering är ett av sätten genom vilken nationell CSIRT, NCSC och de samverkande myndigheterna får en initial bild av omfattningen av en cybersäkerhetsincident och vilken efterföljande störning den resulterat i.

Olika myndigheter har olika tekniska lösningar som stöd för incidentrapporterna. För rapportering av incidenter till nationell CSIRT finns systemet IRON. Utöver IRON tar även nationell CSIRT emot incidentrapporter på andra sätt, exempelvis e-post och telefon.

Rapportering av säkerhetsincidenter och integritetsincidenter enligt lagen om elektronisk kommunikation (2022: 482) respektive säkerhetsincidenter och integritetsförluster av betydande omfattning i betrodda tjänster sker till PTS via e-post.

Företag rapporterar säkerhetsincidenter till FMV via e-post. Sekretess- och säkerhetsskyddsklassad rapport får endast skickas in med godkända metoder, exempelvis rek- och värdepost eller genom kurir.

3.8.2 Stöd till samhället, varningar och larm

Nationell CSIRT stödjer samhället genom att hitta brister och sårbarheter i system på internet och kontakta driftägare för åtgärd. Utöver detta finns ett antal tjänster som stöd för samhället, bland annat:

- **ANTS (Automatisk Notifiering av Tekniska Sårbarheter)**
  En tjänst som företag, organisationer och myndigheter kan ansluta sig till och som notifierar när en sårbarhet upptäcks hos företaget, organisationen eller myndigheten.

- **Blixtmeddelande**
  Ett kortfattat säkerhetsmeddelande som informerar berörda mottagare om en akut cybersäkerhetshändelse eller ett hot som kräver omedelbara motåtgärder.

Utöver detta finns det inom de samverkande myndigheterna tillgång till:

- **WIS**
  En portal för Sveriges civila beredskap där verksamhetsutövare delar information före, under och efter samhällsstörningar.

- **VMA (Viktigt Meddelande till Allmänheten)**
  Vid störningar som får omedelbar påverkan på liv, hälsa, egendom eller miljö kan det bli aktuellt att använda systemet VMA. Systemet består av meddelanden i radio och tv, som ibland föregås av utomhussignalen ”Viktigt meddelande”, samt en webbsida och applikationer.

- **Rakel**
  Sveriges nationella kommunikationssystem för samverkan och ledning för organisationer med ansvar inom allmän ordning, säkerhet, hälsa och försvar. Detta gör systemet viktigt för att kunna hantera de störningar och följdverkningar av störningar som en särskilt allvarlig incident kan medföra.

- **SGSI**
  Ett kommunikationsnätverk, skiljt från internet, för robust och säker kommunikation mellan användare i Sverige och i Europa.

3.9 Nationella beredskapsåtgärder

Övning och utbildning är en viktig del av att utveckla och validera samhällets förmåga att förebygga, identifiera och hantera cybersäkerhetsincidenter. En viktig del av genomförandet av planen blir att utveckla och genomföra anpassade övningar. Planen omfattar flera olika aktörer och roller som ska agera och fungera tillsammans vid en cybersäkerhetsincident. Övningen behöver därför innefatta de olika besluts- och utförandenivåer och samverkansberoenden som aktualiseras i planen.

Nedan redogörs för de nationella beredskapsåtgärder, inklusive övnings- och utbildningsverksamhet som inkluderas i den nationella strategin för cybersäkerhet 2025–2029.

Den nationella strategin för cybersäkerhet (Skr. 2024/25:121) utgår från nationella behov och från NIS 2-direktivet och dess allriskperspektiv för att hantera en bredd av utmaningar såsom kompetensbrist, komplex reglering, sårbara leveranskedjor och bristande systematiskt cybersäkerhetsarbete. Strategin kommer att uppdateras årligen och är därmed föremål för förändring.

Strategin riktar sig främst till myndigheter med särskilt ansvar för verksamhet som bedrivs inom ramen för NCSC och tillsynsmyndigheter inom den samlade cybersäkerhetsregleringen samt andra organisationer som ingår i beredskaps- och NIS 2-sektorerna.

I bilaga ett till cybersäkerhetsstrategin (Handlingsplan 2025) finns aktiviteter med ansvariga myndigheter och organisationer som svarar på regeringens inriktning och kraven i NIS 2-direktivet. Dessa aktiviteter utgör en viktig del av nationella beredskapsåtgärder, övningar och annan verksamhet för att stärka den nationella cybersäkerheten och sammanfattas nedan.

Bilaga två[18] av cybersäkerhetsstrategin sammanfattar vilka organisationer som har roller och ansvarsområden inom cybersäkerhet från 2025–2029. Dessa myndigheters verksamhet utgör en delmängd av nationella beredskapsåtgärder för att stärka nationell cybersäkerhet.

[18] Skr. 2024/25:121, Bilaga 2: Organisationer med roller och ansvarsområden inom cybersäkerhet.

3.9.1 Myndighetsverksamhet – övergripande beredskapsåtgärder

- NCSC har i uppdrag att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter.

- CSIRT-enheten ska enligt NIS 2-direktivet bland annat övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå samt tillhandahålla varningar och sprida information om dessa.

- Cyberkrishanteringsmyndigheten ansvarar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser.

- Vid en cybersäkerhetsincident finns ett antal aktörer som, beroende på typ av incident, ska ta emot rapporter om incidenter utifrån olika regleringar.

- Sex tillsynsmyndigheter ansvarar för tillsynen inom de sektorer som träffas av NIS-direktivet. MSB driver ett nationellt samarbetsforum gällande NIS-frågor där de sex tillsynsmyndigheterna och Socialstyrelsen ingår. Forumets syfte är att underlätta den nationella samordningen och att åstadkomma en effektiv och likvärdig tillsyn.

- Beredskapsmyndigheterna ansvarar, enligt förordningen (2022:524) om statliga myndigheters beredskap, för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.

- Säkerhetspolisen och Försvarsmakten har enligt säkerhetsskyddsförordningen till uppgift att samordna övriga tillsynsmyndigheter inom säkerhetsskyddsområdet och utövar även tillsyn över de allra mest skyddsvärda verksamheterna.

- FMV är nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt. FMV bedriver tillsyn och samverkan över det europeiska ramverket för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt.

- Kommuner och regioner ansvarar för sin egen cybersäkerhet och har en central roll för Sveriges cybersäkerhet.

3.9.2 Myndighetsverksamhet - övningar:

- FOI, Försvarsmakten och MSB har i samverkan utvecklat Sveriges nationella cyberanläggning för totalförsvaret, Crate. FOI använder sedan 2009 Crate för att tillhandahålla träning i cybersäkerhet till relevanta aktörer inom totalförsvaret.

- RISE Cyber Range är en testbädd som drivs av RISE (Research Institutes of Sweden). Genom testbädden kan företag och organisationer testa tekniska system, identifiera sårbarheter och säkerställa adekvata rutiner och organisation. Målgruppen är både näringsliv som offentlig sektor.

3.9.3 Myndighetsverksamhet - utbildning:

- Cybercampus Sverige inrättades 2024 och har fokus på forskning, innovationer och utbildningar. Det är en satsning och ett samarbete mellan universitet, institut, myndigheter och företag i hela Sverige.

Till strategins pelare och mål kopplas även en handlingsplan som innehåller ett antal aktiviteter som svarar mot regeringens inriktning och kraven i NIS 2-direktivet. Handlingsplanen omsätter strategin i konkret handling genom aktiviteter i form av bland annat specifika uppdrag och styrning av myndigheter.

Handlingsplanen sammanfattar nationella beredskapsåtgärder, inklusive övnings- och utbildningsverksamhet 2025-2029 enligt nedan.

3.9.4 Aktiviteter - övergripande beredskapsåtgärder (urval):

- FRA ska utarbeta en nationell operativ plan för storskaliga cybersäkerhetsincidenter och kriser i enlighet med artikel 9 i NIS 2-direktivet.

- NCSC bedrivs utifrån en ny förordning i syfte att ge tydlig och långsiktig styrning som lägger grunden för ett välfungerande NCSC och tydliggör dess roll i det nationella cybersäkerhetsarbetet.

- CER- och NIS 2-direktiven genomförs nationellt på ett harmoniserat sätt. Genom att stärka och harmonisera lagstiftningen på området skapas förutsättningar för att cybersäkerhetsarbetet hos organisationer ska få större genomslag samt bidra till ökad motståndskraft i samhällsviktig verksamhet och därmed ett stärkt civilt försvar.

- FRA och MSB ska inom ramen för NCSC ta fram riktlinjer som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) kräver.

- MSB fortsätter utveckla och förvalta råd och stöd för organisationers systematiska cybersäkerhetsarbete.

- Finansinspektionen fortsätter utöva tillsyn över den finansiella sektorns cybersäkerhetsarbete och digitala operativa motståndskraft.

- MSB vidareutvecklar Cybersäkerhetskollen för att kunna bistå fler organisationer i fler processer och kunna förmedla en fördjupad nationell lägesbild kring cybersäkerhetsnivån i samhällsviktiga verksamheter.

- MSB tillförs medel för förberedelse av en nationell kartläggning av kommuners tekniska cybersäkerhetsförmåga.

- Över 100 myndigheter implementerar uppdrag att redogöra för hur de förvaltat och utvecklat sitt arbete med informations- och cybersäkerhet.

- MSB etablerar en kompletterande analysmiljö till Cybersäkerhetskollen där drift, förvaltning och utveckling ingår.
- MSB tillhandahåller stöd för samhällsviktig verksamhets arbete med säkerhet i operativ teknik.
- Hotbildsstyrda penetrationstester genomförs regelbundet på organisationer inom den finansiella sektorn.
- Berörda statliga myndigheter fortsätter inom ramen för etablerad NCSC-samordning kring standardisering av cybersäkerhet.
- FMV deltar i samarbeten och aktiviteter som bedrivs inom ramen för EU:s ramverk för cybersäkerhetscertifiering. I dessa sammanhang ska myndigheten bland annat söka få genomslag för svenska ståndpunkter och verka för att nya certifieringsordningar tas fram på ett transparent sätt.
- MSB genomför en kartläggning av digitala leveranskedjor och tar fram en modell för uppföljning av digitala leveranskedjor.
- Berörda statliga myndigheter fortsätter inom ramen för NCSC arbetet med en nationell modell där föreskrifter, allmänna råd och vägledningar så långt som möjligt ensas så att de följer en likartad logik, struktur och terminologi.
- FRA ska inom ramen för NCSC främja samverkan med privata och offentliga aktörer. Stärkt privat-offentlig samverkan skapar förutsättningar för bland annat effektivare informationsdelning.
- NCSC tar fram lägesbilder avseende cyberhot och incidenter. Aktiviteten stödjer målet genom att lägesbilder avseende aktuella cyberhot och incidenter tas fram för näringslivet, kommuner och regioner, myndigheter samt Regeringskansliet och därmed stöttar aktörer i att förstå hotbilden på såväl cyber- som hybridområdet.
- Berörda statliga myndigheter fortsätter att inom ramen för årsrapporter informera om hotbilden inom sina respektive sakområden.
- FRA fortsätter erbjuda tekniskt detekterings- och varningssystem (TDV) till de mest skyddsvärda verksamheterna.
- MSB skapar en samlad portal med smarta formulär för rapportering av incidenter, tillbud, sårbarheter och cyberhot under olika regelverk, primärt NIS 2- och CER-direktivet.
- Polismyndigheten ser över förutsättningarna att etablera en process för ökat samarbete kring incidentrapportering.

3.9.5 Aktiviteter – utbildning

- MSB säkerställer att utbildningar kommer till stånd för organisationer som omfattas av NIS 2-direktivet och beredskapssektorerna. Aktiviteten stödjer målet genom att höja kompetensen hos organisationer som ska bedriva ett systematiskt cybersäkerhetsarbete.

- Säkerhetspolisen och Försvarsmakten utvecklar kontinuerligt stödjande material såsom vägledningar, handböcker och utbildningsmaterial inom säkerhetsskydd.

- MSB förvaltar, utvecklar och tillhandahåller publik databas över svensk terminologi inom cybersäkerhetsområdet.

- MSB tillhandahåller och vidareutvecklar rådgivningstjänst med särskilt fokus på NIS 2-aktörer.

- FRA och MSB ska inom ramen för NCSC ta fram riktlinjer som stärker cyberresiliensen och cyberhygienen hos små och medelstora företag, särskilt de som inte omfattas av NIS 2-direktivet, genom att tillhandahålla lättillgänglig vägledning och stöd för deras specifika behov, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) – j) anger att medlemsstaterna ska anta.

- Medel tillförs MSB för att vidareutveckla kampanjen ”Tänk säkert”.

- FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att främja och utveckla cybersäkerhetsutbildning, cybersäkerhetskompetens, medvetandehöjande åtgärder och forsknings- och utvecklingsinitiativ, samt vägledning om god praxis och kontroll för cyberhygien som riktar sig till medborgare, intressenter och entiteter, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) – j) anger att medlemsstaterna ska anta..

- MSB verkar för att privata och offentliga organisationer ges tillgång till och kan nyttja det tekniska och organisatoriska stöd som tillhandahålls på EU-nivå för att stärka motståndskraften mot storskaliga cyberattacker.

- Polismyndigheten deltar i samarbete med finans- och transaktionsmarknaderna i arbetet för säkrare betalningar.

- Polismyndigheten deltar i brottsförebyggande nätverk gällande cyberbrott.

- Polismyndigheten deltar i brottsförebyggande samarbete med Stöldskyddsföreningen och andra aktörer. Arbetet innefattar att genom Säkerhetskollen.se ge varningar till allmänheten om pågående bedrägeritrender, att via ett kunskapscenter med MSB och flera andra statliga myndigheter skapa bl.a. medvetandehöjande kampanjer och helpdesk samt att genom Digitala varningsgruppen fortsätta det brottsförebyggande arbetet.

3.9.6 Aktiviteter – övningsverksamhet

- Nationell informationssäkerhetsövning (NISÖ) fortsätter att genomföras inom ramen för NCSC. Aktiviteten stödjer målet genom att ge privata och offentliga aktörer möjlighet att öva tillsammans och därigenom stärka samhällets samlade förmåga att hantera it-relaterade samhällsstörningar där skyndsam samordning krävs.

- Statliga myndigheter genomför, inom ramen för NCSC, nationella cybersäkerhetsövningar. Aktiviteten stödjer målet genom övningar som bland annat berör incidenthantering och bidrar till att stärka Sveriges förmåga att förebygga, upptäcka och hantera cyberhot och cyberangrepp.

- MSB fortsätter att planera, genomföra, utvärdera cybersäkerhetsövningar, inklusive att utveckla nationell Cyber Range.

- Inom ramen för NTSG:s krisberedskapsövningar övar aktörer inom elektroniska kommunikationer på cyberincidenter när så är lämpligt. Syftet är att aktörer inom elektronisk kommunikation utvecklar bättre rutiner och färdigheter i hanteringen av cybersäkerhetsrelaterade risker.

4. Förkortningar

I denna skrift används bland annat följande förkortningar:

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
CER-direktivet	Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG
CKHM	Cyberkrishanteringsmyndighet
CSIRT	Computer Security Incident Response Team
Cyberplanen	Rådets rekommendation av den 6 juni 2025 om en EU-plan för hantering av cyberkriser (C/2025/3445)
DORA-förordningen	Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011
Enisa	Europeiska unionens cybersäkerhetsbyrå
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
FMV	Försvarets materielverk
FOI	Totalförsvarets forskningsinstitut
FRA	Försvarets radioanstalt

IKT	Informations och kommunikationsteknologi
MSB	Myndigheten för samhällsskydd och beredskap (1 januari 2026 byter MSB namn till Myndigheten för civilt försvar)
NCSC	Nationellt cybersäkerhetscenter
NCSC-förordningen	Förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
NIS 2-direktivet	Europaparlamentets och rådets direktiv (EU) 2022/2055 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
NISÖ	Nationell informationssäkerhetsövning
NTSG	Nationella telesamverkansgruppen
Nätkoderna	Kommissionens delegerade förordning (EU) 2024/1366 av den 11 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden.
PTS	Post-och telestyrelsen
RISE	Research Institutes of Sweden

NATIONELLT
CYBERSÄKERHETSCENTER

ncsc.se
ncsc@ncsc.se

FRA

fra.se
fra@fra.se