
NATIONELLT
CYBERSÄKERHETSCENTER
En del av FRA
En kraftsamling för Sveriges cybersäkerhet
En årsberättelse från Nationellt cybersäkerhetscenter
2025

Rapporten beskriver NCSC:s verksamhet och det cybersäkerhetsläge som centret följt under 2025. Utvecklingen inom cybersäkerhetsområdet är snabb och händelser kan ha tillkommit efter rapportens färdigställande.

Formgivning och produktion: Intellecta

Tryck: Multiply Solutions, 2026

Omslagsbild: Hans Strand / Folio

Denna bild: Jan Ohrstrom / Shutterstock.com

Stärkt cybersäkerhet byggs varje dag – i varje organisation och i varje verksamhet.

John Billow
chef Nationellt cybersäkerhetscenter

Tillsammans stärker vi Sveriges cybersäkerhet

Detta är den första årliga redovisningen av verksamheten inom Nationellt cybersäkerhetscenter (NCSC) enligt centrets nya styrning och som en del av Försvarets radioanstalt (FRA). Det nya, förstärkta mandatet för NCSC innebär en kraftsamling av ansvar och uppdrag för arbetet med att stärka och utveckla Sveriges förmåga på cybersäkerhetsområdet.

Redovisningen för 2025 visar att NCSC vid FRA, med ett tydligare mandat och styrning, har bättre förutsättningar för att utföra sitt uppdrag. NCSC är under stark tillväxt och utveckling. Under 2025 har vi lagt grunden och angett inriktningen för verksamheten, genomfört flertalet rekryteringar och gjort en första organisatorisk indelning på avdelningen. Nya medarbetare har börjat under hela året, och en ledningsgrupp för centret tillträdde under andra halvåret 2025.

Själv tillträdde jag den 1 september efter att regeringen utsåg mig till chef för NCSC. Under min första tid vid centret har jag fokuserat på att både interagera med externa partners och ge inriktning för det fortsatta bygget av centret vid FRA. I detta har ingått särskilt nära samverkan med Myndigheten för civilt försvar (dåvarande Myndigheten för samhällsskydd och beredskap, MSB) för att förbereda för att den myndighetens uppdrag, ansvar och medarbetare på cybersäkerhetsområdet förs över till NCSC vid FRA den 1 juli 2026.

NCSC:s framgång i uppdraget att stötta verksamhetsutövarna i deras cybersäkerhetsarbete bygger på att skapa meningsfulla partnerskap och samarbeten. I det arbetet är samarbete med olika organisationer, näringsliv och samverkande myndigheter helt centralt. Var och en av våra samarbetspartners har viktig expertis och information som är relevant för uppdraget att stärka Sveriges cybersäkerhet.

Stärkt cybersäkerhet byggs varje dag — i varje organisation och i varje verksamhet. Det är tillsammans som vi skapar ett motståndskraftigt Sverige och vi är alla en del av Sveriges samlade totalförsvar.

John Billow
chef Nationellt cybersäkerhetscenter

Ett center tar form

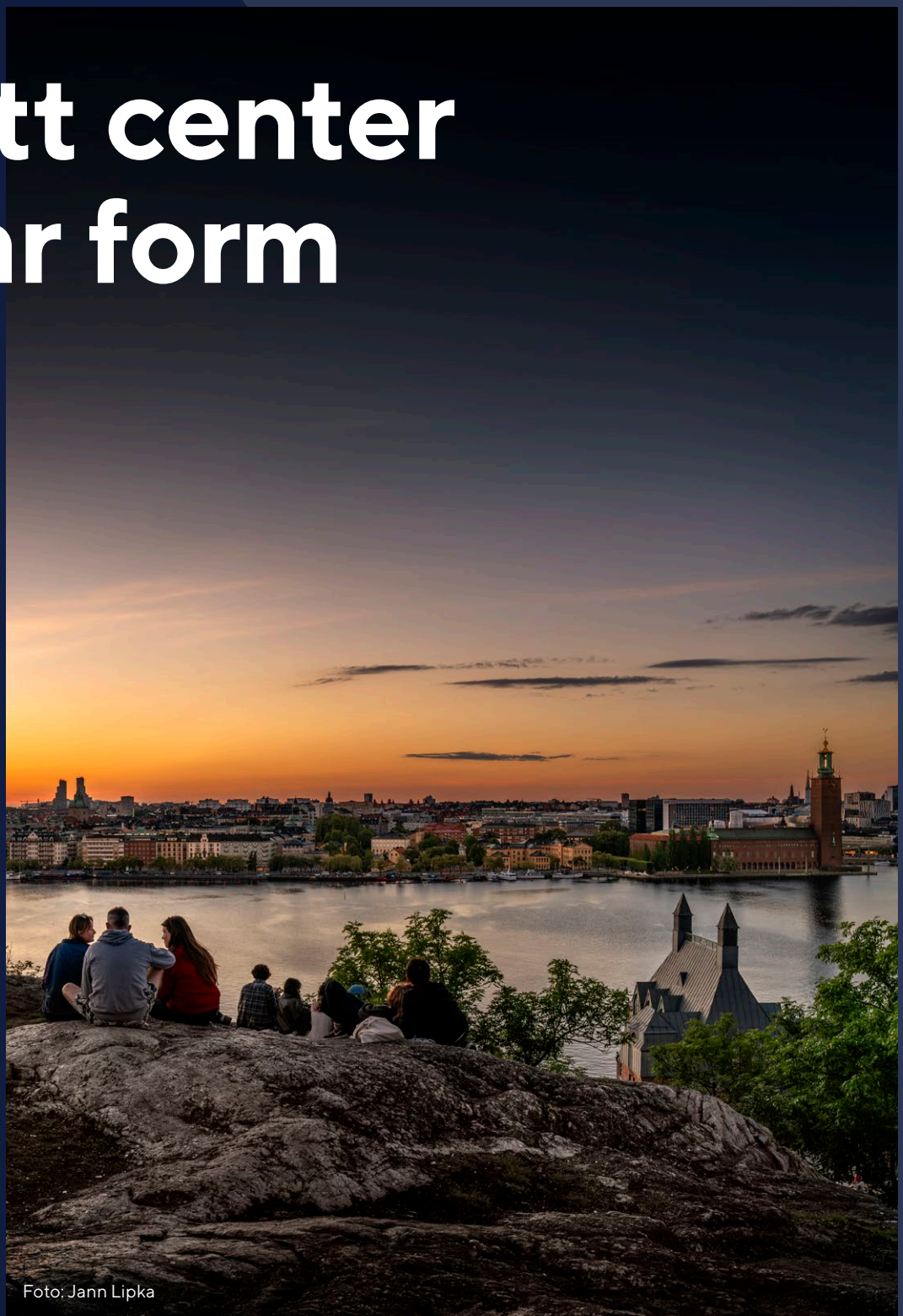

Foto: Jann Lipka

Ny huvudman, ny förordning, nytt uppdrag

Det nationella cybersäkerhetscentret befinner sig i en stor förändring. Med FRA som ny huvudman, en ny förordning och ett förstärkt mandat har NCSC under 2025 lagt grunden för en organisation som ska stärka hela Sveriges cyberförmåga. Det handlar om mer än ett organisationsbyte, det är startskottet för ett nytt kapitel i landets cybersäkerhetsarbete.

Den 1 november 2024 blev Försvarets radioanstalt (FRA) huvudman för Nationellt cybersäkerhetscenter (NCSC), och den 1 januari 2025 blev NCSC organisatoriskt en avdelning inom FRA. Den 22 april 2025 trädde NCSC-förordningen[1] i kraft. Förordningen slår fast att NCSC ska utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Centret ska också utgöra en nationell plattform för samverkan och informationsutbyte mellan privata och offentliga aktörer i frågor som rör cybersäkerhet. FRA ska organisera, leda och planera verksamheten som bedrivs inom ramen för NCSC, och inom ramen för denna verksamhet samverka med de så kallade samverkansmyndigheterna, det vill säga Försvarets materielverk (FMV), Försvarsmakten, Myndigheten för civilt försvar, Polismyndigheten, Post- och telestyrelsen (PTS) och Säkerhetspolisen.

Enligt 6 § NCSC-förordningen ska FRA senast den 1 mars varje år lämna en redovisning av det arbete som utförts inom det nationella cybersäkerhetscentret till Regeringskansliet (Försvarsdepartementet). Försvarets radioanstalt ska i redovisningen värdera, sammanställa och rapportera resultatet av arbetet i centret.

Årsberättelsen inleds med en beskrivning av utvecklingen av cyberangrepp mot svenska verksamheter under året. Därefter redovisas arbetet med NCSC:s uppdrag enligt NCSC-förordningen (samverkan, incidentkoordinering, övning och utbildning, analys och lägesbild, samt kommunikation och kunskapsspridning). Därefter redogörs för NCSC:s kommunikation och medverkan i externa sammanhang. Slutligen presenteras arbetet med regeringsuppdrag, samt NCSC:s aktiviteter i cybersäkerhetsstrategins handlingsplan.

Att bygga ett center

Under 2025 har ett stort fokus varit på att bygga upp NCSC:s egen organisation, samt att etablera nödvändiga och effektiva interna rutiner och processer och därigenom skapa förutsättningar för att centret framgent fullt ut ska kunna axla rollen som nationell plattform för cybersäkerhet i Sverige.

Detta har först och främst innefattat en omfattande rekrytering. Vid årets början hade NCSC 7 medarbetare, och vid årets slut totalt 18 medarbetare. Under året har den operativa verksamheten vid centret till del kunnat genomföras med stöd av inlånade medarbetare från FRA:s cyberavdelning. Ytterligare ett tjugotal rekryteringar, som initierades under slutet av 2025, förväntas kunna slutföras under första halvåret 2026.

[1] Förordning (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt.

I augusti utnämnde regeringen en chef för NCSC, som tillträdde den 1 september. Under september och oktober tillkom också en stabschef och två kontorschefer, och med det hade avdelning NCSC en permanent ledningsgrupp på plats.

Planering för NCSC:s lokalförsörjning, ändamålsenliga tekniklösningar och infrastruktur har tagit betydande resurser i anspråk under 2025 och skett under ledning av FRA:s avdelningar för verksamhetsstöd och teknik. Förberedelser har gjorts både för de tillfälliga och externa lokaler som NCSC ska ta i anspråk från och med 2026 och för den permanenta lokal i Bergshamra dit centret ska flytta omkring 2030.

NCSC har också, med övriga delar av FRA, samverkat med Myndigheten för civilt försvar (dåvarande MSB) under hela 2025 för att planera och förbereda för den överföring av den myndighetens cybersäkerhetsverksamhet till NCSC vid FRA som regeringen beslutade om den 20 november 2025. Verksamhetsövergången sker den 1 juli 2026.

NCSC:s uppdrag: Att stärka Sveriges samlade cyberförmåga

NCSC-förordningen anger att NCSC särskilt ska bidra till att samordna och harmonisera det nationella cybersäkerhetsarbetet. Centret ska lämna råd och stöd till privata och offentliga aktörer i frågor om hot, sårbarheter och risker med koppling till cybersäkerhet; lämna råd och stöd till privata och offentliga aktörer vid it-incidenter; genomföra utbildningar, övningar och andra kompetenshöjande insatser inom cybersäkerhetsområdet; samt ta fram samlade lägesbilder rörande antagonistiska cyberhot och andra it-incidenter till privata och offentliga aktörer.

NCSC 2025 — årsöversikt

Våra samverkansmyndigheter

Myndigheten för civilt försvar

Polisen

FÖRSVARSMAKTEN

PTS

Säkerhetspolisen

FMV

2 apr — Nationell cybersäkerhetsstrategi
kommunikation

3 apr — Natoövning · Regeringskansliet
övning

6 maj — MSB webbinarium
samverkan

15 maj — Faktablad "Rekommendationer kvantsäker kryptografi"
rapport

16 maj — NCSC finansforum 2
samverkan

22 maj — Webbinarium eSam
samverkan

22 maj — Föreläsning Polismyndigheten
samverkan

23 maj — NCSC energiforum 2
samverkan

26 maj — Rundabordssamtal hos Palo Alto
samverkan

Överbelastningsangrepp mot SVT
incident

Kritisk sårbarhet Microsoft SharePoint
incident

12 jun — Rekommendationer DDoS-skydd
kommunikation

24 – 26 jun — Almedalen, 6 panelsamtal
kommunikation

APRIL

MAJ

JUNI

NCSC ska samordna det nationella cybersäkerhets-arbetet, lämna råd vid it-incidenter och vara Sveriges kontaktpunkt i internationella sammanhang.

NCSC ska vidare bistå Regeringskansliet med samlade lägesbilder som bland annat innehåller bedömningar av hotnivån; rapportera till regeringen om förhållanden på cybersäkerhetsområdet som kan leda till behov av åtgärder och lämna förslag på sådana åtgärder; samt informera regeringen om relevanta förhållanden vid ett antagonistiskt cyberhot eller annan it-incident som har vållat, eller kan antas ha potential att vålla, betydande skada.

Centret ska också vara en kontaktpunkt gentemot motsvarande funktioner i internationella sammanhang, och utveckla samarbetet och informationsutbytet med dessa.

I tillägg till NCSC-förordningen innehåller Nationell cybersäkerhetsstrategi 2025–2029 (bilaga 1, handlingsplan)[2] aktiviteter/åtgärder som träffar NCSC tillsammans med flera andra myndigheter. Flertalet av dessa aktiviteter, men inte alla, överlappar med förordningens punkter ovan.

Slutligen har NCSC under år 2025 tagit emot och hanterat fyra separata regeringsuppdrag, varav ett har handlat om att tillsammans med Myndigheten för civilt försvar ta fram riktlinjer i enlighet med NIS 2-direktivet; ett om att utarbeta en nationell operativ plan för hantering av storskaliga cybersäkerhetsincidenter och kriser; ett om att ta fram en modell för mätning av resultatindikatorerna i den nationella cybersäkerhetsstrategin; och ett om att ge stöd inför, under och efter valen 2026.[3]

[2] En ny era av cybersäkerhet — Nationell strategi för cybersäkerhet 2025–2029 (Skr. 2024/25:121), bilaga 1.
[3] Se Regeringsuppdrag och strategiska aktiviteter, Övriga uppdrag och uppgifter under året.

... fortsättning årsöversikt

Foto: Shutterstock.com

Utpressningsangrepp Svenska kraftnät
- incident

1 – 30 okt — Tänk säkert-kampanj
- kommunikation

7 – 8 okt — MISP-övning 1
- övning

10 okt — Energiforum 3
- samverkan

20 – 21 okt — Nationell Cybersäkerhetskonferens
- kommunikation

21 okt — FOI rapport Ragnarök
- övning

21 – 22 okt — MISP-övning 2
- övning

23 – 24 okt — MISP-övning 3
- övning

13 nov — MSB konferens beredskapsmyndigh.
- samverkan

18 – 19 nov — Mässa THS Armada
- kommunikation

21 nov — Webbinarium statliga bolag
- samverkan

25 nov — Arbetsgrupp cybersäk. valnätverk
- samverkan

28 nov — Samverkansgrupp Gotland
- samverkan

1 – 3 dec — Cyber Coalition 2025
- övning

5 dec — NCSC finansforum 4
- samverkan

9 &18 dec — Filmer 10 säkerhetsåtgärder
- kommunikation

11 dec — ITCF nätverksträff
- samverkan

12 dec — Redovisning samverkansmodell
- samverkan

15 dec — Länsstyrelsen Sthlm
- samverkan

OKT NOV DEC

Utveckling av cyberangreppen 2025

Foto: Folio

Cyberangreppens utveckling

Hoten mot Sverige är reella, återkommande och i ständig förändring. Under 2025 drabbades svenska myndigheter, företag och samhällsviktig infrastruktur av både överbelastningsangrepp och utpressningsangrepp. Hotaktörerna agerar metodiskt och utnyttjar säkerhetspolitiska händelser, tekniska sårbarheter och mänskliga misstag.

Under året har bekräftade överbelastningsangrepp såväl som uttalade hot om överbelastningsangrepp mot svenska verksamheter eller verksamheter med koppling till Sverige noterats i NCSC:s samlade omvärldsbevakning.

Drabbade verksamheter återfinns inom sektorer som offentlig förvaltning, digital infrastruktur, transport, bank och finans, media samt hälso- och sjukvård. Angreppen har påverkat tillgång till interna system och tillhandahållna e-tjänster.

Förutom bekräftade överbelastningsangrepp publiceras även uttalade hot om överbelastningsangrepp återkommande på sociala mediekonton med koppling till olika hotaktörer. Dessa utpekanden har typiskt sett haft koppling i tid till säkerhetspolitiska händelser såsom politiska arrangemang eller utökat stöd till Ukraina. Även andra händelser utnyttjas återkommande av opportunistiska angripare som försöker genomföra överbelastningsangrepp i anslutning till brett uppmärksammade händelser. Ett exempel från 2025 är när Skatteverket drabbades av överbelastningsangrepp i samband med att tjänsten för inkomstdeklaration öppnade. Tillgången till externa e-tjänster påverkades tillfälligt.

I juni drabbades SVT av återkommande överbelastningsangrepp, vilket påverkade åtkomsten till SVT:s digitala utbud, däribland SVT Play och SVT:s webbplats. Både appen och webbplatsen var delvis otillgängliga.

Under senare delen av november noterades exempelvis en markant ökning i antalet utpekade hot om överbelastningsangrepp mot totalt ett femtiotal svenska verksamheter i både privat och offentlig sektor. Bland dessa fanns politiska partier, statliga myndigheter, regioner, kommuner samt flera företag inom exempelvis telekommunikation- och transportsektorn. Utpekandena bedöms ha koppling till ett forum med fokus på Ukraina, som anordnades i Riksdagen i slutet av november.

Överbelastningsangrepp kan drabba användare när samhällsviktiga tjänster påverkas och inte kan nås. Här kan nämnas de återkommande överbelastningsangreppen mot BankID i april, vilka medförde att användare exempelvis inte kunde använda Swish för betalningar eller logga in på sin bank.

Utpressningsangrepp — när data blir gisslan

Under året har även flera svenska verksamheter utsatts för utpressningsangrepp. De drabbade verksamheterna inkluderar bland annat myndigheter, verksamheter inom energisektorn samt företag inom den privata sektorn. Bland de mest uppmärksammade fallen hör Sportadmin, en administrativ tjänst som nyttjas av tusentals svenska idrottsföreningar, systemleverantören Miljödata samt beredskapsmyndigheten Svenska kraftnät.

Utpressningsangrepp är en allvarlig typ av cyberangrepp. De leder inte sällan till avbrott i den drabbade verksamheten, då man kan förlora tillgång till information och it-system som används i den dagliga verksamheten.

Hur allvarligt ett utpressningsangrepp är beror helt på vilka system som är påverkade. Om alla it-system som exempelvis en kommun förvaltar blir påverkade är det oftast mycket allvarligt och en besvärlig situation både för medarbetare inom kommunen och allmänheten. Har kommunen säkerhetsåtgärder på plats, med säkerhetskopior, reservrutiner, kontinuitetsplaner, krisplaner etc. för att verksamheten ska kunna fortsätta utan it-system en tid, så är förutsättningarna bättre. Men påverkan kommer att bli stor för verksamheten.

Angriparna bakom utpressningsangreppen som observerats under 2025 har i flera fall hotat med, och även verkställt, att läcka och publicera information från den berörda verksamheten. Den läckta informationen har bland annat inkluderat personuppgifter, även skyddade sådana. Konsekvenserna av att informationen gjorts tillgänglig bedöms även utgöra en ökad risk för följdangrepp, till exempel nätfiske och bedrägerier mot verksamheter där person- och kontaktuppgifter har exponerats.

NCSC rekommenderar att svenska verksamheter i både privat och offentlig sektor fortsatt bör bevaka överbelastningsangrepp i sin omvärldsbevakning och se över sina rutiner för att hantera sådana angrepp. Det systematiska it-säkerhetsarbetet och förebyggande insatser är viktiga för att ha en stabil it-miljö och kunna stå emot överbelastningsangrepp.

Så har varit fallet i följderna av angreppen mot Sportadmin och Miljödata, där stora mängder personuppgifter publicerats på Darknet.[4] Det finns exempel på att kontaktförsök med försök till nätfiske förekommit mot organisationer och individer vars namn och/eller kontaktuppgifter publicerats.

Utöver de drabbade verksamheterna som nämns ovan, har flera verksamheter med koppling till Sverige förekommit på en bevakningstjänst för utpressningsangrepp. I vissa fall överensstämmer publiceringen med ett konstaterat angrepp i närtid, men det finns även exempel på när information som stulits vid ett tidigare angrepp publiceras en lång tid senare.

Utpressningsangrepp innebär ofta en påtaglig negativ påverkan för en verksamhet. Det kan exempelvis innebära stora ekonomiska kostnader för återställning av system och potentiella förluster av intäkter för den drabbade verksamheten. Därtill kan system och funktioner slås ut, vilket påverkar verksamheter och samhällskritiska tjänster. Det kan även skada förtroende hos allmänheten såväl som kunder gentemot den drabbade verksamheten.

[4] Med Darknet avses alternativa nätverk som är invävda i ”det öppna internet”. För att kunna ansluta sig till ett Darknet krävs i regel specialmjukvara, till exempel en särskild webbläsare. Darknet är designat för att erbjuda anonymitet och vara motståndskraftigt mot censur och övervakning.

Mot bakgrund av förekommande hot och utförda utpressningsangrepp, uppmanar NCSC svenska verksamheter, både i privat och offentlig sektor, att vara fortsatt vaksamma på avvikelser i sina it-miljöer som kan innebära att risken att utsättas för utpressningsangrepp ökar.

Organisationer behöver ha rutiner för att hålla sina it-system uppdaterade för att undvika att en angripare utnyttjar sårbarheter för att få tillgång till it-miljön. En annan viktig del i det systematiska arbetet är att utbilda organisationen i god cyberhygien. Alla användare på en arbetsplats, även i egenskap av privatpersoner, är en del av lösningen i att skydda och försvara it-miljön och därför behöver användarna utbildas i att exempelvis vara vaksamma vid e-posthantering. Skadlig kod kan komma in via e-post i länkar och bifogade dokument, och kan då användas av en angripare för att skaffa sig tillgång till it-miljön.

Tillsammans stärker vi cyberskyddet

Foto: Shutterstock.com

Forum, förtroende och nya strukturer

Ingen aktör kan ensam möta de cyberhot som Sverige står inför. Samverkan är därför inte ett komplement till NCSC:s uppdrag, utan en central del av arbetet. Under 2025 har NCSC fortsatt att utveckla och upprätthålla samverkan med offentliga och privata aktörer genom forum, nätverk och strukturer för informationsutbyte under trygga former.

Samverkan är en central del av NCSC:s verksamhet, och en förutsättning för att centret ska klara sitt samlade uppdrag. Samverkan handlar om att skapa långsiktiga och förtroendefulla relationer. NCSC bidrar till detta bland annat genom att erbjuda en mötesplats och en miljö där information och erfarenheter kan delas mellan olika aktörer under trygga former. NCSC kan också koppla ihop aktörer som kan ha nytta av att tala med varandra. Inom ramen för NCSC:s samverkan sker ett värdefullt informationsutbyte mellan offentliga och privata aktörer i olika sektorer och branscher. På så sätt kan olika aktörer stärka varandra genom att dela med sig av sina erfarenheter av incidenter och händelser, och hur dessa har hanterats.

Under 2025 har NCSC arbetat med samverkan bland annat genom centrets formella forum, NCSC Finansforum och NCSC Energiforum. NCSC har också samverkat med transportsektorn och telekomsektorn, samt med ett stort antal aktörer i bland annat näringslivet och försvarssektorn.

Arbete har också gjorts under året med att utveckla strukturer och former för NCSC:s framtida partnersamverkan. Fokus har varit på att skapa strukturer som fungerar praktiskt med hänsyn till etablerade roller, ansvar och arbetssätt hos NCSC. Ambitionen har varit att de strukturer som tas fram ska kunna vidareutvecklas över tid, vartefter erfarenheter som NCSC kan ta lärdom av samlas in. Fokus för 2026 är att implementera detta operativt. I slutredovisningen av arbetet har ett antal olika etableringsformer föreslagits, som möjliggör för NCSC att utveckla sin samverkansförmåga i takt med att organisationen växer och mognar.

Cybersäkerhet i finanssektorn

NCSC Finansforum etablerades 2022 och består i dag av ett tjugotal medlemmar från näringslivet, branschorganisationer och myndigheter. Forumets syfte är att genom samverkan stärka cybersäkerheten inom finanssektorn och tillsammans öka Sveriges motståndskraft mot cyberhot. Forumet drivs av en styrgrupp där NCSC, Myndigheten för civilt försvar och ett antal utvalda medlemmar i forumet ingår. Styrgruppen planerar forumets möten och ansvarar också för att inrikta forumets arbete och framdrift. Inom forumet finns fyra arbetsgrupper (AG): AG informationsdelning, AG hotaktörsanalys, AG övning och utbildning, samt AG medlemsriktlinjer.

AG informationsdelning har under 2025 bland annat deltagit i referensgruppen för det nationella MISP-SE-projektet, som leds av Myndigheten för civilt försvar.

AG medlemsriktlinjer startades upp 2025 med syfte att se över forumets medlemsriktlinjer och omhänderta frågor om hur forumet ska arbeta framgent. Ett förslag till nya medlemsriktlinjer har tagits fram som ska presenteras för NCSC.

Under 2025 har Finansforum haft fyra strategiska möten, det vill säga möten för forumets samtliga medlemmar. Mötena är fysiska och roterar mellan medlemsorganisationerna.

Cybersäkerhet i energisektorn

NCSC Energiforum etablerades 2024 och har i dag 22 medlemmar från den privata sektorn, branschorganisationer och myndigheter. Syftet med forumet är att genom samverkan stärka cybersäkerheten inom energisektorn. En styrgrupp för forumet har formaliserats under 2025 under namnet AG stab. AG stab leds av NCSC och består i övrigt av representanter från Energimyndigheten, Myndigheten för civilt försvar och Säkerhetspolisen. Inom forumet finns två arbetsgrupper, varav en för informationsdelning och kommunikation och en för kompetensutveckling och samordning.

I Energiforum har man under 2025 arbetat med att ta fram en svensk version av övningen Cyber Europe, som i grunden arrangeras av EU:s cybersäkerhetsmyndighet Enisa, anpassad specifikt för den svenska energisektorn. NCSC har faciliterat och deltagit i detta arbete, köpt in en övningsplattform från Enisa, samt haft rollen som övningsledare när övningen i september 2025 genomfördes för första gången under namnet Red Juice.

Under 2025 har Energiforum haft tre strategiska möten. Dessa möten är fysiska och roterar mellan medlemsorganisationerna. NCSC bistår med administrationen kring mötena.

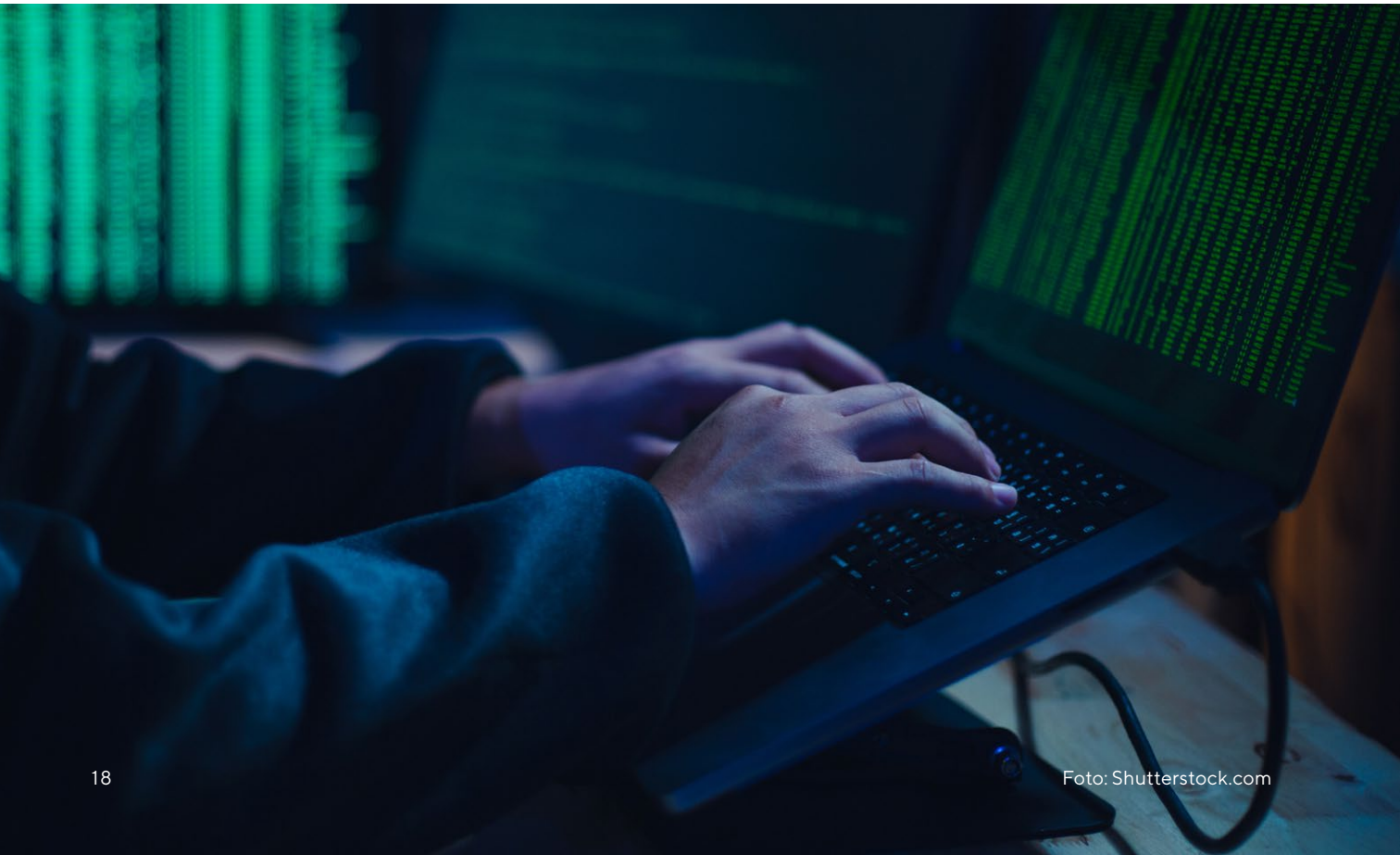

Foto: Shutterstock.com

Bredden i den nationella samverkan

NCSC har under 2025 deltagit i samverkan med transportsektorn inom ramen för Trafikverkets samverkansforum BT POS.[5] NCSC har också deltagit i samverkan med telekomsektorn dels inom ramen för Post- och telestyrelsens forum NTSG[6], dels genom Myndigheten för civilt försvars forum FIDI telekom.[7] I de senare två forumen har NCSC deltagit indirekt via representanter från samverkansmyndigheterna.

NCSC har under året också haft möten med bland annat Integritetsskyddsmyndigheten (IMY), Jordbruksverket, Trafikverket, Myndigheten för psykologiskt försvar (MPF), FOI, eHälsomyndigheten, Sveriges Kommuner och Regioner (SKR), flera länsstyrelser och Malmö stad; med CIO-nätverket för statligt ägda bolag, Riksbanken, eSam, branschorganisationerna Svenskt näringsliv och Säkerhets- och försvarsföretagen (SOFF); samt med Cybercampus, Stöldskyddsföreningen och ett stort antal andra intressenter.

Vidare har NCSC under 2025 deltagit i möten och event arrangerade av bland annat Polismyndigheten, Tullverket, Länsstyrelsen Stockholm, Myndigheten för civilt försvar, Tech Sverige, Totalförsvarets forskningsinstitut (FOI), Cybercampus, Ericsson, Truesec och Palo Alto.

Foto: Johnér Bildbyrå

Cybersäkerhet över gränserna

NCSC har under året påbörjat en utveckling av den internationella samverkan, utifrån uppdraget att vara kontaktpunkt för motsvarande funktioner i andra länder. Chefen för NCSC deltar i nätverket Cyber Security Directors Meeting (CSDM) som träffas cirka två gånger per år. CSDM består av 32 europeiska länder (EU27, EFTA/EES-länderna, Ukraina och Storbritannien) samt Enisa.[8]

Mötet är en plattform för att diskutera aktuella ämnen, samt dela information och kunskap om cybersäkerhet. I februari deltog en representant för NCSC vid CSDM-mötet i München i Tyskland och i oktober deltog chefen för NCSC vid mötet i Haag i Nederländerna.

Bilateral kontakt har genomförts med den ukrainska informationssäkerhetsmyndigheten SSSCIP med samtal om utvecklat samarbete framöver. NCSC har under 2025 också haft utbyte med företrädare för Tysklands och Storbritanniens beskickningar i Stockholm, samt tagit emot ett besök från myndigheter med ansvar för cybersäkerhetsfrågor i Qatar. Chefen för ICANN[9] besökte centret och samtal fördes bland annat om deras utbildningsverksamhet och informationsmaterial. Utbyte har även skett med flera länder inom ramen för årets cybersäkerhetsövningar.

Täta band mellan myndigheter

NCSC har under 2025 samverkat kontinuerligt med samverkansmyndigheterna. Detta sker inom ramen för den löpande verksamheten på NCSC i arbetsgrupperna för samverkan (AG ES), incidentkoordinering (AG IK) och lägesbild (AG LB).

Samverkan sker också vid regelbundna möten med kontaktpunkterna vid respektive myndighet (POC-gruppen), som äger rum varannan vecka. POC-gruppen är ett forum där NCSC och samverkansmyndigheterna samordnar verksamhet och utbyter kunskap, kompetens och information.

Slutligen träffas FRA:s generaldirektör och chefen för NCSC med generaldirektörerna på samverkansmyndigheterna i det strategiska samverkansrådet, ett format som inrättades genom NCSC-förordningen. År 2025 genomfördes det första mötet den 19 september enligt den nya förordningen. Rådet träffas minst två gånger per år.

[5] BT-POS: Beredskap transport privat-offentlig samverkan.
[6] NTSG: Nationella Telesamverkansgruppen.
[7] FIDI Telekom: Forum för informationsdelning avseende cybersäkerhet inom telekomsektorn.
[8] Enisa (European Union Agency for Network and Information Security) är EU:s cybersäkerhetsbyrå.
[9] ICANN, Internet Corporation for Assigned Names and Numbers.

Europaparlamentet i Bryssel
Foto: Shutterstock.com

Samordnat stöd vid cyberangrepp

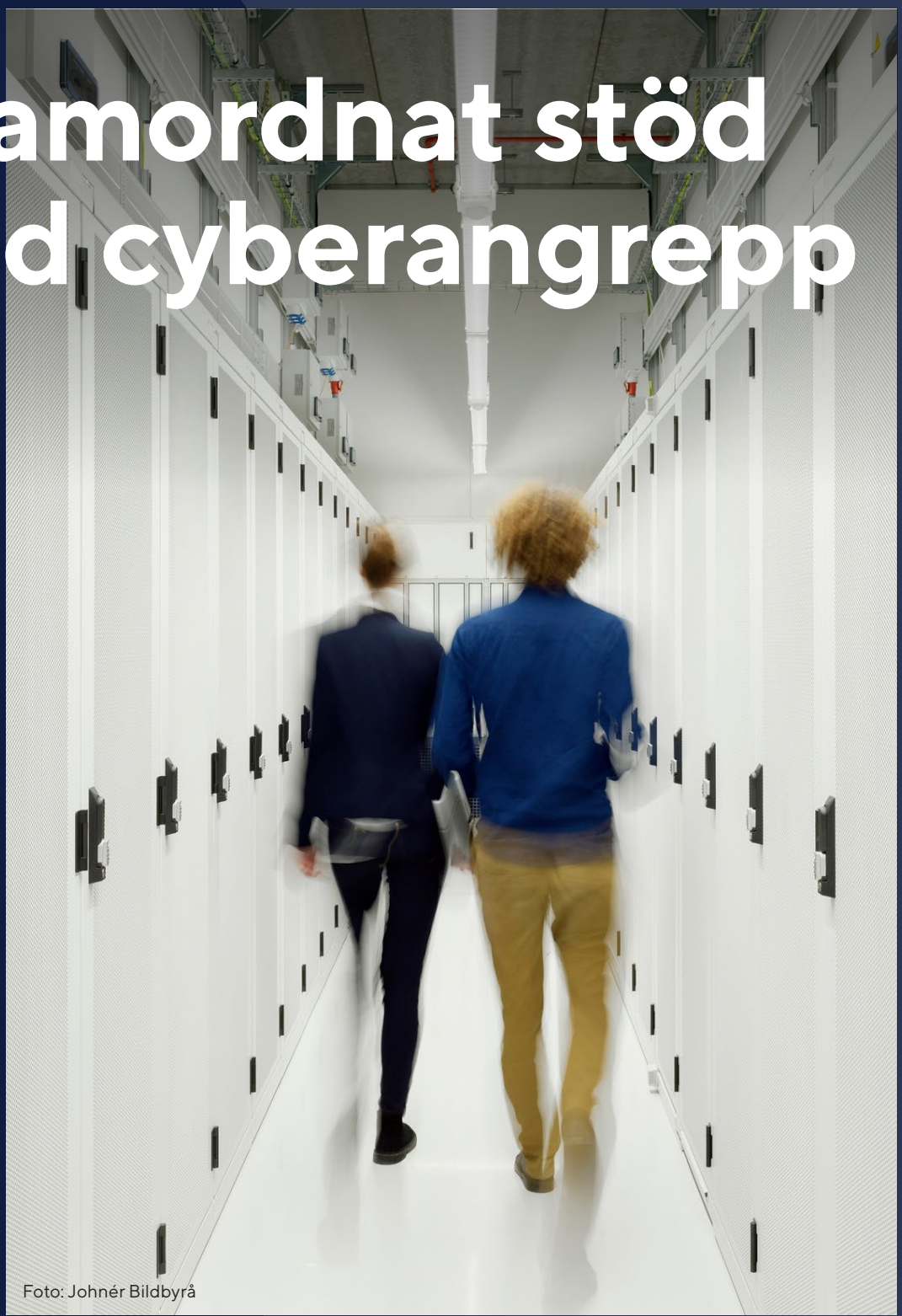

Foto: Johnér Bildbyrå

Rätt aktörer, rätt stöd, rätt tid

Cyberangrepp kräver att rätt aktörer kan agera snabbt, och tillsammans. Inom arbetsgruppen för incidentkoordinering samlas myndigheter med ansvar och operativ förmåga för att skapa en gemensam lägesbild och stödja drabbade verksamheter. Under 2025 aktiverades gruppen vid fem större cybersäkerhetsrelaterade händelser.

Samordning och informationsdelning gällande cybersäkerhetsincidenter sker inom ramen för arbetsgruppen för incidentkoordinering (AG IK). Arbetsgruppen leds av NCSC vid FRA och består i övrigt av representanter från Myndigheten för civilt försvar (med CERT-SE), Försvarsmakten, Polismyndigheten, PTS samt Säkerhetspolisen.

AG IK sammanträder regelbundet enligt rutin, och sammankallas också vid behov när större cybersäkerhetsrelaterade händelser drabbar svenska myndigheter, företag eller andra organisationer.

Syftet med AG IK är att de ingående myndigheterna ska ha en gemensam lägesuppfattning vid cybersäkerhetsrelaterade händelser, och att man i vissa fall ska kunna bistå en drabbad organisation inom ramen för myndigheternas respektive ansvarsområden. Myndigheternas bidrag till arbetsgruppen kan se olika ut beroende på incidentens art och omfattning.

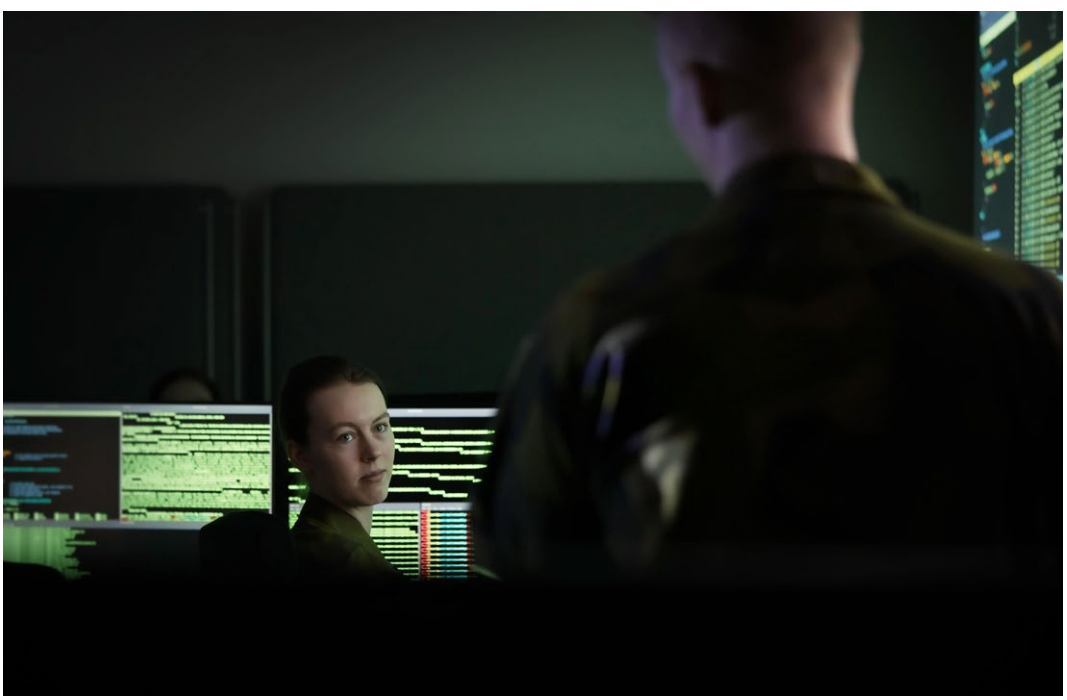

Foto: Försvarsmakten

Under 2025 sammankallades AG IK vid fem cybersäkerhetsrelaterade händelser:

01

Utpressningsangreppet mot Sportadmin i januari, då en stor mängd data och personuppgifter läckte.

02

Överbelastningsangreppet mot SVT i juni, som bland annat ledde till att SVT Play låg nere.

03

Upptäckten av en kritisk sårbarhet i applikationen Microsoft Sharepoint i juni, som innebar att en angripare skulle kunna installera skadlig kod på sårbara servrar. AG IK sammankallades eftersom NCSC bedömde att samhällspåverkan kunde ha blivit omfattande.

04

Utpressningsangreppet mot Miljödata i augusti, som ledde till att en stor mängd personuppgifter läckte. Efter denna incident tog NCSC fram rekommendationer vid intrång och informationsläckage, som publicerades på NCSC:s webbplats.

05

Utpressningsangreppet mot Svenska kraftnät i oktober, som ledde till att en stor mängd personuppgifter läckte.

NCSC och AG IK kunde vid samtliga dessa händelser skapa en god gemensam lägesuppfattning, och i tillämpliga fall understödja den drabbade organisationen med tekniskt stöd och vägledning.

CERT-SE vid Myndigheten för civilt försvar utgör AG IK:s operativa förmåga vid incidentkoordinering. CERT-SE ger löpande råd och/eller tekniskt stöd till drabbade organisationer, och varnar vid behov andra organisationer som potentiellt också löper risk att bli drabbade. FRA ger i vissa fall kvalificerat tekniskt stöd till drabbade organisationer. När CERT-SE överförs från Myndigheten för civilt försvar till FRA den 1 juli 2026, skapas ytterligare förutsättningar för ett förstärkt samarbete inom AG IK och en utökad operativ förmåga.

Foto: Shutterstock.com

Att öva är att förbereda

Foto: Shutterstock.com

Övningar med ett gemensamt mål: stärkt cyberförmåga

Övning bidrar till förmågan att hantera cyberangrepp och incidenter. Övningar är ett av de viktigaste verktygen för att pröva rutiner, stärka samverkan och identifiera svagheter innan de utnyttjas av en angripare. Under 2025 deltog NCSC i nationella och internationella övningar, och tog fram ett nytt övningskoncept för framtiden.

I takt med samhället ökande digitalisering ökar kraven på och behovet av att skydda sig mot cyberangrepp. Övning är viktigt för att utveckla, upprätthålla och pröva förmågan att hantera olika typer av it-säkerhetsincidenter. Utöver verkliga händelser är övningar ett av de bästa verktyg som finns för att förbereda oss för den hotbild som det digitaliserade samhället medför.

NCSC finansierar och stöttar årligen Cyber Challenge, Försvarshögskolans cybersäkerhetstävling för studenter. Tävlingen genomfördes i februari 2025, med 56 deltagare i 14 lag från olika universitet i Sverige. Cyber Challenge fokuserar på policyfrågor och har därmed ett bredare anslag än traditionella cybersäkerhetstävlingar, som ofta har ett tydligt tekniskt fokus. Tävlingen riktar sig därför även till den som inte har en teknisk bakgrund.

I april deltog NCSC tillsammans med Regeringskansliet i en cybersäkerhetsövning i Natos regi. Under övningen testades virtuellt cybersäkerhetsstöd mellan medlemsländerna, det vill säga stöd i hanteringen av en eller flera parallella it-säkerhetsincidenter. Sådant stöd kan till exempel handla om att göra tekniska analyser av data, vilket kan ske virtuellt och alltså utan att det stödjande landet behöver skicka personal till det drabbade landet. Det gemensamma deltagandet syftade till att diskutera nationella rutiner i händelse av att en sådan begäran skulle bli aktuell, oavsett om det skulle handla om att efterfråga eller erbjuda stöd.

Under 2025 bjöd NCSC för tredje året i rad in samverkanspartners och andra relevanta aktörer till MISP-övningar, som genomförs vid FOI:s cyberanläggning i Linköping. MISP (Malware Information Sharing Platform) är en plattform för strukturerad och standardiserad insamling, lagring, analys och delning av information om cyberhot och it-incidenter. Bland annat kan information om hotindikatorer (exempelvis ip-adresser, domäner och skadlig kod) delas, i syfte att göra det lättare att snabbt reagera på nya hot. Syftet med övningarna är bland annat att utveckla förmågan hos teknisk personal i användningen av MISP utifrån olika incidenthanteringsscenarier, samt att skapa förtroende och relationer mellan deltagarna i övningarna.

NCSC:s MISP-övningar har blivit särskilt relevanta i och med att en nationell MISP (MISP-SE) har utvecklats av Myndigheten för civilt försvar och lanserats i början av 2026. Under 2025 bjöd NCSC in kommuner och regioner, statliga myndigheter samt deltagarna i referens- och arbetsgruppen för nationell MISP till de tre övningstillfällena.

Utöver verkliga händelser är övningar ett av de bästa verktyg som finns för att förbereda oss för den hotbild som det digitaliserade samhället medför.

MISP-övningarna har haft stor betydelse för lanseringen av MISP-SE, och bidragit till att höja intresset för samverkan genom informationsdelning.

I december genomfördes Natos flaggskeppsövning Cyber Coalition, som i Sverige samordnas av Försvarsmakten. NCSC deltog i den civila delen av övningen, tillsammans med CERT-SE och samverkansmyndigheterna. Övningen simulerade en redan genomförd verksamhetsgenomgång av cyberverksamhet från Myndigheten för civilt försvar till FRA. Några av målen för övningen var att träna incidenthantering med fokus på effektiv samordning, både internt och mellan aktörer, samt att utveckla arbetet kring informationsdelning om cyberhot. Övningen synliggjorde bland annat behovet av att utveckla en gemensam stabsmetodik efter verksamhetsövergången.

Under 2025 har NCSC tillsammans med övningsexperter från samverkansmyndigheterna och FOI arbetat med att ta fram ett helt nytt koncept för en cybersäkerhetsövning som ska vara både hållbar över tid, sett till omvärldsutvecklingen, och resurseffektiv. Övningskonceptet, som fått namnet Ragnarök, erbjuder både flexibilitet och målgruppsanpassning, och innehåller en metod för hur cybersäkerhetsförmåga kan utvärderas och mätas över tid. Konceptet beskrivs i en FOI-rapport[10] som publicerades i oktober 2025, och är öppet tillgänglig för aktörer i både offentlig och privat sektor att ta inspiration från vid framtagande av egna cybersäkerhetsövningar.

[10] Ragnarök - från kaos till lärande och stärkt cyberförmåga - Övningskoncept för stärkt incidenthanteringsförmåga i samhällsviktig verksamhet, FOI rapport, 2025-09-04.

Foto: Shutterstock.com

Att läsa av läget

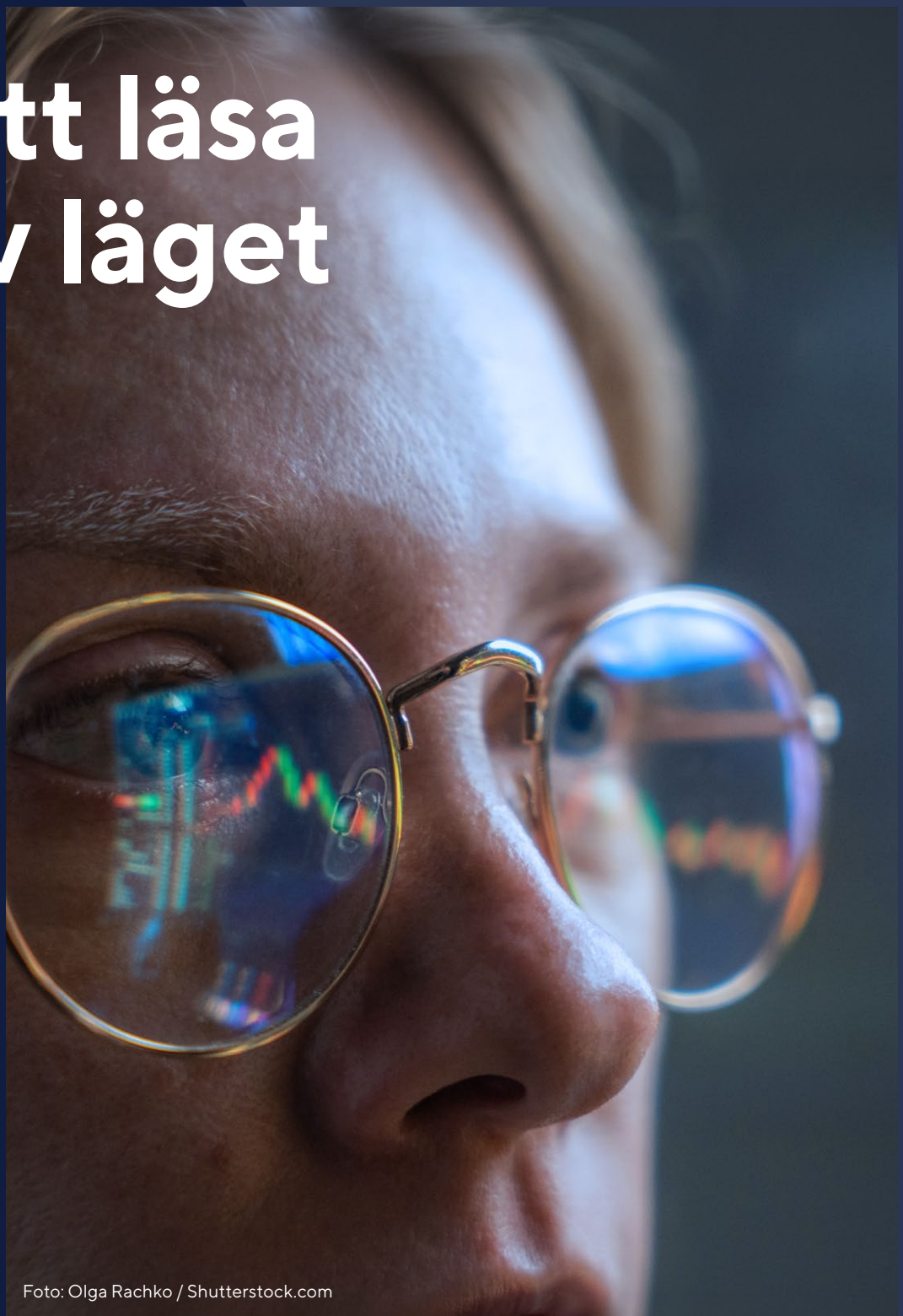

Foto: Olga Rachko / Shutterstock.com

Analyser och en bättre lägesbild

Att förstå hotbilden är en förutsättning för att kunna möta den. NCSC arbetar systematiskt med att samla in, analysera och sprida lägesbilder om cyberangrepp och it-incidenter som drabbar Sverige. Under 2025 har det arbetet fördjupats med månatliga rapporter till regeringen, tematiska analyser och ett nytt format för extern lägesbild under utveckling.

NCSC upprättar varje månad en nulägesrapport, NCSC Nulägesbild. Arbetet med att ta fram nulägesbilden sker i arbetsgrupp lägesbild (AG LB), som leds av NCSC och i övrigt består av representanter från andra delar av FRA, Försvarsmakten, Myndigheten för civilt försvar (med CERT-SE), Polismyndigheten, Post- och telestyrelsen (PTS) och Säkerhetspolisen. Arbetet har under slutet av 2025 förstärkts med deltagande av Myndigheten för psykologiskt försvar.

Nulägesbilden innehåller omvärldsanalys, samt redogör för inflödet av rapporter gällande it-incidenter och it-relaterade händelser under rapporteringsperioden, och analys av dessa. Nulägesbilden redogör också för sårbarheter och angreppsmetoder som uppmärksammats under perioden.

Nulägesbilden fastställs av chefen för NCSC, och delges Regeringskansliet och samverkansmyndigheterna månatligen.

Nulägesbilden föredras sedan mars 2025 också månatligen för Regeringskansliet på både politisk och tjänstemannanivå, detta har under året skett vid sex tillfällen. Vid dessa föredragningar ges mottagarna av rapporterna möjlighet att med NCSC lyfta frågor om specifika händelser, olika företeelser och troliga konsekvenser. Föredragningarna är också ett tillfälle för dialog med Regeringskansliet angående specifik inriktning för nulägesbilden.

Inom ramen för AG LB har under 2025 två tematiska rapporter producerats och publicerats på NCSC:s webbplats, varav den första med titeln Överbelastningsangrepp mot kritisk infrastruktur i Norden, och den andra med titeln Hotaktörers dolda agerande på nätet. Syftet med rapporterna, som bygger bland annat på NCSC:s nulägesbilder, är att uppmärksamma och informera allmänheten om hot, sårbarheter och risker som myndigheterna som deltar i AG LB bedömer vara relevanta och aktuella.

Syftet är att uppmärksamma och informera allmänheten om hot, sårbarheter och risker som myndigheterna bedömer vara relevanta och aktuella.

Ny extern lägesbild för cyberhot och risker

I NCSC:s uppdrag ingår att ta fram samlade lägesbilder till NCSC:s externa målgrupper. Syftet med sådana lägesbilder är att bidra till en ökad medvetenhet och kunskap om aktuella cyberhot och it-händelser hos privata och offentliga organisationer i Sverige.

Under 2025 har NCSC gjort ett större arbete med att ta fram ett koncept för en ny, extern lägesbildsleverans. Konceptet som arbetet mynnat ut i är en webbaserad analysprodukt för beslutsfattare och praktiker med vägledning kring aktuella hot och risker på cybersäkerhetsområdet. Innehållet ska vara varierat och lättbegripligt, och formatet göra det lätt att dela produkten uppåt och neråt i organisationen. Den externa lägesbilden ska innehålla grundläggande information, vägleda till fördjupning på NCSC:s webbplats eller andra ställen, och rekommendera åtgärder.

En första leverans av den externa lägesbilden planeras till första halvan av 2026.

Analys med en längre horisont

Under 2025 har NCSC också påbörjat ett arbete med att utveckla förmågan till strategisk analys och rapportering på cybersäkerhetsområdet. Arbetet har fokuserat på att etablera arbetsprocesser och utveckla relevanta metoder, exempelvis för strukturerad omvärldsbevakning. Ett antal teman som bedöms vara relevanta för att stärka cybersäkerheten i samhället, och/eller analysera trender och fenomen inom cybersäkerhetsområdet, har identifierats som kan vara aktuella för framtida rapportering.

Foto: Jacob Sjöman Svensson / Folio

Cybersäkerhet som samhällsfråga

Foto: Jens Reiterer

Närvaro, dialog och kunskapsspridning

Cybersäkerhet är en samhällsfråga och den behöver diskuteras i offentligheten. Under 2025 har NCSC aktivt sökt sig ut: till Almedalen, till konferenser, till medier och till digitala kanaler. Syftet är att höja kunskapen, stärka förtroendet och tydliggöra centrets roll som nationellt nav för cybersäkerhet.

Under 2025 har NCSC bedrivit ett målinriktat arbete för att öka kunskapen om cybersäkerhet, stärka samverkan mellan samhällsaktörer och tydliggöra centrets roll som nationellt nav för cybersäkerhet. Insatserna har riktats till såväl beslutsfattare och professionella aktörer som till en bredare offentlighet.

NCSC har under året haft en aktiv närvaro i såväl medier som i externa sammanhang. Medierapporteringen har bland annat omfattat presskonferens tillsammans med Regeringskansliet i samband med tillträdet av ny centerchef samt intervjuer i rikstäckande media, däribland Sveriges Radio och TT. Sammantaget har detta bidragit till ökad kännedom om centret och dess uppdrag.

Parallellt har centret bedrivit en aktiv extern verksamhet med inriktning på dialog och kunskapsspridning. Fokus har bland annat varit att informera om NCSC:s roll, ansvar och prioriteringar. Centret har medverkat vid ett flertal konferenser och evenemang, däribland Kvalitetsmässan, Säkerhetsgalan, E-förvaltningsdagarna, FOI:s It-försvarsdag och It i vården-dagen.

Efterfrågan på centrets medverkan i externa sammanhang har fortsatt att öka.

Under året mottogs totalt 95 externa förfrågningar i form av talaruppdrag, mötesinbjudningar och intervjuförfrågningar, varav 52 kunde genomföras med befintliga resurser. Efter centerchefens tillträde i september ökade intresset ytterligare. Under årets sista fyra månader genomfördes fem externa möten, åtta externa presentationer, tre intervjuer samt en podcastinspelning.

Almedalsveckan 2025 – cybersäkerhet som samhällsfråga

NCSC:s medverkan i Almedalsveckan 2025 var ett viktigt led i arbetet med att etablera cybersäkerhet som en självklar del av den bredare samhälls- och säkerhetspolitiska diskussionen. Genom deltagande i sex panelsamtal bidrog centret med perspektiv baserade på operativ erfarenhet, analys och samlad kunskap från nationellt cybersäkerhetsarbete.

Under samtalen lyftes cybersäkerhet som en förutsättning för digital resiliens, totalförsvar och skydd av samhällsviktig verksamhet. Närvaron i Almedalen visade tydligt att cybersäkerhet kan inte längre betraktas som en isolerad teknikfråga, utan måste ses som en grundläggande del av samhällets motståndskraft och förmåga att hantera kriser och antagonistiska hot.

Cybersäkerhet kan inte längre betraktas som en isolerad teknikfråga, utan måste ses som en grundläggande del av samhällets motståndskraft och förmåga att hantera kriser och antagonistiska hot.

Kunskapsspridning genom digitala kanaler

Som en del av den löpande verksamheten har NCSC under året använt digitala kanaler för att kontinuerligt dela kunskap, analyser och rekommendationer. Den huvudsakliga kanalen är NCSC:s webbplats, ncsc.se. Under slutet av 2025 hade NCSC drygt 13 000 följare på LinkedIn, vilket speglar ett växande intresse för centrets arbete och de kunskapsunderlag som delas.

Tillsammans har de digitala kanalerna använts för att sprida information om aktuella hot, publicerade rapporter, uppdaterade rekommendationer samt deltagande i övningar, konferenser och samverkansforum. En ökad räckvidd har stärkt våra möjligheter att snabbt nå ut med relevant information vid förändringar i hotbilden.

Cybersäkerhetskonferensen — nationell plattform för samverkan

NCSC:s årliga cybersäkerhetskonferens arrangerades 2025 tillsammans med Myndigheten för civilt försvar. Konferensen samlade aktörer från myndigheter, näringsliv, akademi och internationella samarbetspartners och skapade förutsättningar för dialog kring både strategiska och operativa cybersäkerhetsfrågor. Över 1 000 personer deltog på plats i Stockholm, och ytterligare flera tusen deltog digitalt. Detta gör konferensen till en av Sveriges största mötesplatser inom cybersäkerhet. Årets konferens fokuserade särskilt på cybersäkerhet, NIS 2-direktivet och aktuell lagstiftning, resiliens, teknikfördjupning, samt på forskning och innovation.

Genom konferensen bidrog NCSC till att fördjupa förståelsen för hotutvecklingen, diskutera konsekvenser av nya regelverk och dela erfarenheter från inträffade cyberincidenter. Konferensen stärkte även vår roll som en samlande aktör och bidrog till att bygga långsiktiga relationer som är viktiga för samverkan vid framtida händelser.

Publikationer och uppdaterade rekommendationer

Under 2025 har NCSC publicerat rapporter och analyser som belyser aktuella cyberhot, hotaktörers metoder och sårbarheter i digital infrastruktur. Publikationerna syftar till att ge både strategiskt och operativt stöd till aktörer med ansvar för cybersäkerhet.

NCSC har även löpande uppdaterat och kommunicerat rekommendationer för hur organisationer kan stärka sin cybersäkerhet, bland annat avseende skydd mot överbelastningsangrepp och hantering av äldre eller sårbara system. Genom att kombinera analys med konkreta råd bidrar NCSC till att omsätta hotinformation till genomförbara åtgärder.

Björn Lyrvall, generaldirektör FRA och Mikael Frisell, generaldirektör Myndigheten för civilt försvar.

Foto: Jens Reiterer

Regeringsuppdrag och strategiska aktiviteter

Foto: Trygve Finkelsen / Shutterstock.com

Särskilda uppdrag för cybersäkerhetscentret

NCSC:s uppdrag sträcker sig bortom den löpande verksamheten. Under 2025 tog centret emot fyra separata regeringsuppdrag. Arbetet spänner över lagstiftning, strategi och beredskap, och visar bredden i NCSC:s verksamhet.

Den 27 februari 2025 fick FRA och Myndigheten för civilt försvar i uppdrag av regeringen att ta fram riktlinjer i enlighet med NIS 2-direktivets[11] artikel 7.2.[12] Artikel 7 beskriver NIS 2-direktivets krav på respektive EU-medlemsstats nationella cybersäkerhetsstrategi. Enligt artikel 7.2 ska medlemsstaterna, som en del av den nationella strategin för cybersäkerhet, anta ett antal riktlinjer. Arbetet ska slutredovisas i slutet av 2026.

En grundplatta för framtida cyberkrishantering

Enligt NIS 2-direktivet ska alla EU-länder anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och cyberkriser (cyberkrishanteringsplanen). Mot denna bakgrund gav regeringen den 27 februari 2025 FRA i uppdrag att utarbeta en sådan plan.[13] FRA genom NCSC redovisade planen och regeringsuppdraget för Regeringskansliet (Försvarsdepartementet) i december 2025.

Cyberkrishanteringsplanen har utformats för att kunna utgöra en grundplatta för fortsatt utveckling av det nationella cyberkrishanteringsarbetet i samarbete med företag, myndigheter och andra intressenter. Planen kommer att operationaliseras med dessa aktörer och även justeras under 2026 med anledning av de förändrade ansvarsförhållanden på cyberområdet i Sverige.

Mätning av den nationella cybersäkerhetsstrategins mål

Den 23 oktober 2025 fick FRA genom NCSC i uppdrag av regeringen att ta fram mätmetoder för och genomföra en första mätning av de 13 resultatindikatorer som anges i Nationell strategi för cybersäkerhet 2025–2029.[14]

Arbetet med uppdraget har skett i projektform, med ledning av och medarbetare från NCSC och övriga FRA, samt med stöd av Försvarsmakten och Myndigheten för civilt försvar. Samråd har också skett med samverkansmyndigheterna. Under 2025 har arbetet bestått av analys av resultatindikatorerna; avstämning med Regeringskansliet bland annat kring behov av definitioner och avgränsningar rörande enskilda indikatorer; kartläggning av relevanta datakällor; samt mejlkontakt och dialog eller möten med ett stort antal organisationer och myndigheter med förfrågningar om information.

Uppdraget redovisades till Regeringskansliet (Försvarsdepartementet) i mars 2026.

Cybersäkerhet som förutsättning för demokratin

Den 20 november 2025 fick FRA genom NCSC i uppdrag av regeringen att delta i det myndighetsgemensamma arbetet och stödja relevanta aktörer i frågor om cybersäkerhet inför, under och efter genomförandet av valen till riksdag, region- och kommunfullmäktige 2026.[15]

På förfrågan av Valmyndigheten har NCSC tagit rollen som ansvarig och sammankallande för arbetsgruppen för cybersäkerhet (AG Cybersäkerhet) inom ramen för det av Valmyndigheten inrättade Nationellt valnätverk. NCSC deltar också med representanter i de övriga tre arbetsgrupperna i valnätverket, AG Operativ samordning, AG Omvärld och hotanalys, samt AG Kommunikationssamordning.

NCSC:s uppgift som sammankallande för arbetsgruppen är att planera, samordna, samverka, koordinera och ansvarsfördela arbetet med att sammanställa lägesbilder och hotbilder, göra riskanalyser och föreslå riskreducerande åtgärder, bland annat baserat på erfarenheter från tidigare val i Europa; samt att arrangera workshops och övningar, och etablera gemensamma rutiner för incidentkoordinering, informationsdelning och krishantering.

AG Cybersäkerhet hade ett uppstartsmöte den 25 november med deltagare från FRA, Försvarsmakten, Myndigheten för civilt försvar, MPF, Polismyndigheten, PTS, Skatteverket, Säkerhetspolisen och Valmyndigheten. Under 2025 inleddes planeringsfasen av uppdraget, som fortsätter med vidare förberedelser, genomförande och utvärdering under 2026.

Uppdraget ska slutredovisas till Regeringskansliet (Försvarsdepartementet) i december 2026.

[11] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen.
[12] Uppdrag till Försvarets radioanstalt och Myndigheten för samhällsskydd och beredskap att ta fram riktlinjer i enlighet med artikel 7.2 i NIS 2-direktivet (Fö2025/00389), 2025-02-27.
[13] Uppdrag till Försvarets radioanstalt (FRA) att utarbeta en nationell operativ plan för hanteringen av storskaliga cybersäkerhets-incidenter och kriser (Fö2025/00388), 2025-02-27.
[14] Uppdrag till Försvarets radioanstalt genom det nationella cybersäkerhetscentret att genomföra mätning av resultatindikatorer (Fö2025/01547), 2025-10-23.
[15] Uppdrag till Försvarets radioanstalt genom det nationella cybersäkerhetscentret att stödja cybersäkerhetsarbetet inför, under och efter valen till riksdag, region- och kommunfullmäktige 2026 (Fö2025/01712) 2025-11-20.

Foto: Johnér Bildbyrå

Genomförande av den nationella cybersäkerhetsstrategin

NCSC och samverkansmyndigheterna ansvarar för ett brett spektrum av aktiviteter i den nationella strategins handlingsplan, från riktlinjer och standardisering till övningar och informationsdelning. Här redovisas det arbete som genomförts under 2025.

I aktivitetsplanen kopplad till den nationella cybersäkerhetsstrategin[16] finns ett antal aktiviteter som har relevans för NCSC eller anger NCSC tillsammans med samverkansmyndigheter som ansvariga genomförare. Nedan redovisas aktiviteterna och den verksamhet som utförts av NCSC och dess samverkansmyndigheter. Flera aktiviteter finns beskrivna i andra delar av föreliggande redovisning.

[16] En ny era av cybersäkerhet – Nationell strategi för cybersäkerhet 2025–2029 (Skr. 2024/25:121).

Pelare A, mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer

Mål	Beskrivning	Ansvarig(a) utförare	Utförda aktiviteter av NCSC & samverkansmyndigheterna
1:5	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att främja utveckling och integrering av relevant avancerad teknik som syftar till att genomföra moderna riskhanteringsåtgärder för cybersäkerhet, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) – j) kräver.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 39–40

Pelare A, mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering

Mål	Beskrivning	Ansvarig(a) utförare	Utförda aktiviteter av NCSC & samverkansmyndigheterna
2:4	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) – j) anger att medlemsstaterna ska anta.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 39–40

Pelare A, mål 3: Stärkt säkerhetsarbete inom kritisk infrastruktur

Mål	Beskrivning	Ansvarig(a) utförare	Utförda aktiviteter av NCSC & samverkansmyndigheterna
3:2	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att upprätthålla den allmänna tillgängligheten, integriteten och konfidentialiteten hos den offentliga kärnan i det öppna internet, inbegripet, i tillämpliga fall, cybersäkerheten hos undervattenskablar, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) – j) anger att medlemsstaterna ska anta.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 39–40

Pelare A, mål 4: Robustare digitala leveranskedjor och minskat beroende

Mål	Beskrivning	Ansvarig(a) utförare	Utförda aktiviteter av NCSC & samverkansmyndigheterna
4:1	Berörda statliga myndigheter fortsätter inom ramen för etablerad NCSC-samordning kring standardisering av cybersäkerhet.	FRA och MSB i samverkan med FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen.	Under 2025 har NCSC:s arbetsgrupp för standardiseringsfrågor hållit tre möten. Exempel på aktuella frågor som representaterna för de samverkande myndigheterna diskuterat är arbetet i CEN[17] och ETSI[18] med att ta fram harmoniserade standarder under cyberresiliens-förordningen (CRA), standardiseringen av 6G samt utvecklingen inom post-quantum kryptografi.
4:4	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av entiteter när de tillhandahåller sina tjänster, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) – j) anger att medlemsstaterna ska anta.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 39–40

Pelare A, mål 5: Förenklad regelefterlevnad och stärkt funktionellt tillsynsarbete

Mål	Beskrivning	Ansvarig(a) utförare	Utförda aktiviteter av NCSC & samverkansmyndigheterna
5:2	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, Försvarsmakten, MSB, Säkerhetspolisen och FMV.	Arbetsgrupp (AGNM) med berörda myndigheter har under året haft över 20 möten. Gruppen har: • kartlagt myndigheternas intressenter, • identifierat dokument med stöd och råd som myndigheterna redan utvecklat och som kan påverka eller påverkas av en Nationell Modell med tillhörande Norm, • analys av svenska och internationella regelverk och standarder med relevans för de ingående myndigheterna och deras intressenter (totalt har ca 25 regelverk analyserats), • utvecklat utkast för de olika delar som bör ingå i normen.

[17] CEN, European Committee for Standardisation.
[18] ETSI, European Telecommunications Standards Institute.

Pelare A, mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete

Mål	Beskrivning	Ansvarig(a) utförare	Utförda aktiviteter av NCSC & samverkansmyndigheterna
6:1	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.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 39–40

Pelare B, mål 8: Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet

Mål	Beskrivning	Ansvarig(a) utförare	Utförda aktiviteter av NCSC & samverkansmyndigheterna
8:5	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.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 39–40

Pelare C, mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt

Mål	Beskrivning	Ansvarig(a) utförare	Utförda aktiviteter av NCSC & samverkansmyndigheterna
11:1	FRA ska inom ramen för NCSC främja samverkan med privata och offentliga aktörer.	FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 17–18
11:2	NCSC tar fram lägesbilder avseende cyberhot och incidenter.	FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 31–32
11:3	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer inbegripet relevanta förfaranden och lämpliga verktyg för informationsutbyte för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan entiteter i enlighet med unionsrätten, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) – j) kräver.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 39–40
11:4	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter enligt NIS 2-direktivets artikel 12.1, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) – j) kräver.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 39–40
11:5	Berörda statliga myndigheter fortsätter att inom ramen för årsrapporter informera om hotbilden inom sina respektive sakområden.	FRA, Försvarsmakten, MSB, Säkerhetspolisen, Polismyndigheten, FMV och PTS.	Se sidan 31–32

Pelare C, mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter

Mål	Beskrivning	Ansvarig(a) utförare	Utförda aktiviteter av NCSC & samverkansmyndigheterna
12:2	Nationell informations-säkerhetsövning (NISÖ) fortsätter att genomföras inom ramen för NCSC.	MSB i samverkan med berörda aktörer	Se sidan 17–18
12:3	Statliga myndigheter genomför inom ramen för NCSC nationella cybersäkerhetsövningar.	FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 31–32
12:7	FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att främja ett aktivt cyberskydd, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) – j) kräver.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 39–40
12:10	FRA ska utarbeta en nationell operativ plan för storskaliga cybersäkerhetsincidenter och kriser i enlighet med artikel 9 i NIS 2-direktivet.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen.	Se sidan 39–40

NATIONELLT
CYBERSÄKERHETSCENTER
En del av FRA

ncsc.se