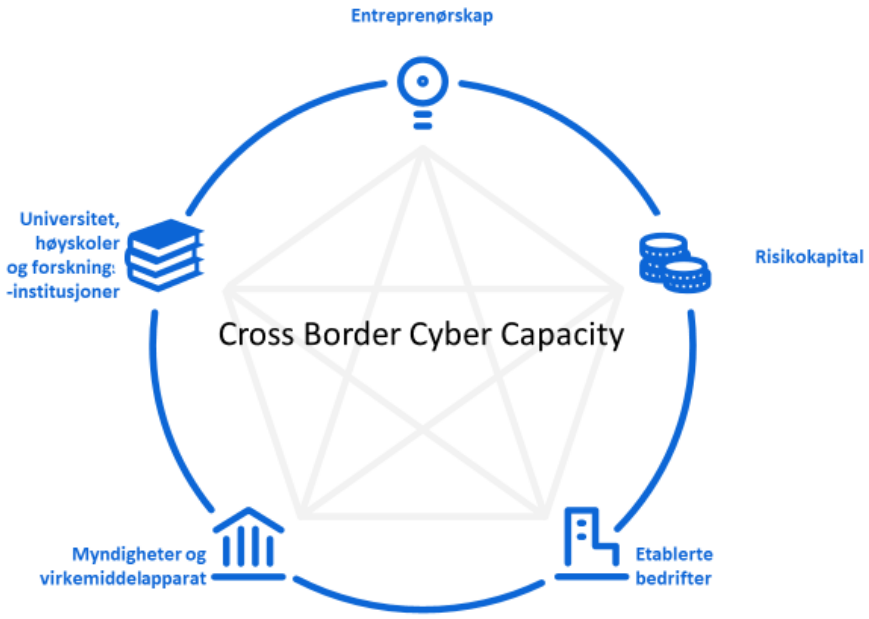
Cross Border Cyber Capacity



DIGITAL INNLANDET compare

INN Høgskolen i Innlandet · NTNU · VÅGER INNOVASJON · KARLSTADS KOMMUN · Karlstads Universitet

Bakgrunn og motivasjon

Cybersikkerhet som samfunnsutfordring og næring

Improving cybersecurity is essential for people to trust, use and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information. Cybersecurity is indispensable to the network connectivity and the global and open Internet that must underpin the transformation of the economy and society in the 2020s.

EU's Cybersecurity Strategy for the Digital Decade (European Union 2020, p.4)

Bill Gates forutså i 1999 at innen 2020 vil «folk betale regninger og kommunisere med legen gjennom internett». Han uttalte dette da kun 14% av belgierne brukte internett og 30% hadde mobiltelefon, men Gates så hvor trenden var på vei. Den verden Bill Gates forutså er her nå, og med den mange forenklinger gjennom digitalisering. Få forutså imidlertid for 20 år siden den kompleksiteten og omfanget av trusler samfunnet, institusjoner, næringsliv og personer i vår digitale verden står ovenfor.

De siste årene har det vær en stadig sterkere fokus på cybersikkerhet og trusler mot samfunn, næring og privatpersoner. Cyberattack, løsepenger og risiko knyttet til datadeling og personvern er høyt oppe på bevisstheten. Fra å være et problem for IT-avdelingen har cybersikkerhet nå blitt til et tema som adresseres i toppledelsen og i styrerommet i samfunns- og næringsliv. IT og cyberrelaterte næringer er i vekst, og det er stor etterspørsel etter løsninger som sikrer motstandsdyktighet mot angrep, samt kompetanse knyttet til sikkerhet og personvern. Vi ser fremvekst av klynger eller hubber som samler forskning, næringsliv og myndigheter for felles innsats, og samarbeid for utnyttelse av muligheter for regional vekst og utvikling knyttet til den nye sikkerhetsnæringen.

Både i Norge og Sverige har det siden midten av 2000-tallet vært satsinger på cyber- og samfunnssikkerhet. I Norge har det vokst frem et sterkt kompetansesentrum i Innlandet, mens i Sverige har Värmland posisjonert seg. Den geopolitiske situasjonen siden 2022 aktualiserer et forsterket nasjonalt samarbeid innen feltet, og et mulig svensk NATO-medlemskap åpner dører for nye samarbeidsflater knyttet til blant annet data- og informasjonsdeling. Dette reflekteres også på næringssiden, der en ny avtale om næringssamarbeid knyttet til IKT mellom Norge og Sverige ble inngått våren 2022.

På regionalt nivå fremheves IKT som et av områdene hvor det prioriteres å styrke fagmiljøer og klynger gjennom grenseoverskridende innovasjonssystemer (Samarbeidsavtale Innlandet fylkeskommune-Region Värmland 2023-2025). Inom EU har begreppet Strategi för Smart Specialisering (S3) fastställts som ett verktyg och arbetssätt för regional utveckling. Smart specialisering är ett sätt att kraftsamla för innovation och hållbar utveckling inom de områden där det finns störst potential. Digitalisering och Samhällsäkerhet är identifierade som strategiskt viktiga plattformar i det regionala tillväxtarbetet i Värmland. Samarbeid er etablert mellom universitets- og høgskolemiljøene, og det er pågår større grenseregionale satsinger på krisehåndtering og beredskap (blant annet Interreg Sverige-Norge prosjektet CrisisIT). Både Norges teknisk-naturvitenskapelige universitet (NTNU) och Karlstads universitet (KAU) har tidigare gått samman i forskningsprojekt, inklusive PETweb II-projektet finansierat av Norges Forskningsråd med KAU som extern projektmedlem, och CyberSec4Europe EU H2020-projektet, där både KAU och NTNU har varit projektpartners. Begge regioner har sterkt

forankrede strategiske satsinger og sterke miljøer knyttet til IKT og cybersikkerhet som skaper gode forutsetninger for verdiskaping og grenseoverskridende samarbeid innenfor en ny næring.

Forprosjekt og mulighetsanalyse: Identifiserte muligheter, grenseoverskridende utfordringer og behov knyttet til cybersikkerhet som vekstnæring i Innlandet og Värmland

Til tross for sterke kompetansemiljøer knyttet til universitetet/høyskolemiljøene og sterke offentlige kompetansemiljøer innen cyber- og samfunnssikkerhet, er det svakheter særlig i de næringsrettede delene av økosystemene både i Innlandet og Värmland. Dette er en av konklusjonene fra et Interreg-forprosjekt mellom Digital Innlandet fra norsk side og Compare fra svensk side gjennomført i 2022, som også underbygges av forprosjektet til NCCS. I forprosjektet «Tech Innovation Cluster» ble det jobbet med å kartlegge felles styrkeområder og utfordringer, samt områder for å utnytte og utvikle felles kompetanse tilknyttet innovasjon og digitalisering. Spesifikt ble det jobbet med å identifisere hvordan satsinger rundt cybersikkerhet og helse kunne kobles på tvers av regionene, samt se på barrierer for innovasjon og vekst knyttet til eksisterende økosystem for cyber- og samfunnssikkerhet. Det ble identifisert konkrete utfordringer der en samlet og målrettet grenseoverskridende innsats gjennom hovedprosjektet Cross Border Cyber Capacity Innlandet-Värmland vil håndtere utfordringene på en styrket måte sammenlignet med regional innsats:

Behov for økt tilvekst av nye bedrifter: Både Innlandet og Värmland har få nyetablerte bedrifter basert på teknologi, særlig sammenlignet med storbyregioner. Det finns et stort behov for å styrke og støtte tilveksten av nye bedrifter innen nye kompetansebaserte næringer. Spesielt innenfor cybersikkerhet og IT er det store muligheter. Cybernæringen er imidlertid en relativt ny næring i våre regioner, og det er behov for et sterkere miljø rundt vekst og bedriftsetablering. Det er også viktig å stimulere til og støtte "intraprenørskap" - innovasjon og utvikling i og spin-offs fra eksisterende virksomheter. Det ligger også et potensial i å styrke samhandlingen mellom de etablerte virksomhetene og start-ups. Gjennom et nærmere interregionalt samarbeid vil vi kunne utnytte innovasjonsstrukturen på tvers av landegrensen til det beste for eksisterende og nye selskaper.

Behov for økt bruk av innovasjons- og forskningsvirkemidler, og kunnskapsflyt mellom forskning og næringsliv: Nasjonalt står begge regionene for en liten del av forskningsinnsatsen, men i Innlandet står cybersikkerhet for en vesentlig del av kunnskapsproduksjonen og forskningsaktiviteten. I Värmland er datavetenskap inklusive cybersäkerhetsforskning valts som en av KAUs utmärkta forskningsmiljöer i 2014. Det er imidlertid et behov for å øke samarbeidet mellom akademia/forskning og næringslivet i begge regioner, særlig med tanke på å få til en sterkere kunnskapsflyt som grunnlag for innovative løsninger og forskningsbasert innovasjon, og med tanke på å bidra med løsninger på viktige samfunnsutfordringer – gjerne på basis av prioriterte innsatser i EU/Horisont Europa. I begge regioner er det et tydelig behov for internasjonalisering av resultatene av innovasjonsarbeid og utvikling/lansering av nye produkter og tjenester. For å lykkes med dette trengs gode partnerskap nasjonalt, men ikke minst på internasjonalt nivå.

Bedre tilgang til risikokapital: Både Värmland och Innlandet är små regioner som har svårt att attrahera kapital för satsningar i innovativa företag. Genom att driva gemensamma satsningar över gränsen som stärker de innovativa företagen ökar möjligheten att attrahera kapital. Det samlede miljøet blir større, mer komplett og dermed mer attraktivt.

Behov for økt attraktionskraft för kompetens och talanger: IT-kompetens är en knapphetsresurs, i synnerhet finns det ett stort behov av fler personer med specialistkompetens inom cybersäkerhet. I hela Europa är det stort fokus på "Cybersecurity skills gap". European Union Agency for Cybersecuritys (ENISA) report påpekar att antalet utexaminerade under de kommande 2–3 åren förväntas fördubblas.

Könsfördelningen är dock fortfarande ett problem med endast 20 % av studenterna som är kvinnor. ENISAs rekommendation är att det behövs mer stöd och riktat arbete för skapandet av ett enhetligt förhållningssätt mellan myndigheter, industri och lärosäten genom antagandet av ett gemensamt ramverk för cybersäkerhetsroller, kompetenser, färdigheter och kunskaper. Dette er også velkjent i både Innlandet og Värmland. Dette gapet setter nærings- og samfunnsliv i fare, og etterspørselen etter komeptanse og talenter knyttet til IT og cybersikkerhet er økende. I dette perspektivet er det også bekymringsfullt at kompetansebasen og næringen mangler diversitet knyttet til kjønn og etnisitet. Kun 25% av arbeidsstyrken knytett til cybersikkerhet på verdensbasis er kvinner (ISC 2022 Cybersecurity workforce study). Lignende studier finnes ikke fra Värmland og Innlandet, men det er grunn til å tro at andelen kvinner er enda lavere i vår region. Det er bredt dokumentert at bedre mangfold gir bedre løsninger, og det er behov for å økt mangfold og likestilling knyttet til cybersikkerhet og IT i våre regioner.

Grenseoverskridende merverdi og motivering for Cross Border Cyber Capacity: Overordnet perspektiv

På bakgrunn av felles utfordringer og mulighetsrom med utgangspunkt i Innlandet og Värmland som sterke kompetansesentrum innen cyber- og samfunnssikkerhet, sammenfattes motivasjonen for prosjektet i følgende modell, utledet fra modell for grenseregional merverdi *fra prosjekthåndbok Interreg Sverige- Norge 2021-2027 (s.9):*

Modell 1: Modell for grenseregional merverdi (fra prosjekthåndbok Interreg Sverige - Norge) sett opp mot Cross Border Cyber Capacity sitt grenseoverskridende potensial.

Vi ser at regionene har **komplementær kompetanse** knyttet til cyber- og samfunnssikkerhet innen blant annet utdanning og forskning, strategiutvikling og næringsliv, og forprosjektet har bekreftet at det er nyttig å få videre innsikt i hverandres arbeid knyttet til cyber- og samfunnssikkerhet for å skape forståelse og få nye perspektiver på egen utvikling, posisjon og arbeid. Cross Border Cyber Capacity legger til rette for dette gjennom dypere kjennskap og gjensidig forståelse (Nivå 1 grenseregional merverdi i modellen over).

Vi ser også at de grenseoverskridende utfordringene beskrevet i 1.2 over kan tas tak igjennom å legge til rette for **overføring av kompetanse, praksiser og strukturer.** Vi har utfyllende øvingslabber og kapasiteter for innovasjon, teknisk utvikling og testing, vi ønsker å lære av hverandres aktiviteter knyttet til innovasjonssamarbeid og teknikkutnyttelse, blant annet overføre suksesselementer fra den

svenske modellen med en nordisk venture-akselerator innen helse-tech til en felles satsing innen cyber- og samfunnssikkerhet (Nivå 2 grenseregional merverdi).

Som nevnt i del 1.1 over har både Innlandet og Värmland over tid bygd opp sterke økosystemer koblet til cyber- og samfunnssikkerhet der næringsliv, akademia, finansieringsaktører, myndigheter og offentlig sektor samvirker for verdiskaping og vekst. Vi mener at det å koble sammen disse økosystemene til et **grenseoverskridende innovasjonsøkosystem koplet til cyber- og samfunnssikkerhet** gir bedre forutsetninger for at regionene lykkes med sine ambisjoner på området (Nivå 3 grenseregional merverdi).

Både Innlandet og Värmland har forsknings- og utdanningsmiljøer som er i verdensklasse innenfor sine felt knyttet til cyber- og samfunnssikkerhet. Vi ser i begge regioner et stort potensial for at etablerte selskaper og start-ups i større grad utnytter denne kunnskapen til utvikling av nye kommersielle og konkurransedyktige løsninger og tjenester. Det er et stort behov for og stor etterspørsel etter løsninger/tjenester, og prosjektet legger til rette for forsterket kraft og bedre kunnskapsflyt som leder frem til **ny kunnskap for felles behov** (nivå 4 grenseregional merverdi). Alle potensial og nivåer beskrevet over vil på sikt legger grunnlag for utvikling av konkrete **felles løsninger** (nivå 5 grenseregional merverdi).

Mål og oversiktsbilde prosjektlogikk

Basert på potensial for grenseoverskridende merverdi er vår visjon att utvikla ett grenseoverskridende cyberinnovasjonsøkosystem som skaper vekst og verdiskaping gjennom felles kapasitetsbygging og overføring av teknologi og kompetanse.

Projektets övergripande mål är att stärka och utveckla Värmland och Innlandets forsknings- och innovationskapacitet inom cyber- och samhällssäkerhet med syfte att stärka regionens konkurrenskraft och resiliens, samt sätta grunden till skapandet av ett starkt internationellt innovationsekosystem.

För att uppnå huvudmålen ska projektet resultera i följande tre delmål:

Delmål 1:

Utveckla en gränsöverskridande modell för uppskalning av företag som arbetar inom cyber- och samhällssäkerhet med syfte att öka konkurrenskraften, kommersialiseringen och exporten i startups och SMEs.

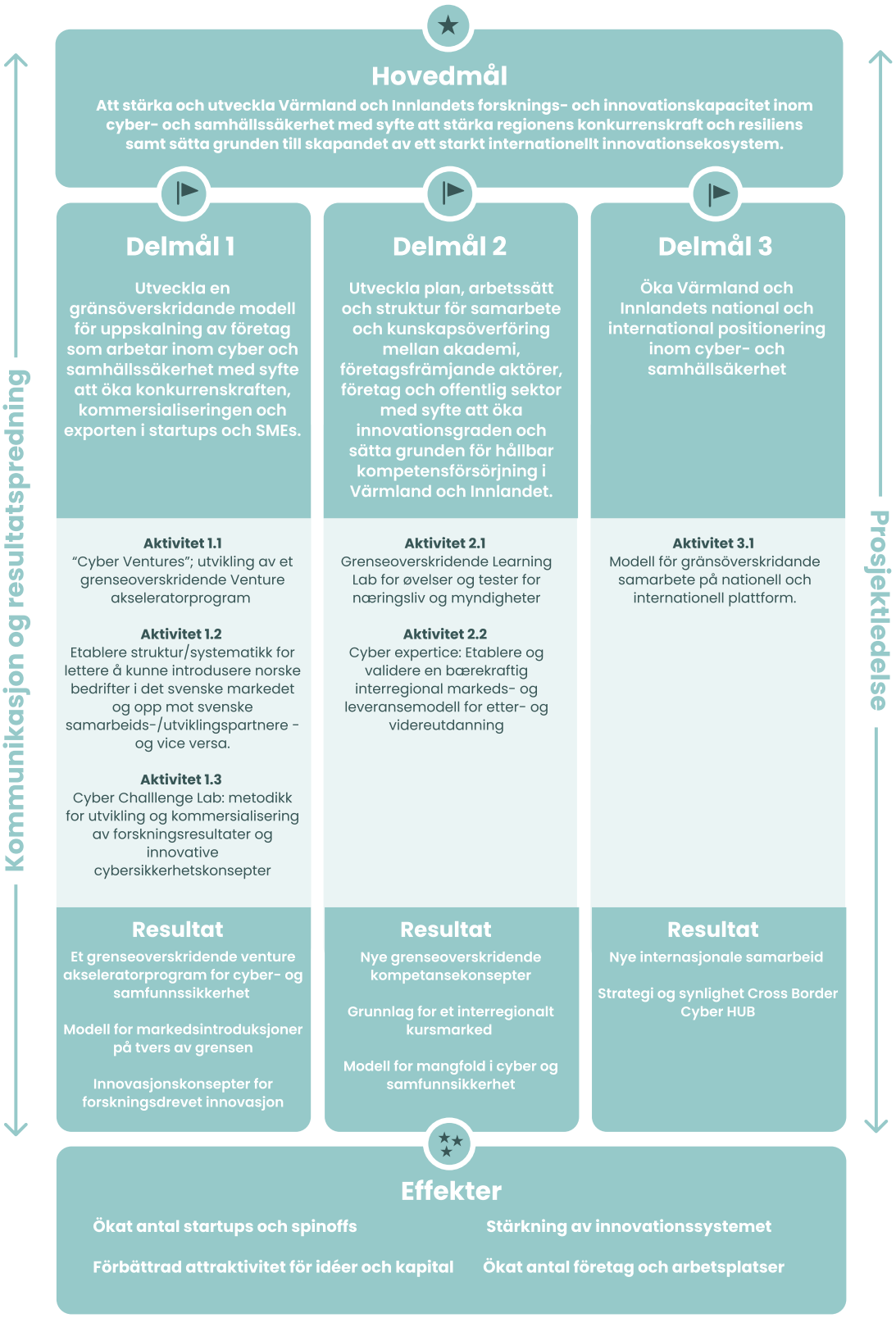
Delmål 2:

Utveckla plan, arbetssätt och struktur för samarbete och kunskapsöverföring mellan akademi, företagsfrämjande aktörer, företag och offentlig sektor med syfte att öka innovationsgraden och sätta grunden för hållbar kompetensförsörjning i Värmland och Innlandet.

Delmål 3:

Öka Värmland och Innlandets national och international positionering inom cyber- och samhällsäkerhet.

Modell 3: Cross Border Cyber Capasity prosjektoversikt



Resultat og effekter

Prosjektet vil i tråd med delmålene levere grenseoverskridende modeller og konsepter som vil stärka och utveckla Värmland och Innlandets forsknings- och innovationskapacitet inom cyber- och samhällssäkerhet.

Resultat	Beskrivning	Mål | AP
Cyber Growth	Ett gränsöverskridande affärsutvecklings modell för företag inom cyber- och samhällsäkerhet.	Mål 1 I AP1
Cyber Academy	Etablerat hållbar samverkansstruktur för genomförande av gemensamma kunskapsspridande och kompetensförsörjande satsningar efter avslutat projekt.	Mål 2 I AP2
Cross Border Cyber Hub	Modell för gränsöverskridande samarbete på nationell och internationell plattform.	Mål 3 I AP3

Bidrag til aktivitetsindikatoren:

Indikator nr	Indikator beskrivelse	Antall
RCO01	Företag som får stöd (fördelade per mikroföretag, små, medelstora, stora företag) (Med stöd avses aktiviteter som finansieras av projektet. Avsikten med stödet är att företagets förmågor ska stärkas och i förlängningen kunna ändra beteende. Ex. få kunskap för att hitta nya marknader. Företagen ska rapporteras in i Min Ansökan med organisationsnummer både på svenska och norska företag.	40
RCO10	Företag som samarbetar med forskningsorganisationer	40
RCO 83	Gemensamt utarbetade strategier och handlingsplaner	3*

*Cyber Growth, Cyber Academy, Cross Border Cyber Hub

Et gjennomgående sentralt element i Cross Border Cyber Capacity er fokus på å bringe sammen utfyllende kompetanse, infrastruktur og erfaringer for å forsterke kapasitet for innovasjon knyttet til cyber- og samfunnssikkerhet. Gjennom Cyber Growth får start-ups og etablerte bedrifter styrket kapasitet til å lykkes i et globalt marked. Gjennom Cyber Academy får samfunns- og næringsliv i regionene et styrket kompetansetilbud, og Cross Border Cyber Hub styrker grenseregionen sin kapasitet for strategisk posisjonering nasjonalt og internasjonalt.

För att följa upp resultaten i tabellen ovan har vi valt att sätta följande projektspecifika KPI:

→Et grenseoverskridende venture akseleratorprogram for cyber- og samfunnssikkerhet med kapasitet til å få frem konkurransedyktige starts-ups og legge til rette for skalering. Målet er at 12 bolag på svensk og norsk side kvalifiserer til og deltar i programmet i prosjektets år 2 og 3, etter en utviklingsfase i år 1.

→Introduksjon til markeder på tvers av grensen for minst 6 bolag

→Innovasjonskonsepter for forskningsdrevet innovasjon innen cyber og samfunnssikkerhet. Vi har som mål at minst 3 Challenge Lab cases tas ut og videreutvikles til konsepter / innovasjons-prosjekter for videreutvikling.

→Kompetansekonsepter innen cyber- og samfunnssikkerhet og grunnlag for et interregionalt kursmarked etableres. Målet er minst 2 grenseoverskridende kompetansekonsepter, samt strateginotat for felles kompetansemodell.

→Modell for økt mangfold i cyber- og samfunnssikkerhet. Minst 3 Female Focus grupper og felles arrangementer.

→ Strategi for økt synlighet gjennom «Cross Border Cyber Hub».

→2 nye internasjonale samarbeid

Videre legges det i prosjektaktivitetene vekt på å utvikle bærekraftige modeller og konsepter som videreføres etter prosjektperioden. Dette vil la seg gjøre gjennom prosjekteiere med operative og finansielle muskler til å videreutvikle resultatene fra prosjektet, og som har en etablert posisjon innen digitalisering, cyber- og samfunnssikkerhet i regionene. Men ikke minst gjennom etablerte samarbeidsstrukturer med prosjektets partnere på begge sider.

Basert på dette har Cross Border Cyber Capacity gode forutsetninger for å sette varige avtrykk i grenseregionen, og også på den nasjonale og internasjonale arenaen. Prosjektet vil skape varige effekter på ulike områder, som i korthet kan summeres i følgende punkter:

- **Ökat antal startups och spinoffs:** Genom att erbjuda bättre förutsättningar för affärsutveckling och tvärregional samverkan syftar projektet till att uppmuntra tillkomsten av nya startups och spinoffs från forskningsmiljöer, befintliga företag och offentliga organisationer. Detta kan leda till ökat entreprenörskap och jobbskapande, särskilt inom området cyber och samhällssäkerhet.
- **Förbättrad attraktivitet för idéer och kapital:** Projektet syftar till att stärka grunden för affärsutveckling och öka tillgången till relevant expertis och kunskapsflöde. Detta kan hjälpa till att förbättra den övergripande innovationssystemet inom cyber, göra det mer attraktivt för idéer och kapitalinvesteringar.
- **Stärkning av innovationssystemet:** Projektet syftar till att skapa tvärnationala arenor för kunskapsflöde mellan akademin, företagsfrämjande aktörer och industri. Detta kan hjälpa till att underlätta överföringen av avancerad teknik och att främja samarbete, vilket kan bidra till stärkningen av innovationssystemet.
- **Ökat antal företag och arbetsplatser:** Den ökade antalet startups och spinoff, kombinerat med förbättrade förutsättningar för affärsutveckling och stärkt innovationssystem, kan leda till ett ökat antal företag och arbetsplatser inom området cyber och samhällssäkerhet. Detta kan bidra till ekonomisk tillväxt och jobbskapande i regionen.