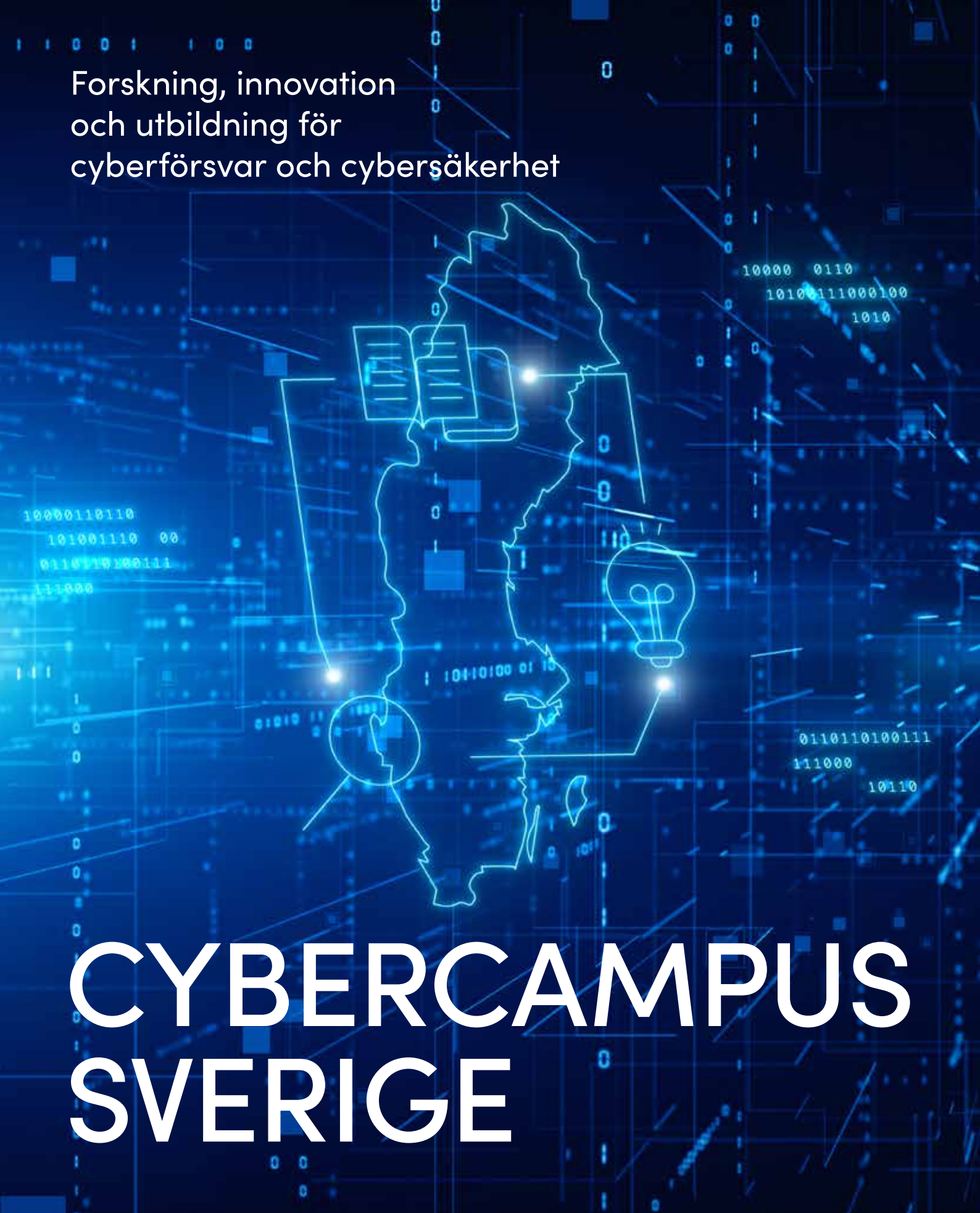
Forskning, innovation
och utbildning för
cyberförsvar och cybersäkerhet



CYBERCAMPUS SVERIGE

Varför behövs Cybercampus Sverige?

Om våra digitala infrastrukturer inte är säkra riskerar vi våra samhällskritiska funktioner.

Cybersäkerhet är en central fråga för digitaliseringen av Sverige. Men att bygga och förvalta digitala system har hittills visat sig vara en överväldigande utmaning. Följden av osäker teknik är stora krav på de som arbetar med cybersäkerhet. Det behövs hög kompetens för att säkra och försvara de förvånansvärt sårbara system som idag utgör samhällets digitala infrastrukturer.

Det behövs bättre verktyg och metoder för att utveckla och förvalta säkra it-system, liksom fortbildning av yrkesverksamma. Detta förutsätter löpande tillgång till kunskap och lösningar från forskning och innovationsarbete.

Ansvaret för att skydda den svenska cyberdomänen delas mellan många organisationer. Uppdelningen finns även inom akademisk utbildning och forskning i cybersäkerhet som genomförs utan samordning och gemensam inriktning av forskargrupper vid högskolor och institut i hela landet.

Andra europeiska länder såsom Norge, Schweiz, Frankrike och Tyskland har etablerat nationella knutpunkter för samverkan inom forskning, innovation och utbildning i cybersäkerhet. Dessa satsningar kallas emellanåt för cybercampus. Vi är övertygade om att en motsvarande svensk satsning behövs på ett campus där forskare, yrkesutövare och beslutsfattare kan samarbeta för en cybersäker digitalisering av Sverige.

Vid Cybercampus Sverige sker samarbeten inom forskning och innovation; där erbjuds säkerhetsutbildningar och ges expertstöd till svenska beslutsfattare; där koordineras svenska insatser i EU-forskningsprojekt och görs satsningar som bidrar till att Sverige gör avtryck på den internationella arenan. Cybercampus Sverige utgör en nationell forskningsinfrastruktur och organiseras nationellt mellan lärosäten, forskningsinstitut, myndigheter och svenskt näringsliv.

Sigbritt Karlsson
Rektor, KTH

Pia Sandvik
CEO, RISE

Micael Bydén
Överbefälhavare
Försvarsmakten

Ett trängande behov av forskning, innovation och utbildning

Den senaste tidens cyberattacker visar att det är nästintill omöjligt att bygga och underhålla it-system på ett säkert sätt.

Även i de mest grundläggande systemen i våra digitala infrastrukturer, som nätverkskomponenter och operativsystem, upptäcks löpande sårbarheter och säkerhetshål. Dessa finns trots att informationstekniken utvecklas av globala företag med 1000-tals världsledande ingenjörer och säkerhetsexperter. Det här långdragna misslyckandet understryker hur svårt det är att utveckla säkra mjukvarusystem.

En nyligen gjord studie visar att det saknas nära 200 000 yrkesverksamma i cybersäkerhet enbart i Europa.

Källa: (ISC)2 Cybersecurity Workforce Study, 2021

När ett problem är för svårt att lösa manuellt blir tekniken ofta räddningen, så även för it-utveckling och it-drift. Vi behöver säkrare programmeringsspråk, nätverksprotokoll, utvecklingsplattformar, testmetoder och systemförvaltningsverktyg. Det finns inga andra sätt att övervinna säkerhetsutmaningarna som hotar våra digitala infrastrukturer. Nya verktyg och metoder ges av vetenskaplig forskning och innovation. Tyvärr har inte cybersäkerhetsforskningen kunnat hålla jämna steg med samhällets digitalisering. Och svensk innovation för cybersäkerhet släpar efter sektorer som spelutveckling, media, och finans.

För att kompensera för bristen på säkra verktyg och arbetssätt behövs medarbetare som är synnerligen kunniga i cybersäkerhet. Men inte ens organisationer som har de bästa och flesta säkerhetsexperterna lyckas säkra och försvara sina it-system. För övriga organisationer är situationen än allvarligare. Sammantaget har detta lett till en situation med ett oroande stort kompetensgap. En nyligen gjord studie visar att det saknas nära 200 000 yrkesverksamma i cybersäkerhet enbart i Europa.

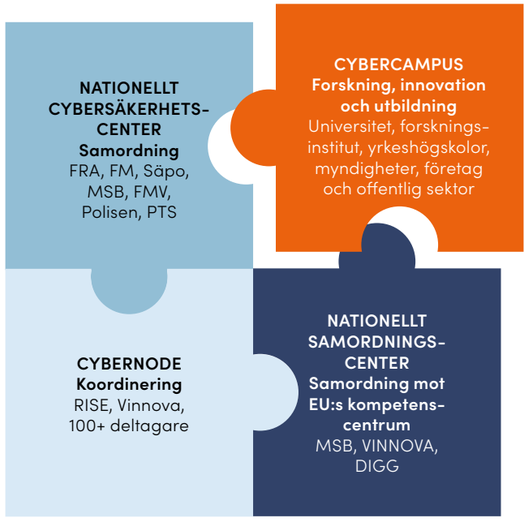
Forskning, utbildning och innovation med sammanhang och riktning

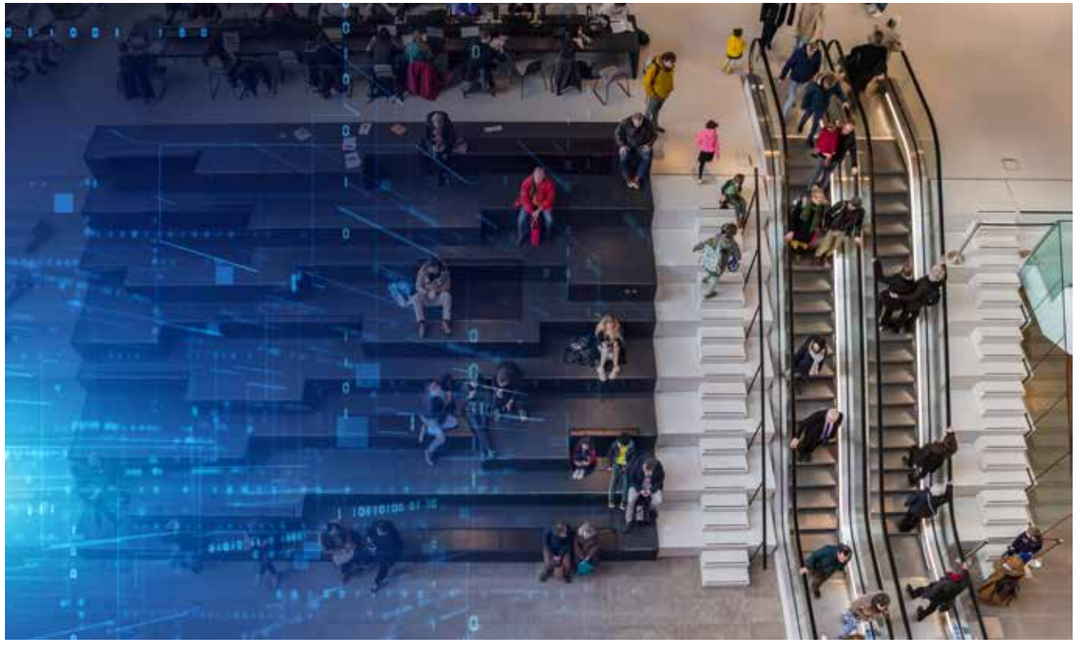
Ansvaret för att skydda den svenska cyberdomänen delas mellan många myndigheter. Inga, eller ett fåtal, av dessa organisationer bygger eller tillhandahåller svensk kritisk digital infrastruktur. Detta görs i stället av en mängd privata aktörer som därmed är lika viktiga för svensk cybersäkerhet. Det splittrade ansvaret gäller inte enbart utveckling och drift av dagens digitala system, utan även forskning, innovation och utbildning inom cybersäkerhetsområdet som idag saknar samordning och gemensam inriktning.

Svensk forskning om cybersäkerhet utförs utan större samarbete av små eller mellanstora forskargrupper utspridda över landet. Detta gör det svårt att möta nationella och internationella behov och att etablera och underhålla dyra infrastrukturer såsom cyberanläggningar, beräkningskraft och kvantdatorer. Avsaknaden av samarbete hindrar innovationer eftersom tillgång till kapital och expertis för entreprenöriella satsningar inte säkerställs. Detsamma gäller utbildning. Inget svenskt lärosäte har förmågan att driva cybersäkerhetsutbildningar i tillräcklig omfattning för livslångt lärande. Cyberområdets snabba utveckling står i bjärt kontrast till hur snabbt universitet kan omorganisera sig för att möta kontinuerligt förändrad efterfrågan på utbildningar. Syftet med ett svenskt nationellt cybercampus är inte att ersätta utan att komplettera redan pågående akademiska utbildningsinsatser och att etablera en universitetsöverskridande struktur som möter svenska cybersäkerhetsbehov med agil utbildning, gemensam forskning och disruptiv innovation.

Faktum är att Sverige har potential att på kort tid förbättra cybersäkerheten: forskningen som genomförs exempelvis på KTH vid Centrum för cyberförsvar och informationssäkerhet (CDIS) och på RISE har högt anseende internationellt. Utbildningen vid svenska lärosäten är modern och av hög kvalitet. Universitetens innovationsstöd och intresset från industrin finns. Utmaningen ligger i att skapa ett sammanhang, en gemensam riktning och prioritera vilka åtgärder som behöver vidtas.

Sverige behöver därför en nationell satsning, där universitet, forskningsinstitut och yrkeshögskolor kan möta och interagera med myndigheter och näringsliv. Sverige behöver ett cybercampus!





Ett svenskt cybercampus är ett komplement till andra befintliga nationella initiativ (se figur). Nationellt cybersäkerhetscenter har bland annat i uppgift att ge samordnat stöd till olika verksamheter i privat och offentlig sektor för skydd mot cyberattacker. Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet, vid Myndigheten för samhällsskydd och beredskap (MSB), knyter kontakter mellan aktörer i branschen och främjar EU-satsningar i Sverige med stöd vid utlysningar av forskningsanslag. RISE och Vinnova har etablerat en svensk innovationsnod för cybersäkerhet.

Cybercampus Sverige ska fokusera på forskning, innovation och utbildning som stöd för alla samhällssektorer och möta behov som inte adresseras av någon av de andra aktörerna för svenskt cyberskydd.

Andra nationers satsningar

Cybersäkerhet är en global angelägenhet som omfattar frågor gällande såväl individ och samhälle som ingenjörskonst och matematiska frågeställningar. För att hantera alla aspekter av cybersäkerhet behövs helhetsperspektiv för forskning, innovation, affärsutveckling, utbildning och yrkesträning. Runt om i världen finns åtskilliga exempel på sådana initiativ. Cybercampus hämtar inspiration från jämförbara europiska kompetenscentra och campus.

Nedan följer översiktliga beskrivningar av befintliga europeiska initiativ som exempel för ett framtida Cybercampus Sverige: Cyber Defence Campus i Schweiz, Norges Centre for Cyber and Information Security, Research Institute CODE i Tyskland, Security Delta i Nederländerna och Pôle d'Exellence Cyber i Frankrike. Även andra relevanta satsningar för forskning och innovation beskrivs, vilka tjänat som exempel för vårt förslag.

Cyber Defence Campus, CYD, Schweiz
Armasuisse, Schweiz motsvarighet till Försvarets materialverk, ansvarar för ett initiativ som ska stärka Schweiz förmåga att hantera cybersäkerhetshot genom samarbete mellan universitet, federala och kantonala myndigheter, och privata sektorn. CYD har verksamhet på tre platser: hos Armasuisse i Thun samt vid de tekniska högskolorna EPFL och ETH Zürich. Verksamheten påbörjades 2019 då de tre verksamhetsställena invigdes. CYD har en årlig budget om cirka 10 miljoner CHF med fler än 25 samarbetspartners som deltar i 50-talet projekt, från forskning till innovation och affärsutveckling. CYD är det internationella exempel som mest liknar den satsning vi föreslår.

Center for Cyber and Information Security, CCIS, Norge
CCIS är en norsk nationell centrumbildning för forskning, testning, utbildning och övningar. CCIS bildades 2010 i samverkan mellan fler än 40 norska offentliga, privata, civila, militära, och internationella parter. Den årliga budgeten omfattar cirka 100 miljoner NOK. Innovationsaktiviteter genomförs tillsammans med Norges Centre for Cybersecurity in Critical Sectors, NORCICS, som knyter till sig tjugotalet organisationer med representation från industrin, statliga myndigheter och akademiska utbildningsinstitut. CCIS målsättning är att Norge ska bli världens mest cybersäkra digitaliserade land.

Security Delta (HSD), Nederländerna
Security Delta erbjuder sina över 275 medlemsföretag, myndigheter och lärosäten kunskapsutveckling, innovationsstöd, kommersiella nätverk, rekryteringskanaler och riskkapitalnätverk. En del av Security Delta utgörs av HSD Campus, en fysisk mötesplats för nederländska intressenter inom cybersäkerhetsområdet. I jämförelse med exempelvis det tyska CODE är Security Delta mer orienterat mot näringslivs- och innovationssektorn.

Cyber Defence Research Institute, CODE, Tyskland
Tyska satsningar inom cybersäkerhet och cyberförsvar är utspridda över flera aktörer. Forskning genomförs huvudsakligen av följande: Cyber Defence Research Institute, CODE vid Tysklands försvarshögskola; Max-Planck Institute for Cyber Security and Privacy; CISPA Helmholtz Center for Information Security; KASTEL – Institute of Information Security and Dependability, och Fraunhofer ATHENE research centre for cybersecurity and privacy. Med cirka 250 anställda, varav 13 professorer, bedriver CODE gemensam forskning, innovation och etablering av nya företag i syfte att lyfta fram cybersäkerhet och digital suveränitet för EU-ändamål. CODE har ett eget datacenter och planerar att anskaffa en kvantdator.

Pôle d'Excellence Cyber, Frankrike
Excellenscentret i cybersäkerhet i Bretagne bedriver både fortbildning och akademisk forskning. Centret har en bred medlemsbas med universitet och "grandes écoles", forskningslaboratorier som CNRS och INRIA, stora företag samt små och medelstora entreprenörsföretag. Ett kompletterande initiativ – Campus Cyber vid La Défense i Paris – lanserades 2021 med ambitionen att främja fransk cybersäkerhetsexpertis i en internationell knutpunkt för affärsutveckling, innovation och entreprenörskap.

Andra internationella satsningar på cybersäkerhet

Helsinki-Aalto Institute for Cybersecurity, HAIC, Finland
HAIC är ett gemensamt initiativ mellan Aaltouniversitetet och Helsingfors universitet som syftar till att utveckla en världsledande centrumbildning for forskning och utbildning i cybersäkerhet.

NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE, Estland
CCDCOE bedriver forskning, träning och övningar i cyberförsvar inom områdena teknik, strategi, genomförande och juridik för medlemsländer och NATO. Sverige är medlem i centret.

London Office for Rapid Cybersecurity Advancement, LORCA, Storbritannien
LORCA är en accelerator för cybersäkerhet där experter på teknik och affärsutveckling arbetar tillsammans med investerare för att stärka affärssektorn och förbättra brittiskt cyberförsvar.

Utanför Europa
Betydande centrumbildningar för cybersäkerhet utanför Europa är de kinesiska initiativen i Tianjin utanför Peking och i Wuhan, amerikanska Cyber NYC på Manhattan samt israeliska CyberSpark i Beersheva.

Fyra röda trådar

Den första röda tråden i initiativen ovan är fokus på innovation som ett sätt att få fram nya system, lösningar och metoder till företag, offentlig sektor och statliga myndigheter. Effektiv innovation åstadkoms genom samlokalisering av alla relevanta aktörer, som är den andra röda tråden. Samlokalisering på ett campus med stödfunktioner möjliggör gemensamma projekt med hög synlighet som drar till sig investeringskapital. En tredje röd tråd är fortbildning av personal i cybersäkerhet. Sådan yrkesträning är starkt kopplad till utbildning av it-specialister och ökat säkerhetsmedvetande hos andra personalkategorier, till exempel i hälso- och sjukvården, finanssektorn och handeln. Den fjärde röda tråden är nationell samverkan mellan forskare för att lösa verkligt utmanande problem, driva och bekosta forskningsinfrastrukturer och för att konkurrera om europeisk forskningsfinansiering.

Uppdrag och målsättning

Uppdraget för Cybercampus Sverige är att bidra till ett digitaliserat och motståndskraftigt Sverige genom cybersäkerhetsforskning, innovation och utbildning. Målsättningen för verksamheten är att åstadkomma banbrytande resultat bortom det möjliga för enskilda universitet, institut, företag, eller myndigheter.

Målen för Cybercampus Sverige omfattar följande:

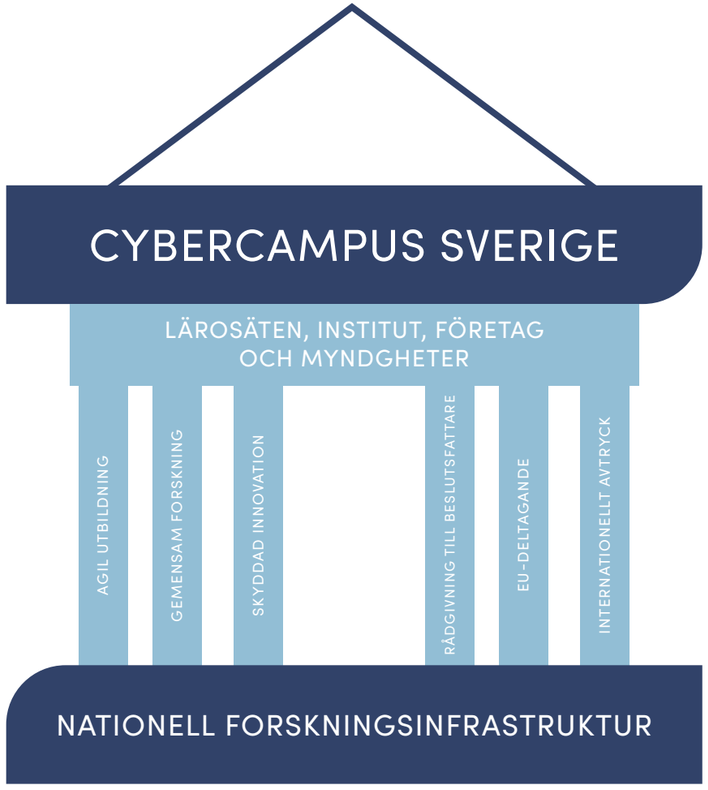
Agil utbildning i cybersäkerhet. Det råder en alarmerande brist på arbetskraft i Sverige inom cybersäkerhetsområdet eftersom lärosätena utexaminerar för få ingenjörer och tekniker för att tillgodose efterfrågan. De akademiska utbildningsprogrammen ger heller inte alla de färdigheter som efterfrågas på arbetsmarknaden. Verksamheten vid Cybercampus avser att höja kapaciteten för yrkesmässig träning. Nya cybersäkerhetsutbildningar kan utvecklas i samarbete mellan lärosäten utifrån deras olika expertiser. Tekniska kandidatprogram ger en stark kunskapsbas med möjlighet till ämnesmässig fördjupning; masterutbildningar och fortbildning bidrar till arbetskraft med rätt kompetens för svenska organisationers behov.

Gemensam forskning. Svensk cybersäkerhetsforskning är konkurrenskraftig, med framstående forskargrupper på universitet som KTH och forskningsinstitut som RISE. Men forskningen som utförs är inte tillräckligt koordinerad eller tvärvetenskaplig. Cybercampus Sverige ska kartlägga behov samt koordinera och bedriva gemensam forskning mellan universitet, högskolor och institut som är vital för svenska civila och militära säkerhetsintressen liksom för svensk konkurrenskraft.

Skyddad och säker innovation. Cybercampus Sverige är en inkluderande mötesplats för akademi, myndigheter, näringsliv och entreprenörer. Mötesplatsen, utbildningsprogrammen och den tvärvetenskapliga forskningen ska vara en nationell innovationsmiljö för cyberområdet. Cybercampus länkar samman akademisk forskning och säker innovation för såväl totalförsvaret som industrin.

Nationell forskningsinfrastruktur. Cybercampus Sverige avser att upprätta en unik forskningsinfrastruktur för cybersäkerhet och säker digitalisering. Infrastrukturen möjliggör samverkan med befintliga forsknings- och innovations-anläggningar som till exempel cyberträningsanläggningen CRATE vid Totalförsvarets forskningsinstitut (FOI) och RISE Cyber Range.

Rådgivare till beslutsfattare. Cybercampus Sverige ska kunna ge aktuella, opartiska och välgrundade råd och expertbedömningar till beslutsfattare i cybersäkerhets- och cyberförsvarsfrågor. Detta innefattar råd som rör EU-regleringar, utvärdering av säkerheten i nationella digitala infrastrukturer, satsningar på såväl forskning och innovation som samhällsviktiga produkter och tjänster som används i nationella system.



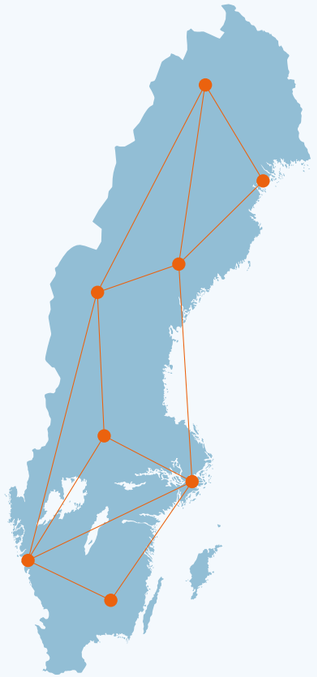
Samordnat EU-deltagande. EU erbjuder mångmiljardsatsningar på digitalisering och cybersäkerhet. Det råder obalans mellan hur svenska organisationer tar del av EU-satsningarna och hur Sverige bidrar finansiellt till satsningarna. Det krävs resurser för att komma med i initiativen, professionellt stöd som kan hålla ihop ansökningsarbetet och senare bistå i projektledning och -koordinering. Det föreslagna Cybercampus Sverige ska ha förmåga att ansöka om och leda projekt som finansieras av EU.

Internationellt avtryck. Cybercampus ökar Sveriges avtryck i internationella forsknings- och innovationssammanhang. Ett campus blir en enande kraft med tillgång till en forskningsinfrastruktur som tillsammans med långsiktig svensk och internationell finansiering sörjer för svensk cybersäkerhet i vetenskapens framkant. Detta attraherar i sin tur expertis till Sverige som ytterligare stärker det nationella ekosystemet för cybersäkerhet.

Organisation och lokalitet

Erfarenheten ger vid handen att nationella forsknings-infrastrukturer ger bäst nytta om de upprätthålls i samarbete mellan flera universitet, högskolor och andra intressenter.

Ett framgångsrikt exempel är SciLifeLab som grundades som en gemensam satsning av fyra universitet (KTH, Uppsala universitet, Karolinska institutet och Stockholms universitet), varav ett är värd (KTH). Styrkan hos SciLifeLab, som grundades 2009, är den gemensamma infrastrukturen som är tillgänglig för alla svenska universitet som är verksamma inom biovetenskapen. SciLifeLab hanterar även databaser, ger utbildning på infrastrukturen och för över forskningsresultat till innovationsarbete. Andra aktörer från hälso- och sjukvårdssektorn och industrin har också starka band till SciLifeLab och använder infrastrukturen. Angreppssättet möjliggör integrerad samverkan, forskning, datautbyten och utbildning. Styrkan i en sådan nationell forskningsinfrastruktur är också något som intressenterna kunnat dra nytta av under pandemin.



Mot bakgrund av detta föreslås att Cybercampus Sverige organiseras som ett nationellt samarbete mellan flera lärosäten, forskningsinstitut, statliga myndigheter och privata företag i Sverige. Medarbetarna består av fakultet från ingående lärosäten och forskare vid institut, liksom utvald personal från företag och myndigheter som blir knutna till campuset.

Lokalerna för Cybercampus Sverige utformas för att inspirera medarbetarna och skapa en dynamisk och neutral mötesplats för alla berörda parter från privat och offentlig sektor. Både organisation och lokaler utformas för att möjliggöra forskning och innovation kring frågeställningar som rör Sveriges säkerhet och företagshemligheter. Lokalernas planering och verksamhetens organisation regleras så att både skyddat och öppet samarbete möjliggörs med avseende på fysiskt skydd och informationssäkerhet. Uppdelningar som begränsar kontakter ska stödjas vid behov, samtidigt som en öppen miljö för samarbete bibehålls där det är möjligt.

Handlingsplan

Nedan redovisas förslag till åtgärder för att upprätta och påbörja verksamheten vid Cybercampus Sverige.

Nödvändiga externa beslut

- Besluta om att inrätta Cybercampus Sverige med långsiktig finansiering för verksamheten.
- Utse en styrgrupp med representanter från ingående universitet, högskolor, forskningsinstitut, statliga myndigheter och företag.
- Utse en intressentgrupp med representanter från andra svenska högskolor och yrkeshögskolor samt branschföreträdare som kan bidra med ett nationellt perspektiv på campusets verksamhet.

Interna förberedande aktiviteter och beslut

- Utforma en plan för etableringen av Cybercampus Sverige.
- Rekrytera personal till ledning och stab.
- Anskaffa Cybercampus-lokaler.
- Ta fram en strategi för att stärka den nationella ställningen i cybersäkerhet och -skydd.
- Utveckla utbildning.
- Upprätta en verksamhetsplan för infrastrukturer på campus – med teknologier, expertis, och mötesplatser – för svenska forskare och innovatörer inom cyberförsvar och -säkerhet.
- Inrätta ett internationellt råd för att säkerställa att Cybercampus Sverige utvecklas i linje med internationella trender och praxis.

Om organisationerna bakom Cybercampus Sverige

KTH Kungliga Tekniska Högskolan
KTH är Sveriges största och mest produktiva universitet inom cybersäkerhetsforskning. KTH utvecklar ny kunskap som stärker svensk cybersäkerhet i takt med samhällets digitalisering. KTH:s Centrum för cyberförsvar och informationssäkerhet är ett forsknings- och utbildningssamarbete mellan KTH, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Försvarets radioanstalt, Totalförsvarets forskningsinstitut och Försvarshögskolan. Centrumbildningens forskning utgörs av nydanande metoder och verktyg för informationssäkerhet liksom resultat som stärker cyberförsvaret. CDIS möjliggör kunskapsöverföring till de ingående parterna och andra utpekade organisationer. På uppdrag av Försvarsmakten utbildar KTH också värnpliktiga cybersoldatergenom genom kurser som bygger på kunskap i forskningens framkant.

RISE Research Institutes of Sweden
RISE, som är Sveriges största statligt ägda forskningsinstitut, har sitt huvudkontor i Göteborg och verksamhetsställen i alla större svenska städer. Ett fokusområde för RISE är cybersäkerhet med drygt 30 forskare. Utöver grundforskning och tillämpad cybersäkerhetsforskning, deltar RISE i strategiska forskningssatsningar i Sverige och EU i nära samarbete med industrin. Viktiga aktiviteter är att leda arbetet i Sveriges nationella cybersäkerhetsnod för innovation (cybernode.se), att testa och demonstrera cybersäkerhet i RISE Cyber Range samt att vara partner och en del av ledningsgruppen för Concordia EU Cybersecurity Network of Excellence.

Försvarsmakten
Försvarsmakten försvarar Sverige, landets frihet och skyddar allas vår rätt att själva välja hur vi ska leva. Försvarsmakten växer, stärker sina förmågor och utvecklar morgondagens försvar. Tillgång till banbrytande kunskap i forskningens framkant är central för Försvarsmaktens förmågeutveckling, inte minst inom cyberförsvar och informationssäkerhet. Försvarsmakten utvecklar sin förmåga tillsammans med nationella och internationella samarbetsparter.

Kontakt

Pontus Johnson
Föreståndare för CDIS, KTH
pontusj@kth.se

Shahid Raza
Föreståndare för Avdelningen för cybersäkerhet, RISE
shahid.raza@ri.se

David Olgart,
Utvecklingsledare och koordinator för forskning och teknikutveckling inom cyberförsvar, Försvarsmakten
david.olgart@mil.se