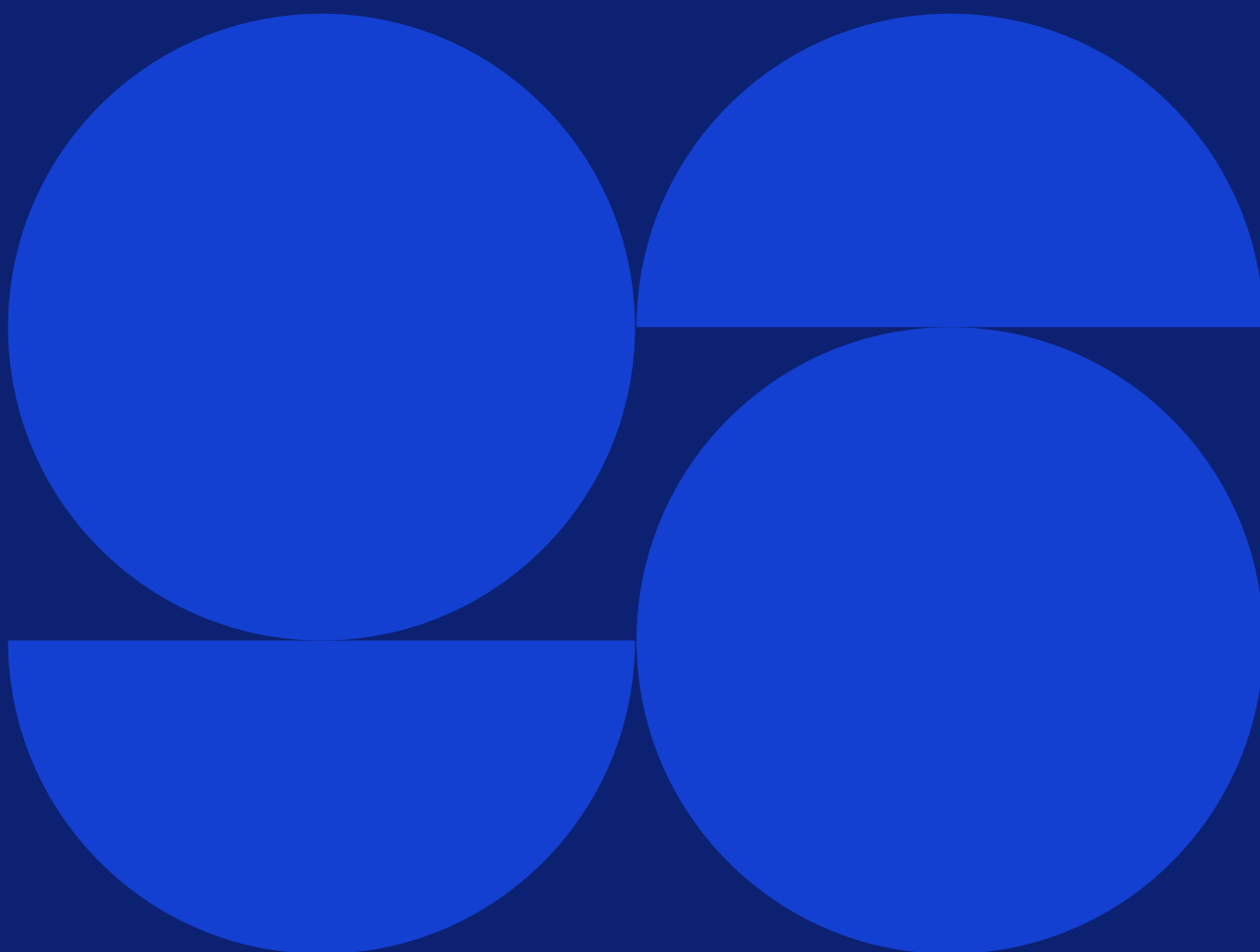


Riktlinjer för att utveckla, förbättra och främja användningen av cybersäkerhetsverktyg och säker nätinfrastruktur





Riktlinjer för att utveckla, förbättra och främja användningen av cybersäkerhetsverktyg och säker nätinфраstruktur

1 Bakgrund, syfte och målgrupp

Dessa riktlinjer syftar till att vägleda och ge stöd till lärosäten, forskningsinstitut och forskningsfinansiärer att utveckla, förbättra och främja användningen av cybersäkerhetsverktyg och säker nätinфраstruktur.

Vetenskapsrådet har, i enlighet med regleringsbrev för 2025 (U2025/01357) och i samverkan med berörda aktörer, utarbetat dessa riktlinjer.

Riktlinjerna har sin grund i direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS 2-direktivet).¹ Av direktivet framgår att varje medlemsstat ska ta fram en nationell cybersäkerhetsstrategi och riktlinjer inom tio policyområden.²

Dessa riktlinjer utgör ett av de tio policyområdena och bygger på Sveriges nationella cybersäkerhetsstrategi³. De övriga policyområdena är följande:

- aktivt cyberskydd,
- cyberresiliens och cyberhygien,
- sårbarhetshantering,
- utbildning och forskning,
- digitala leveranskedjor,

¹ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

² Se artikel 7 i NIS 2-direktivet.

³ Nationell cybersäkerhetsstrategi 2025-2029, regeringens skrivelse 2024/25:121.



- säker upphandling,
- det öppna internet,
- ny cybersäkerhetsteknologi och
- säker informationsdelning.

Myndigheten för civilt försvar (MCF) och Försvarets radioanstalt (FRA) har inom ramen för det Nationella cybersäkerhetscentret (NCSC) fått i uppdrag att ta fram riktlinjer inom dessa nio policyområden.

Den nationella cybersäkerhetsstrategin tillsammans med de tio nationella riktlinjerna syftar till att stärka Sveriges cybersäkerhetsförmåga inom centrala cybersäkerhetsområden.

Dessa riktlinjer ersätter inte EU-rättsliga krav eller nationella lagar, förordningar och föreskrifter inom cybersäkerhetsområdet utan avser att vägleda och ge stöd till lärosäten, forskningsinstitut och forskningsfinansiärer i arbetet med att utveckla, förbättra och främja användningen av cybersäkerhetsverktyg och säker nätinфраstruktur.

I dessa riktlinjer har begreppen cybersäkerhetsverktyg och nätinфраstruktur samma innebörd som säkerhetsåtgärder respektive nätverks- och informationssystem.

Målgruppen för riktlinjerna är de svenska lärosätena, forskningsinstituten och forskningsfinansiärerna. Den primära målgruppen hos lärosätena och forskningsinstituten är funktioner inom ledning och styrning, expertfunktioner inom cybersäkerhet samt forskningsledare hos lärosäten och forskningsinstitut. Den primära målgruppen hos forskningsfinansiärerna är funktioner inom ledning och styrning.

2 Nuläget och nulägesanalys

2.1 Användningen av cybersäkerhetsverktyg och säker nätinфраstruktur inom forskningssektorn

Flera rapporter pekar på att cybersäkerheten behöver höjas, inte minst hos de svenska lärosätena som bedriver forskning⁴. Detta innebär att lärosätena behöver öka sin cybersäkerhetsförmåga. Universitet och högskolor behöver arbeta systematiskt med frågor relaterade till cybersäkerhet för att förhindra såväl antagonistiska som icke-antagonistiska incidenter. En central del i detta arbete att utveckla användningen av ändamålsenliga och effektiva cybersäkerhetsverktyg och säkra nätinфраstrukturer.

I dag präglas användningen av cybersäkerhetsverktyg inom lärosätena och forskningsinstituten av en fragmenterad flora av verktyg som är anpassade till

⁴ Säkerhetspolisen konstaterar i sin årsrapport 2025/2026 att svensk forskning och innovation är eftertraktad och därmed är ett attraktivt mål för främmande makt. I Riksrevisionens rapport, RiR 2023:20, Informationssäkerhet vid universitet och högskolor – hanteringen av skyddsvärda forskningsdata, lämnar revisionen kritik i hanteringen av forskningsdata.



många olika system och som är svåra att integrera och samordna. Vilka verktyg som används styrs av beställarkrav och externa krav som i praktiken utgör en miniminivå, snarare än incitament för proaktiv utveckling. Vilket it-stöd som används styrs även av externa samarbeten, vilket medför svårigheter att få en överblick av den faktiska IT-miljön. Vidare präglas användningen av höga kostnader för kommersiella lösningar, vilket hämmar experimenterande, innovation och lokal anpassning.

Vetenskapsrådet ansvarar för kommunikationssystemet Swedish University Computer Network (Sunet) och tillhandahåller anslutning åt organisationer inom högre utbildning. Något motsvarande finns inte för forskningsinstitut som inte är lärosäten.

Inom forskningssektorn finns ett växande intresse för verktyg i egen regi, särskilt kopplat till säker kommunikation, datadelning och identitetshantering, men även för användning av öppen källkod och ny teknik, men ofta saknas långsiktiga resurser för förvaltning och vidareutveckling. Det finns även behov av långsiktighet i utveckling och förvaltning av säkra infrastrukturer, där säkra behandlingsmiljöer lyfts som ett utvecklingsområde.

Forskningssektorn ser tydliga trender med AI-baserade cybersäkerhetsverktyg. Forskningssektorn ser även ett ökat fokus på säkerhet, kommunikation, identitet och tillitsramverk, samt ett ökat behov av skalbara, gemensamma lösningar snarare än lokala punktinsatser.

Det sker satsningar på cybersäkerhet inom forskningssektorn och det finns ändamålsenlig teknik, men det råder stor osäkerhet kring regelefterlevnad exempelvis avseende dataskydd, sekretess, säkerhetsskydd och cybersäkerhet. Osäkerheten hämmar användningen. Vissa satsningar upplevs även som skilda från den praktiska användningen i verksamheten och är svåra att omsätta i konkreta verktyg eller operativa lösningar.

Mot bakgrund av det försämrade säkerhetsläget ser lärosätena och forskningsinstituten även ett behov av ökad rådighet över digitala lösningar. Fler cybersäkerhetsverktyg utvecklas med öppen källkod och fler tjänster och produkter utvecklas på såväl den svenska som den europeiska marknaden, men långsiktighet och incitament krävs för att de ska kunna sättas i praktisk drift. Tröskeln för att använda nya verktyg är i flera fall hög, och det erfordras insatser för att avhjälpa brister och fortsätta utvecklingen.

För att möjliggöra en högre nivå av cybersäkerhet lyfter sektorn att cybersäkerhetsfrågorna behöver få större tyngd i verksamheterna och i större utsträckning betraktas som en verksamhetskritisk förutsättning.

Det finns former för kunskapsdelning och erfarenhetsutbyte, bland annat genom nationella samverkansforum och informationsinsatser som nyhetsbrev, utbildningar och övningar, men lärosätena och forskningsinstituten efterfrågar ökad samordning, såsom bland annat strukturer för systematisk erfarenhetsåterföring och gemensam utveckling och vidareförvaltning av nätverks- och informationssystem och säkerhetsåtgärder.



2.2 Forskning och utveckling av cybersäkerhetsverktyg och säker nätinфраstruktur

Traditionen av nära samarbete mellan staten, lärosäten och industri finns inom cybersäkerhetsområdet. Cybersäkerhetsforskning bedrivs vid flertalet universitet, högskolor och forskningsinstitut vilka finansieras av såväl statliga som privata forskningsfinansiärer. Sverige har starka forskargrupper inom några av cybersäkerhetsforskningens områden men forskningen är begränsad och inriktad på ett fåtal områden, vilket medför att den sällan bedrivs tvärvetenskapligt. Forskningslandskapet arbetar även till stor del avskilt från varandra och koordinering inom cybersäkerhetsforskningen har ofta saknats, vilket medför att det saknas en gemensam bild.

Insatser har gjorts för att underlätta samarbete mellan näringsliv och akademi i syfte att främja kunskapsutveckling och att överbrygga eventuella gap till marknad, bland annat genom Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE), Cybernoden, Cybercampus Sverige och Sweden Secure Tech Hub, men mer arbete kvarstår. Det efterfrågas mer samverkan mellan forskningen, kommersialisering och tillämpningen för att hitta behovsstyrda och gemensamma nätverks- och informationssystem och säkerhetsåtgärder som kan införas i praktisk drift.

Sverige har flera forskningsfinansiärer inom cybersäkerhetsområdet, såväl offentliga finansiärer som Myndigheten för civilt försvar, Vetenskapsrådet och Formas och som privata finansiärer, däribland Knut och Alice Wallenbergs Stiftelse. Dessa aktörer samverkar i begränsad omfattning kring finansieringen av cybersäkerhetsforskning. Sektorn efterfrågar ökad samordning och samverkan dels mellan forskningsfinansiärerna, dels mellan forskningsfinansiärerna och andra aktörer som fördelar medel, såsom exempelvis Verket för innovationssystem (Vinnova) och Tillväxtverket.

3 Målbild för 2029

3.1 Användningen av cybersäkerhetsverktyg och säker nätinфраstruktur inom forskningssektorn

Lärosätena och forskningsinstituten har fungerande processer som hanterar cybersäkerhet från utveckling till förvaltning och cybersäkerhetsarbetet utgår ifrån ett allriskperspektiv. Cybersäkerheten ses i större utsträckning som en integrerad del i forskningsverksamheten och som en verksamhetskritisk förutsättning.

Lärosätena och forskningsinstituten arbetar i större utsträckning tvärfunktionellt och tillsammans med andra aktörer för att främja och utveckla användningen av ändamålsenliga och säkra digitala lösningar.

Lärosätenas och forskningsinstitutens användning av cybersäkerhetsverktyg och säker nätinфраstruktur ökar, är mer behovsstyrt och sker med ökad långsiktighet, inbyggd flexibilitet och med ökad rådighet över användningen. Som ett led i denna utveckling främjas användningen av cybersäkerhetsverktyg med öppen källkod



med tydliga applikationsprogrammeringsgränssnitt (API) eller andra lösningar som syftar till att öka rådigheten. Utvecklingen och användningen av säker kommunikation sker med bästa praxis, såsom stark autentisering och med automatiserad och säker certifikathantering. Lärosätena och forskningsinstituten hanterar behovet av verktygsstöd för cybersäkerhetsarbetet och arbete sker i större omfattning automatiserat.

Utvecklingen av säkra behandlingsmiljöer för forskning fortsätter och anpassas efter behov och riskbild. Säkra behandlingsmiljöer med olika säkerhetsnivåer har etablerats och fler lärosäten och forskargrupper har anslutit sig till eller tagit sådana miljöer i drift. Forskningen och olika forsknings- och utvecklingssamarbeten sker i större utsträckning i säkra behandlingsmiljöer.

Genom samverkan finner lärosätena, forskningsinstituten och forskningsinfrastrukturerna synergier för att främja och utveckla användningen av cybersäkerhetsverktyg och säker nätinфраstruktur. Genom samverkan finner aktörerna även gemensamma digitala lösningar utifrån gemensamma behov när det är lämpligt.

3.2 Forskning och utveckling av cybersäkerhetsverktyg och säker nätinфраstruktur

Lärosätena, forskningsinstituten och forskningsfinansiärerna bidrar till att främja forskning och utveckling av effektiva och ändamålsenliga cybersäkerhetsverktyg och säkra nätinфраstrukturer.

Forskningen och utvecklingen av cybersäkerhetsverktyg och säkra nätinфраstrukturer styrs av både nyfikenhet och behov i syfte att finna svar och lösningar som stärker verksamhetens förmåga att förebygga och hantera såväl antagonistiska som icke-antagonistiska hot. Arbetet bedrivs i större utsträckning med en tvärvetenskaplig ansats där olika förmågor, kunskaper och erfarenheter sammanlänkas. Olika forskningsnät används mer experimentellt för forskning, och nya samarbetsytter etableras.

Gapet mellan grundforskning, innovation och praktisk tillämpning av cybersäkerhetsverktyg har minskat och arbetet utgår i större utsträckning från behov och problembild. Utvecklingen bidrar till ökad koordinering av cybersäkerhetsforskning och innovation och till bättre förutsättningar för att utveckla användningen av cybersäkerhetsverktyg och säkra nätinфраstrukturer.

Forskningsfinansiärerna samverkar och samordnar sitt arbete för att skapa en gemensam nulägesbild och analys för åtgärder för att främja cybersäkerhetsforskning men även för att stärka cybersäkerhetsförmågan i forskningsprojekt som får medel. Samverkan sker även med andra finansiärer, såsom finansiärer inom innovation och andra utvecklingsinsatser.



4 Åtgärder för att nå målbilden

4.1 Användningen av cybersäkerhetsverktyg och säker nätinfrastruktur inom forskningssektorn

Följande rekommendationer riktas till forskningsfinansiärerna i syfte att främja användningen av cybersäkerhetsverktyg och säker nätinfrastruktur:

1. Vidta åtgärder för att främja att aspekter som rör cybersäkerhet uppmärksammas vid finansiering av forskning samt följ upp effekten av åtgärden utifrån målbilden.

Sådana åtgärder kan till exempel vara att ställa upp villkor för att erhålla medel, att upplysa om vikten av adekvat cybersäkerhet för hantering av forskningsdata, att inkludera aspekter som rör cybersäkerhet i vägledningar, datahanteringsplaner, informationsinsatser, rapporter eller liknande, samt att följa upp aspekter som rör cybersäkerhet inom det som finansieras. Åtgärder och uppföljning av åtgärder är ett område som kan vara föremål för samverkan, se rekommendation 4.

Följande rekommendationer riktas till lärosätena och forskningsinstituten i syfte att främja användningen av cybersäkerhetsverktyg och säker nätinfrastruktur:

2. Utveckla det interna cybersäkerhetsarbetet i syfte att stärka användningen av ändamålsenliga cybersäkerhetsverktyg och säkra nätinfrastrukturer genom att:
 - a. etablera eller utveckla interna samarbeten utifrån lokala förutsättningar mellan olika funktioner och kompetensområden, särskilt mellan medarbetare inom IT, säkerhet, juridik, arkiv och forskare i såväl utveckling som förvaltning av cybersäkerhetsverktyg och säker nätinfrastruktur, samt följa upp effekten utifrån målbilden.
 - b. genomföra regelbunden översyn av organisationens användning av cybersäkerhetsverktyg och nätinfrastrukturer i syfte att utvärdera, identifiera behov och eventuell överlappning av verktyg med liknande funktionaliteter samt vidta åtgärder utifrån behov och en allriskbedömning och analys. I analysen ska även den nationella säkerhetshotbilden beaktas.

För att stärka cybersäkerhetsarbetet bör verksamheterna ta hjälp av externa referensramverk såsom ISO 27000-serien, Myndigheten för civilt försvars metodstöd och ENISA:s vägledningar samt dela information, erfarenheter och lärdomar inom ramen för samverkan, se rekommendation 3.

3. Etablera eller vidareutveckla externa samverkansformer i syfte att främja användningen av cybersäkerhetsverktyg och säker nätinfrastruktur med fokus på att:
 - a) stärka den gemensamma cybersäkerhetsförmågan genom delning av information, erfarenheter, kunskaper, goda exempel om hur cybersäkerhetsverktyg och säker nätinfrastruktur kan nyttjas på ett ändamålsenligt sätt samt följa upp effekten av samverkan utifrån målbilden.



- b) identifiera samarbetsområden för utveckling av användningen av cybersäkerhetsverktyg och säkra nätinфраstrukturer samt följa upp effekten utifrån målbilden.

Exempel på samarbetsområden är att utveckla samordnad verktygs- och infrastrukturstrategi, stödstrukturer för verktyg för cybersäkerhetsverktyg och säkra nätinфраstrukturer, gemensam kravställning, gemensam testning av verktyg, samt gemensamma digitala lösningar med centralt delade resurser.

4.2 Forskning och utveckling av cybersäkerhetsverktyg och säker nätinфраstruktur

Följande rekommendationer riktas till forskningsfinansiärerna i syfte att främja forskningen och utvecklingen av cybersäkerhetsverktyg och säker nätinфраstruktur:

4. Etablera och utveckla samverkansformer för analys av nuläge och åtgärder inom forskningsområdet cybersäkerhet, samt identifiera synergier mellan olika projekt i syfte att bidra till att överbrygga gapet mellan forskning, kommersialisering och operativ drift.

Samverkan kan exempelvis avse kommande satsningar inom cybersäkerhet och för att få en gemensam helhetsbild av forskningsområdet.

5. Vidta åtgärder för att främja tvärvetenskaplig forskning om cybersäkerhetsverktyg och säker nätinфраstruktur.

Åtgärder kan till exempel vara riktade utlysningar inom området som ställer krav på tvärvetenskaplig forskning i utlysningstexter eller tillse samordning av utlysningar. Åtgärder och uppföljning av åtgärder är ett område som kan vara föremål för samverkan, se rekommendation 4.

Följande rekommendationer riktas till lärosätena och forskningsinstituten i syfte att främja forskningen och utvecklingen av cybersäkerhetsverktyg och säker nätinфраstruktur:

6. Identifiera och vidta åtgärder som skapar incitament för att ta tillvara forskningsresultat i praktisk verksamhet samt följ upp om åtgärden fått avsedd effekt.

Åtgärder kan exempelvis vara att utveckla finansieringsmodeller så att forskningsresultat, samverkan och implementering premieras tydligare. Ett strukturerat återkoppling- och kvalitetsgranskningssystem kan skapa starkare incitament för nyttiggörande, stärka samarbeten mellan akademi, näringsliv och myndigheter samt höja deltagandet i internationella program. Genom att även följa upp hur lärosäten internt använder och stödjer sina forskningsresultat kan kapaciteten för kommersialisering, utbildningskoppling och kompetensförsörjning förbättras. Detta kan bidra till ett mer samlat och effektivt cybersäkerhetsekosystem.



Exempel på forskning inom området:

- *Post-kvantkryptografi (PQC)*
- *Bästa praxis tillämpningar inom totalsträckskryptering (end-to-end kryptering)*
- *Säker programutveckling (SDLC) och SBOM-ekosystem*
- *Samarbete och testbäddar för cybersäkerhetsforskning för näringsliv och myndigheter*

7. Vidta åtgärder för att främja tvärvetenskaplig forskning om cybersäkerhetsverktyg och säker nätinfrastruktur och följ upp om åtgärden lett till ökad tvärvetenskaplig forskning inom området.

Åtgärder kan exempelvis kan vara att främja kunskapsutbytet och därmed öka medvetandegraden kring området inom och mellan lärosäten och forskningsinstitut.

8. Delta aktivt i samverkan mellan forskare, andra lärosäten, forskningsinstitut, forskningsinfrastrukturer och näringsliv i syfte att identifiera synergier och samarbetsytor inom forskning och utveckling av cybersäkerhetsverktyg och säker nätinfrastruktur, samt följ upp om åtgärden fått avsedd effekt.

5 Giltighetstid

Dessa riktlinjer gäller från och med den 11 maj 2026 tills vidare.