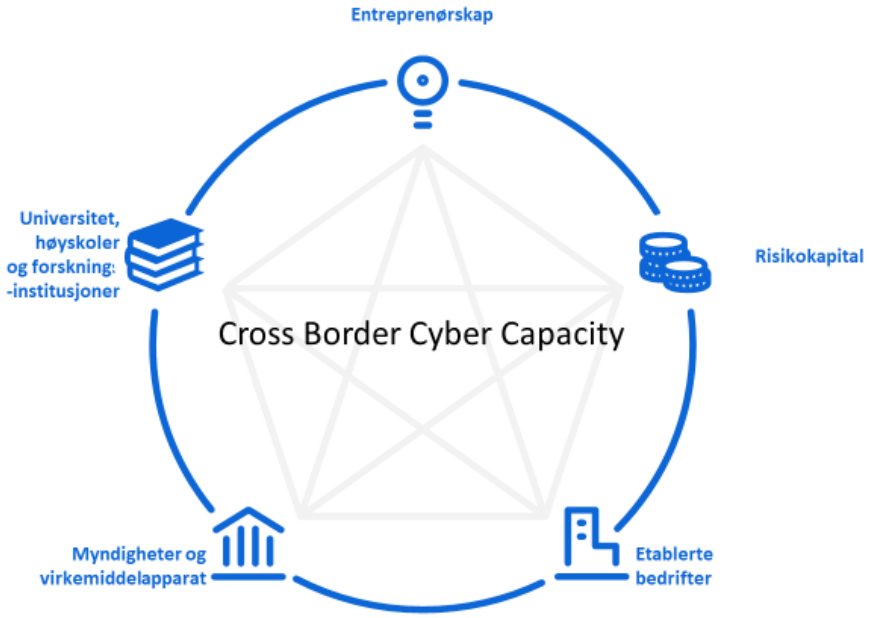
Prosjektbeskrivelse

Cross Border Cyber Capacity



DIGITAL INNLANDET

compare

Høgskolen i Innlandet

NTNU

VÅGER INNOVASJON

KARLSTADS KOMMUN

KARLSTADS UNIVERSITET

Contents

1. Bakgrunn og motivasjon

1.1 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.

1.2 Innlandet og Värmland - Kompetansesentrum for cyber- og samfunnssikkerhet

I Norge har den sterkeste utviklingen av kunnskap og kapasitet innenfor cyberområdet foregått i Innlandet, med NTNU i Gjøvik og Cyberforsvaret i Lillehammer som spydspisser. Medregnet bachelor-, master- og doktorgradsutdanninger fra NTNU, så representerer disse institusjonene hele to tredjedeler av den totale kunnskaps- og kompetanseproduksjonen innen cybersikkerhet i Norge. Institusjoner som Center for Cyber and Information Security (NTNU CCIS) (privat/offentlig og sivilt/militært forskningspartnerskap), SFI Norwegian Center for Cyber Security in Critical Sectors (NORCICS), og Norsk Senter for Informasjonssikring (NorSIS) (den norske regjeringens satsing på bevisstgjøring og rådgivning), har sine utspring fra NTNU. Videre er NTNU Norwegian Cyber Range (NCE) etablert som en nasjonal øvings-/testarena innenfor cyberdomenet.

I økosystemet finner vi også Cyberingeniørhøgskolen (CIS) som er en del av Forsvarets Høyskole og det norske Cyberforsvaret - som tilbyr utdanning på bachelornivå til kandidater i Forsvaret. CIS ønsker industrien inn på tilbydersiden i form av sivilt – militært samarbeid. Dette også som en erkjennelse av industriens betydning i en totalforsvarssammenheng. Høgskolen i Innlandet (HINN) tilbyr kompletterende utdanningstilbud innen informasjons- og cybersikkerhet, og Fagskolen Innlandet utdanner fagarbeidere innen IKT, drift og IKT-sikkerhet/cybersikkerhet. I Innlandet ligger også Kommune-CSIRT som er et respons- og kompetansesenter for kommunene. Innlandsregionen har også forpliktende nettverkssamarbeid mellom industri og kompetanseaktører for leveranser til forsvaret (Total Defence Group).

Prosjektet det «The Norwegian Cluster for Cyber Security» (NCCS) ble etablert i 2022 med Digital Innlandet som prosjekteier og operatør. NCCS er en næringsdrevet nasjonal klynge med regional forankring i Innlandet. Klyngen hadde ved etablering 19 næringspartnere i tillegg til NTNU, Fagskolen Innlandet og Vaager Innovasjon, og vil våren 2023 styrke ressursgrunnlaget gjennom opptak av nye partnere.

På svensk sida har Värmland ett antal styrkor inom området samhällssäkerhet, bland annat som kompetenscentrum och inom akademin. Återetableringen av Artilleriregementet A9 i Kristinehamn, den nya myndigheten för Psykologiskt försvar, Plikt- och prövningsverket, Myndigheten för samhällsskydd och beredskap samt delar av Försvarhögskolan med relevant forskning bidrar alla till att skapa en stark miljö för dessa frågor. Vid Karlstads universitet (KAU) finns Centrum för forskning om samhällsrisker, datavetenskap med fokus på informations- och cybersäkerhet, och Centrum för forskning om hållbar samhällsförändring utgör en viktig kunskaps- och forskningsresurs. KAU har 2022 startat ett nytt mastersprogram som erbjuder en specialisering för cybersäkerhet. Under våren 2023 startar Sveriges första företagsforskarskola inom cybersäkerhet vid Karlstads universitet. Inledningsvis kommer 8 doktorander att tillsammans med företag och seniora forskare utveckla cybersäkerhetslösningar för företag. I regionen finns även en stark närvaro av privat samhällsviktig verksamhet som Ellevio och Telia som har sina driftscentraler belägna här och företag som CGI Defence och Saab. KAU är också medlem i planeringsgruppen för Cybercampus Sweden.

1.3 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 kompetanse 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.

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

På bakgrunn av disse felles utfordringene 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).

1.5 Grenseoverskridende merverdi og motivering for Cross Border Cyber Capacity: Samarbeidet som støttefunksjon i et grenseoverskridende innovasjonssystem knyttet til cyber- og samfunnssikkerhet

Som nevnt i 1.2 og 1.3 har Innlandet og Värmland en rekke satsinger og kompetansemiljøer koplet til cyber- og samfunnssikkerhet. En viktig motivasjon og bakgrunn for en grenseoverskridende satsing er at vi gjennom Cross Border Cyber Capacity etablerer en koblingsarena for initiativer som utgjør spydspissene i våre regionale innovasjonssystemer knyttet til cyber- og samfunnssikkerhet, og til sammen utvikler et grenseoverskridende økosystem for cyber og samfunnssikkerhet. Dette illustreres i modell 2 under, etter en kort beskrivelse av utfyllende hovedsatsinger i begge regioner:

Innlandet har en rekke større pågående initiativer og satsinger koblet til cybersikkerhet som gjennom Cross Border Cyber Security bidrar inn i et grenseoverskridende innovasjonsøkosystem. Tre utvalgte hovedsatsinger er:

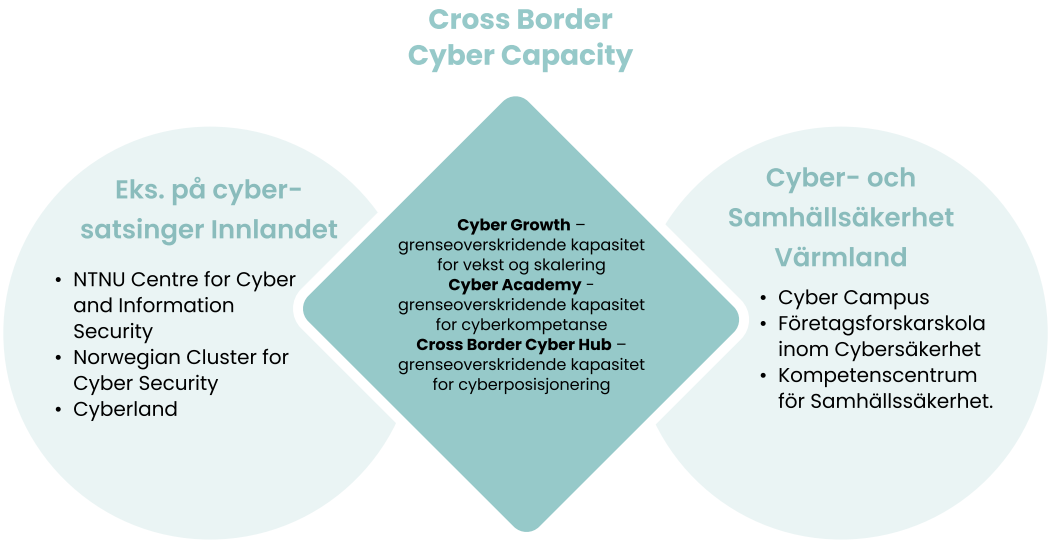
- Center for Cyber and Information Security (NTNU CCIS) er et nasjonalt senter for forskning, utdanning, testing, trening og kompetanseutvikling innen cyber- og informasjonssikkerhet ved NTNU. Senteret er et offentlig-privat, militært-sivilt og internasjonalt samarbeid med mer enn 75 nasjonale og internasjonale partnere.
- Norwegian Cluster for Cyber Security (NCCS) ble etablert i 2022 med Digital Innlandet som prosjekteier og operatør. NCCS er en næringsdrevet nasjonal klynge med regional forankring i Innlandet. Klyngen hadde ved etablering 19 næringspartnere i tillegg til NTNU, Fagskolen Innlandet og Vaager Innovasjon. NCCS utgjør et faglig komplett leveransesystem og en nasjonal kapasitet som er viktig for næringsliv, industri, offentlig sektor også i en totalforsvarssammenheng. Klyngens partnere leverer ledende produkter, teknologier, tjenester, utdanning og forskning.
- Cyberland er en regional satsing med mål om å utvikle Norges ledende økosystem innen cyber- og informasjonssikkerhet i Innlandet. Innlandet fylkeskommune, Gjøvikregionen Utvikling og Lillehammer-regionen Vekst står bak CyberLand, i samarbeid med Statsforvalteren i Innlandet, NTNU og Cyberforsvaret. NCCS har sitt utspring fra CyberLand.

Värmland har senaste tiden ett allt större fokus på Samhällsäkerhet och speciellt inom Cybersäkerhet. Verksamheten inom akademien har byggts upp under många år och här finns idag internationellt erkända forskare. I Värmland kan tre områden nämnas som starkt bidrar till uppbyggnaden av ett

regionalt kompetenscentrum för Samhällsäkerhet och även till ett gränsöverskridande innovationssytem.

- Karlstads universitet (KAU) är en del av **Cyber Campus** som bedriver agil spjutspetsforskning, utbildning och innovation inom cybersäkerhet som är avgörande för ökad motståndskraft och som går utöver vad som är möjligt för ett enskilt universitet, institut, myndighet eller företag.
- Karlstads universitet startar Sveriges första **Företagsforskarskola** inom Cybersäkerhet som har som syfte att höja kompetensen inom Cybersäkerhet för svenska företag.
- Karlstad kommun arbetar för att utveckla ett nationellt **Kompetenscentrum för Samhällssäkerhet.** Karlstad ligger väldigt bra placerad mellan Stockholm och Göteborg samt närheten till Norge. Samt att Karlstad har flera statliga myndigheter placerade här och en stark akademi.

Modell 2 – Interreg prosjektet Cross Border Cyber Capacity som koblingsarena mellom cyber- og samfunnsikkerhetsatsninger i Innlandet og Värmland



2. Mål, målgruppe og programrelevans

2.1 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.

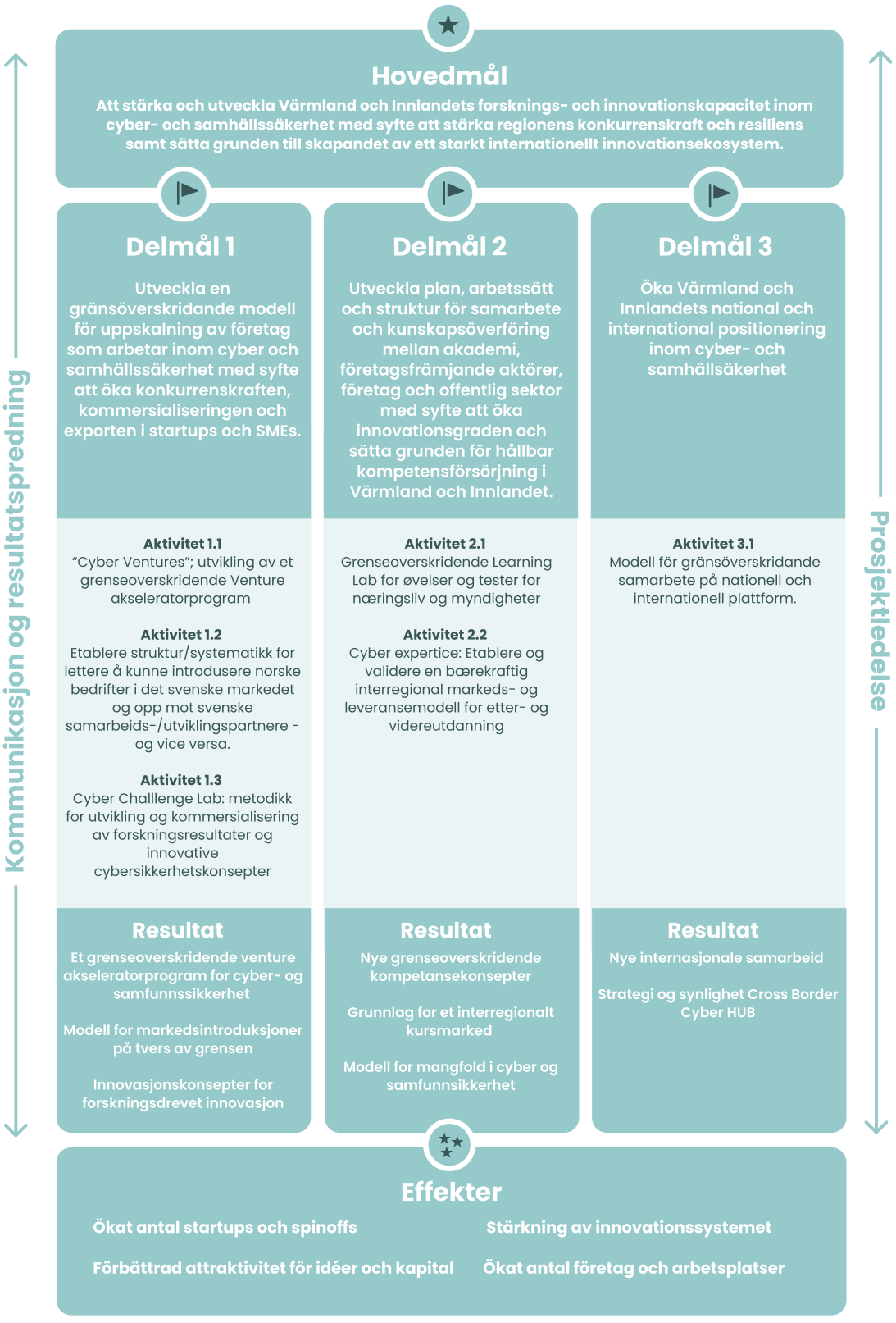
Delmål 2:

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



2.3 Programrelevans

Cross Border Cyber Capasity sine tre delmål bidrar till Interreg Sverige-Norges prioritering ”En smartare gränsregion” och specifikt mål ”Innovativa miljöer” genom att:

- Uppmuntra samarbete mellan akademi, företagsfrämjande aktörer och företag för att sammanföra spetsforskning och praktisk affärsutveckling.
- Främja gränsöverskridande utbyte av kunskap och expertis för att driva innovation och kompetensförsörjning inom områdena cyber- och samhälssäkerhet.
- Bygga nätverk som kopplar samman företag och akademi, skapa möjligheter för att dela information, utforska ny teknik och tillämpa avancerad teknik inom forskning och innovation.
- Främja användningen av avancerad teknologi för att förbättra processer och system inom områdena cyber- och samhällssäkerhet, vilket säkerställer fortsatt tillväxt och utveckling.

Nedanför beskrivs några konkreta exempel:

1. **Koppla affärsutveckling till forskning och innovation:** Delmål 1 syftar till att stärka grunden för affärsutveckling kopplat till cyber- och samhällssäkerhet. Detta kan uppnås genom att främja forskning och innovation inom dessa områden och ge nystartade företag det stöd som krävs för att lyckas på den globala marknaden.
2. **Underlättande av kunskapsflöde**: Delmål 2 fokuserar på att stärka tillgången till relevant expertis och skapa gränsöverskridande arenor för kunskapsflöde. Detta kan utnyttjas för att främja samarbete mellan akademin, företagsfrämjande aktörer och industrin, och för att uppmuntra överföring av avancerad teknologi, samt bidra till ökat kompetensförsörjning inom dessa två områden.
3. **Förbättra internationell positionering:** Delmål 3 syftar till att stärka nätverk och internationell positionering. Detta kan utnyttjas för att höja Värmlands och Innlandets profil och för att locka internationella partner att delta i forsknings- och innovationsaktiviteter. Genom att utnyttja internationella partnerskap kan vi få tillgång till en bredare pool av expertis och avancerad teknik, som kan användas för att vidareutveckla forsknings- och innovationskapaciteten samt öppna möjligheter för Värmlandska och Innlandska företag exportera sina tjänster och produkter.

2.4 Cross Border Cyber Capacity målgrupper

Målgrupper for Cross Border Cyber Capasity er:

Næringsliv: Etablerte og nye virksomheter i grenseregionen som enten leverer kompetanse, produkter, teknologi eller tjenester innenfor cyberdomenet eller som utgjør krevende brukermiljøer og avtaker av sikkerhetskompetanse og -løsninger. En hovedmålgruppe er bedrifter i Digital Innlandet, Norwegian Cyber Security Cluster (NCCS) og Compare, til sammen utgjør dette om lag sammen 200 bedrifter. Prosjektet Cross Border Cyber Capacity er initiert etter ønske fra næringslivet, og er godt forankret gjennom deltakelse i forprosjekt og prosjektutviklingsfasen gjennom workshops og dialog. Digital Innlandet, NCCS og Compare vil alle ha representanter i styringsgruppen for Cross Border Cyber Capasity (ref. 6.3 Styringsgruppe).

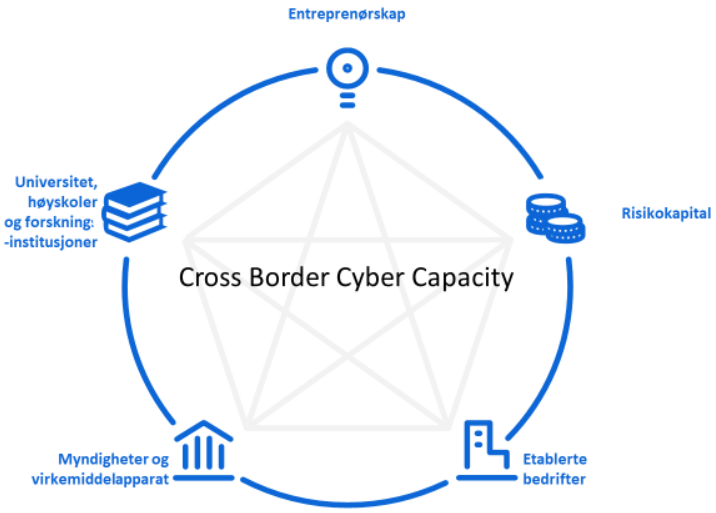
Myndigheter, virkemiddelapparat og kapital- og investeringsaktører, næringsstøtte: Myndigheter med strategisk og operativt ansvar for samfunnssikkerhet- og beredskap, ansvar for regional utvikling og næringsutvikling knyttet til regionenes cyberressurser, virksomheter som bidrar til å understøtte og muliggjøre satsing på cyber- og samfunnssikkerhet.

Forsknings- og utdanningsaktører: NTNU, HINN og Karlstad universet som partnere, Fagskolen Innlandet, Cyberingeniørskolen och Försvarshögskolan

Til sammen utgjør målgruppen ulike aktører i en Pentahelixmodell. Pentahelix er et verktøy för att strukturera intressentkartan, og ligger til grunn for prosjektet Cross Border Cyber Capacity. Komplexa samhällsproblem påverkar och påverkas ofta av flera olika sektorer. Deras lösningar uppstår därför även ofta i samverkan mellan aktörer i olika sektorer. Ofta består bristerna i nuvarande lösningar av brist på samverkan mellan olika sektorer, men även på grund av stuprör inom enskilda sektorer. Därför är det viktigt när man tar fram nya lösningar att man gör det genom dialog, samverkan och samarbete över de olika sektorsgränserna.

Samhället går att dela upp i olika sektorer. Tripple helix är ett väl etablerat begrepp kopplat till det traditionella innovationsbegreppet. Förenklat innebär det att de tre sektorerna Offentlig sektor, Privat sektor och Akademin ingår i innovationsprocessen. I Penta Helix ingår ytterligare två sektorer, alltså totalt fem. Där vi i detta projekt ser Entreprenörskap som en viktig del liksom tillgång till Riskkapital som är nödvändigt för innovationer. Pentahelixmodellen kan användas som ett stöd i arbetet med att identifiera relevanta individer och aktörer att involvera i sociala innovationsprocesser. Dels som en påminnelse för att tänka brett och få med alla olika sektorer, och dels som ett stöd när man strukturerar upp intressenter i t.ex. en intressentkarta.

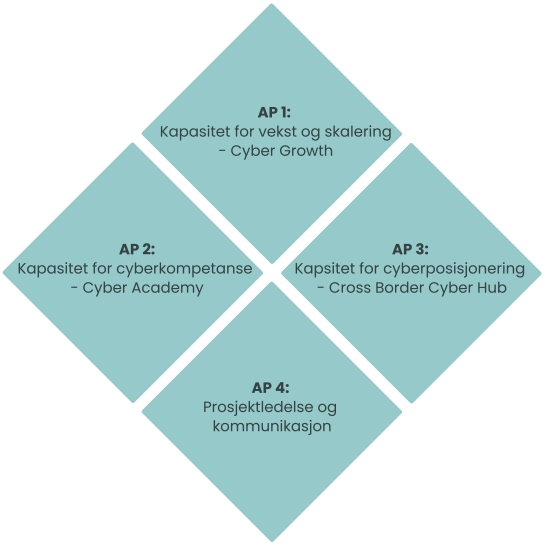
Modell 4: Pentahelix som grunnlag for Cross Border Cyber Capacity



3. Aktiviteter

Prosjektet gjennomføres innenfor rammen av 4 arbeidspakker / hovedaktiviteter, med kopling til hver av prosjektets delmål.

Modell 4: Oversikt Cross Border Cyber Capasity arbeidspakker



3.1. Arbetspaket /hovedaktivitet 1: Kapacitet för tillväxt och skalning – Cyber Growth

Mål:

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

Leder: Compare och Vaager Innovasjon

Övergripande beskrivning:

Arbetspaketet handlar om att lägga grunden för att nya verksamheter, etablerade verksamheter och innovativa koncept/lösningar ska få en stärkt förmåga att lyckas på en global marknad genom interregionalt samarbete. Arbetspaketet består av tre huvudaktiviteter: i) Utveckling och implementering av ett gränsöverskridande venture acceleratorprogram för cyber och samhällssäkerhet; ii) Etablera ett system för företags- och marknadsintroduktion i Sverige och Norge; iii) Cyber Challenge Lab - Utveckling/anpassning och testning av modeller och metodik för utveckling och kommersialisering av forskningsresultat och innovativa cyber- och samhällssäkerhetskoncept och lösningar.

Aktivitet 3.1.1: "Cyber Ventures" - utveckling av ett gränsöverskridande acceleratorsprogram

Programmet kommer att utvecklas genom att bygga vidare på Compares erfarenhet av etablering och utveckling av "Digital Well Ventures" (en accelerator inom hälsoområdet). Detta kommer att kopplas till Vaager Innovation och NTNUs initiativ och erfarenheter från arbete med kommersialisering av forskningsresultat och idéer, samt forskning inom cyberdomänen.

Cyber Ventures kommer att vara en accelerator i Sverige och Norge. Målgruppen är företag som utvecklar och levererar produkter, teknologier eller tjänster inom samhällssäkerhet- och cyberdomänen. I erbjudandet kommer vi att fokusera på att öka företagens evne til forretningsutvikling, investeringsberedskap, förbereda verksamheter för skalning, pitchutbildning och skapa arenor för interregional pitching för investerare.

Genomförande:

- Etablering av en representativ och professionell struktur för genomförande
- Erfarenhetsutbyte och modellöverföring mellan Compare och Vaager Innovation
- Genomföra en behovskartläggning av näringslivsaktörer och investeringsmiljöer på svensk och norsk sida

- Att lära sig av liknande modeller/anläggningar - speciellt "Digital Well Ventures" och eventuellt andra internationella referenssatsningar
- Tillsammans med näringslivsaktörer och investeringsmiljöer på svensk och norsk sida utforma en kravspecifikation
- Utveckla koncept, modell och metodik – utifrån krav och benchmark
- Marknadsföring/rekrytering av verksamheter/case och investeringsmiljöer gällande pilotering
- Implementera modell/föreläsningar/event för et antal verksamhet-/innovationscase, inkl. spesielle events for å sikre “equial opportunites” for minoritetsgrupper
- Utvärdera modellen
- Utvikling av Female Focus concept for hackaton
- Produktifisering av kapaciteten och etablering av en slutgiltig och robust modell/struktur/organisation för fortsatt drift efter projektets slut

Aktivitet 3.1.2 Etablera struktur/systematik för att lättare introducera norska företag på den svenska marknaden och till svenska samarbets-/utvecklingspartners - och vice versa

- Modellutveckling och gränsöverskridande B2B

Aktivitet 3.1.3 Cyber Challenge Lab - metodik för utveckling och kommersialisering av forskningsresultat och innovativa samhälls- och cybersäkerhetskoncept

Cyber Challenge Lab riktar sig till företag (etablerade och nya) som vill utforska nya idéer och ämnes-/marknadsområden tillsammans med gränsöverskridande forskarteam med avsikt att utveckla koncept vidare i en tvärvetenskaplig samverkan. Detta kommer att ske genom så kallade sprints och workshops utifrån en konkret utmaning definierad av deltagarna.

Genomförande:

- Etablering av en representativ och professionell struktur för implementering
- Erfarenhetsutbyte mellan partners på norsk och svensk sida
- Genomföra en behovskartläggning av forsknings- och näringslivsaktörer på svensk och norsk sida
- Lärande av liknande modeller/strukturer i Danmark (Cyber HUB) och eventuellt andra internationella referensinsatser
- Tillsammans med näringslivsaktörer på svensk och norsk sida utforma en kravspecifikation, inkl. diversitet knyttet til kjønn og etnisitet hos deltagerne
- Utveckla modell och metodik - baserat på kravspecifikation och benchmark
- Marknadsföring/rekrytering av research och business case för pilotering
- Implementera modell/process för antal utvecklingscase (pilotering)
- Utvärdera modellen
- Produktifisering av kapaciteten och etablering av en slutgiltig och robust modell/struktur/organisation för fortsatt drift efter projektets slut

3.2. Arbeidspakke / hovedaktivitet 2: Kapasitet for cyberkompetanse – Cyber Academy

Mål: 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.
Leder: KAU og NTNU
Overordnet beskrivelse:

Arbeidspakken dreier seg om å lage arenaer for kompetanseflyt mellom akademia og næringsliv, og trekke veksler på komplementære fagmiljøer innen cyber- og samfunnssikkerhet ved NTNU, HINN og KAU samt testfasiliteter knyttet til disse kompetansemiljøene, for å bygge kompetanse som grunnlag for motstandsdyktighet og grunnlag for nye løsninger og konsepter. Arbeidspakken består av to hovedaktiviteter: i) Grenseoverskridende Learning Lab for øvelser og tester for næringsliv og myndigheter ii) Etablere og validere en bærekraftig interregional markeds- og leveransemodell for etter- og videreutdanning

Aktivitet 3.2.1 Grenseoverskridende Learning Lab for øvelser og tester for næringsliv og myndigheter

Gjennom aktiviteten utnyttes komplementær kompetanse i Innlandet og Värmland, samt infrastruktur og utviklede øvingskonsepter til et forsterket tilbud til næringsliv og myndigheter.

Gjennomføring:

- Gjennomføring av en interregional behovskartlegging hos næringsliv og offentlige aktører knyttet til øving og testing
- Avgrensning og utvikling av en plattform for felles interregional kapasitet for øving og testing på samfunns-, bedrifts- og produktnivå
- Pilotering av foreløpig felles øvings-/testkapasitet
- Utvikling og organisering av felles modeller, øvings-/testscenarier og –manualer, inkl. utvikling av Female Focus concept
- Produktifisering av kapasiteten og etablering av endelig og robust modell/struktur/ organisering for operasjonell videreføring etter prosjektets slutt. Plattformen skal danne utgangspunkt for videreutvikling mot en "Nordic Cyber Range"

Aktivitet 3.2.2 Cyber Expertice - etablere og validere en bærekraftig interregional markeds- og leveransemodell for etter- og videreutdanning

Behovet for kompetansetilbud og utdanninger knyttet til cyber- og samfunnssikkerhet er stort. Denne arbeidspakken skal adressere behov for ny innsikt og kunnskap, og legge til rette for god formidling til næringslivet. Et eksempel på et aktuelt felt er OT-sikkerhet (operasjonell teknologi). Arbeidet skal legge grunnlag for et interregionalt kursmarked for nasjonale kompetanseaktører.

Gjennomføring:

- Gjennomføring av behovs- og ressurskartlegging - med utgangspunkt i regionens næringsliv (Digital Innlandet, NCCS, Compare m.fl.)
- Identifisering av nasjonale infrastrukturelementer som kan videreutvikles i fellesskap
- Utvikling, pilotering og evaluering av felles tilbud rettet mot næringsliv og offentlig sektor med fokus på økning av kvinnlig representation
- Produktifisering og etablering av endelig og robust modell/struktur/organisering for operasjonell videreføring etter prosjektets slutt
- Utvikling, pilotering og evaluering av et grenseoverskridende kompetansetilbud rettet mot startups fra minoritetsmiljøer. Tilbudet baseres på tilsvarende nasjonale referansekonsepter/-tilbud

3.3. Arbeidspakke / hovedaktivitet 3: Kapasitet for cyberposisjonering – Cross Border Cyber Hub

Mål:

Öka Värmland och Innlandets national och international positionering (och nätverk) inom cyber- och samhällsäkerhet
Leder: Compare og Digital Innlandet
Overordnet beskrivelse: Arbeidspakken dreier seg om å bygge kapasitet for strategisk samarbeid for videreutvikling av cybersatsingene, samt felles posisjonering nasjonalt og internasjonalt. Arbeidspakken skal etablere en plattform for nettverksutvikling og strategisk posisjonering av grenseregionen som ett komplett nordisk økosystem innenfor cyber- og samfunnssikkerhet. Gjennom aktivitetene i arbeidspakken kobles kompetanse og ressurser fra Innlandet og Värmland for felles læring/erfaringsutveksling, posisjonering og synlighet. Arbeidspakken består av hovedaktiviteten utvikling av en modell för gränsöverskridande samarbete på nationell och internationell plattform.
Aktivitet 3.3.1 Modell för gränsöverskridande samarbete på nationell och internationell plattform. Med utgangspunkt i komplementære ressurser, miljøer og nettverk vil prosjektet gjennom arbeidspakken jobbe frem en systematisk modell for nasjonal og internasjonal posisjonering. Gjennomføring: • Kartlegging og mobilisering av aktører innen samfunns-/cybersikkerhet i Värmland • Samarbeid om utvidelse av eksisterende events, møteplasser og konferanser innen cyber- og samfunnssikkerhet på tvers av grensen og inkl. kvinnenettverk (eks. Security Divas) • Konseptutvikling «Cross Border Cyber Hub» gjennom utforming av policynotat rettet mot regionale og nasjonale beslutningstakere og prosjektpartnerne selv. Policynotatet vil inneholde faglige anbefalinger for videre strategiske satsinger, og hvordan næringen selv og et tettere privat-offentlig grenseregionalt samarbeid kan bidra til økt posisjonering og samarbeid mellom grenseregionen, EU og internasjonale cyberklynger. • Koblingsarenaer i Brussel og strategisk samarbeid mot internasjonale cyber klynger. • Strategiutforming og synlighet Cross Border Cyber HUB • Internasjonal posisjonering for skalering og vekst og nettverksbygging og utvikling av europeiske partnerskap – og se til Horizon Europa/Digital Europa/EDIH

3.4. Arbetspaket / hovedaktivitet 4: Projektledning och kommunikation

Mål: Säkerställa god samordning av projektet, god ekonomistyrning samt intern och extern kommunikation och spridning.
Leder: Compare och Digital Innlandet
Övergripande beskrivning: Genom strategisk projektledning ska arbetspaketet säkerställa en god samordning av projektet, god ekonomistyrning samt intern och extern kommunikation och spridning.
Aktiviteter: • Leda och fördela arbetet – kalla till och planera projektgruppsmöten och styrgruppsmöten • Samordna aktiviteter över arbetspaket • Rapportering och dialog Interregsekretariatet • Dialog med samarbetspartners och externa aktörer • Budgethantering • Utarbeta en kommunikationsplan, leda och samordna kommunikationsaktiviteter • Kommunicera och förankra mål och visioner i projektorganisation och kluster • Mobilisera för deltagande • Sprida och dela resultat regionalt, nationellt och internationellt

Mer detaljerad beskrivning av några av punkterna, se del 6.

4. 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.

5. Horisontella kriterier och hållbarhet

Cross Border Cyber Capacity stödjer arbetet mot de globala hållbarhetsmålen i Agenda 2030/**Sustainable Development Goals (SDG)**, med specifikt långsiktig fokus på Mål 5 Jämställdhet; Mål 8 Anständiga arbetsvillkor och ekonomisk tillväxt; Mål 9 Hållbar industri, innovationer och infrastruktur; Mål 10 Minskad ojämlikhet; Mål 12 Hållbar konsumtion och produktion; samt Mål 13

Bekämpa klimatförändringarna. Alla medsökande og prosjektpartnere har erfarenhet av att driva projekt med hållbarhetsperspektiv och vi kommer att fortsätta följa upparbetade rutiner.

Enligt Eurostat var andelen kvinnor i chefspositioner i EU under 2020 mindre än 30 procent och teknikbranschen, specifikt cybersäkerhet, är ännu mindre jämställd. Vi behöver attrahera fler kvinnor och öka mångfalden i rekryteringsbasen och för det behövs det riktade insatser för kvinnor. Cross Border Cyber Capacity arbetar med att **förbättra jämställdheten** genom att involvera kvinnliga experter i projektets genomförande och beslutsfattande (Mål 5.5). Vi strävar efter att uppnå en jämn fördelning mellan män och kvinnor både i ledande ställning och i arbetet som utförs. Genom att projektets aktiviteter är så nära knutna till varandra mellan arbetspaketen, samt genom kontinuerliga gemensamma avstämningar kommer projektets olika perspektiv att få en jämn och balanserad maktfördelning och inflytande (Mål 5.5). Cross Border Cyber Capacity kommer att ha en kvinnlig projektledare (både på svensk och norsk sida) som kommer att sammankalla och utforma styrgrupp och projektgrupp, samt AP-grupper (Mål 5.5.). Projektets styrgrupp kommer att ha representanter från projektägarnas organisationer och det vil etterstrebes en könsmässig jämn fördeling (Mål 5.5. och Mål 10.2). Projektet och dess AP är konstruerade för att skapa samverkan och teamarbete för att säkerställa att alla får tillgång till relevant information och kunskap men också minska risken att vissa uppgifter utförs där vissa grupperingar får större inflyttande (Mål 10.2). Ett av våra långsiktiga mål är att hitta hållbara koncept och metoder för att säkra en bredare bas med fler entreprenörer som är kvinnor; främja nyetablerade företag med jämställda team; och att den teknik som utvecklas ska vara jämlik och inkluderande (Mål 5 och Mål 10). Genom att erbjuda träning inför t.ex. cyberchallenges med endast kvinnliga grupper (AP2) ger vi möjlighet till flera kvinnor att ta plats och utforska sina förmågor samt bygga självförtroende i sina kunskaper för att i nästa steg vara en aktiv part i en blandad gruppering (Mål 5.1).

Att **uppmuntra entreprenörskap** är nyckeln till att uppnå Mål 8 i SDG. Genom att stödja och hjälpa nya företag att utvecklas och skala upp sina erbjudanden (AP1) bidrar vi till skapandet långvariga jobb i regionen (Mål 8.2). När nystartade företag mognar och växer skapar de nya jobbmöjligheter (Mål 8.3). Detta gynnar samhällen och driver ekonomisk tillväxt (Mål 8.1). Nya och förbättrade produkter, tjänster eller teknik från entreprenörer som tar hänsyn till hållbarhetaspekterna (som blir en del av acceleratorprogrammet som kommer att byggas i AP1) gör det möjligt att utveckla nya marknader och skapa nytt välstånd (Mål 8.4; 12.6 och 13.3). Dessutom bidrar ökad sysselsättning och högre inkomster till bättre nationalinkomst i form av högre skatteintäkter och högre offentliga utgifter (Mål 8.1). Genom att flera lösningar prövas och flera frågor diskuteras tillsammans med olika aktörer, som till ex. i ”Challenge labs” (AP1) bidrar Cross Border Cyber Capacity till Mål 9.1 och 9.5. Dessutom tror vi att genom samarbete med offentliga organisationer kan Cross Border Cyber Capacity leda till förbättrad policy och beslutsfattande inom den offentliga sektorn (Mål 9.1). Om vi kan sprida kunskapen till flera aktörer har detta potential att förändra hur vi ser på innovation och finansiering av innovationsaktiviteter där offentlig sektor kan vara en drivande del i innovationsprocessen (Mål 9.1).

Genom innovation och digitalisering kan vi göra nödvändiga förändringar för att skydda planeten genom att modernisera och säkra våra infrastrukturer (Mål 13). Vi ser Cross Border Cyber Capacity som en möjlighet att adressera och integrera ovannämnda hållbarhetsperspektiven både på långt sikt och i arbetet som utförs under projektets gång. Flera möten inom projektet kommer ske digitalt och men även fysiska möten kommer att planeras så hållbart som möjligt. Alla medsökande og prosjektpartnere har en hållbarhetspolicy och kommer att använda kollektivtrafik där det är möjligt samt samåka vid tillfällen där kollektivtrafik inte är ett alternativ. I våra aktiviteter kommer vi att diskutera hur perspektiven kan integreras i verksamheter, utbildningar, trainings samt hur kan vi ställa krav på och hjälpa nya företag att tänka hållbart redan från början (Mål 13.3).

6. Organisering og partnerskap

6.1 Prosjekteiere

Compare er svensk prosjekteier og Digital Innlandet norsk prosjekteier i Cross Border Cyber Capacity.

Compare är ett techinnovationskluster som samlar företag, organisationer och individer som tillsammans och långsiktigt vill utveckla Värmland och lösa samhällets utmaningar med hjälp av framtidsinriktad digital teknik. Kopplat till Compare finns över 100 digitala företag som tillsammans har en omfattande kompetens för utveckling och realisering av digitalisering och digitala tjänster. Compare har kompetens att driva komplexa frågor och projekt inom digitala lösningar, samt arbetar med att stärka företag att utveckla digitala tjänster, kommunikation och kunskapsspridning. Här samlas spetskompetens inom projektledning, test, tjänstedesign, hållbarhet och policyfrågor. Compare är delägare av en internationell spetsaccelerator - DigitalWell Ventures som hjälper företag att attrahera kapital och skala upp sina tjänster. Inkubatorn DigitalWell Govtech Incubator fokuserar på att stödja företag för samarbete med offentlig sektor. Digitalisering av hälsotjänster har en stark koppling till Karlstads universitet. Compare är också en part i ett av Sveriges officiella Europeiska Digitala innovationshubbar (EDIH). Hubben kopplar samman 17 partners från hela Sverige och erbjuder tjänster inom hälsodata, AI, IoT, och relaterade områden till både SME och offentlig sektor. EDIH konsortiet har en stark historia av samverkan både på den nationella och europeiska arenan. Compare är också processledare för vinnväxtsatsningen Digital Well Arena.

Digital Innlandet er et nettverk bestående av nærmere 70 virksomheter som utgjør et sterkt kompetansemiljø innen digitalisering og digital transformasjon på tvers av medlemsbedriftene. Nettverket skal bidra til et digitaliseringsløft for Innlandet gjennom kunnskapsdeling og prosjektutvikling, og gjøre det enkelt for andre å få tilgang til den kunnskapen og det nettverket de trenger for å kunne utnytte de mulighetene digital teknologi gir. Digital Innlandet skal styrke oppmerksomheten rundt digital omstilling og innovasjon i regionen, og bidra til at Innlandet blir en attraktiv digital region, hvor flere personer og bedrifter med digital kompetanse etablerer seg.

Prosjektet det «The Norwegian Cluster for Cyber Security» (NCCS) ble etablert i 2022 med Digital Innlandet som prosjekteier og operatør. NCCS er en næringsdrevet nasjonal klynge med regional forankring i Innlandet. Klyngen hadde ved etablering 19 næringspartnere i tillegg til NTNU, Fagskolen Innlandet og Vaager Innovasjon. Det føres dialog med ytterligere 12 partnere med tanke på opptak første kvartal 2023.

NCCS utgjør et faglig komplett leveransesystem og en nasjonal kapasitet som er viktig for næringsliv, industri, offentlig sektor og i totalforsvarssammenheng. Klyngens partnere leverer ledende produkter, teknologier, tjenester, utdanning og forskning.

6.2 Prosjektpartnere / medsøkande

Karlstads Universitet (KAU) omfattar nationellt och internationellt profilerade forskargrupper inom områdena cybersäkerhet och integritet, krishantering och riskhantering och samhällsrisker/samhällsrisk vid KAU:s två fakulteter (Fakulteten för hälsa, natur- och teknikvetenskap & Fakulteten för humaniora och samhällsvetenskap).

PriSec (Privacy & Security)-gruppen vid datavetenskaps har varit aktiv inom utbildning och forskning inom cybersäkerhet i mer än 25 år. Det erbjuder flera grundkurser, MOOCs och ett masterprogram med inriktning mot cybersäkerhet och integritet, inklusive praktiska kurser i etisk hacking. Den samordnar svenska industriforskarskolan för Cybersäkerhet (SIGS-CyberSec), finansierad av KKS, med deltagande av 8 svenska företag och andra svenska universitet. KAUotic hacking club är en etisk

hackargrupp bildad av forskare och studenter vid KAU som regelbundet tränar och deltar i cyberchallenges och Capture the Flag-tävlingar.

Prisec har dessutom varit aktivt involverad som partner och koordinator i fem cybersäkerhetsprojekt inom EU H2020, samt flera nationella cybersäkerhetsforskningsprojekt finansierade av SSF, KKS, Vinnova med flera, i nära samarbete med svenska och europeiska företag. Den samordnar det svenska IT-säkerhetsnätverket för doktorander och forskare (SWITS - https://sola.kau.se/swits/), finansierat av MSB, och är en av planeringsgruppens medlemmar i Cybercampus Sweden-initiativet (cybercampus.se). Dessutom är PriSec-medlemmar aktiva som experter inom MSB:s cybersäkerhetsråd och arbetsgrupper av ENISA (European Cybersecurity Agency), och styrelseledamot i Cybernode Sweden (den svenska noden för att accelerera innovation och forskning inom cybersäkerhet – cybernode.se).

Karlstads kommun har över 96 000 invånare och det bor 150 000 i Karlstadsregionen. I kommunen finns ett universitet som har ca 75 olika program, i kommunen finns även försvarshögskolan. 2017 fick Karlstads kommun en politisk motion som handlade om att stärka Karlstads förmåga inom samhällssäkerhet. Efter det så arbetar Karlstad efter att uppnå en position inom området inte bara regionalt utan även nationellt och internationellt. Det handlar om att kommunen vill bidra till hela Sveriges totalförsvar på olika sätt bland annat genom att förse Sverige med kompetens. Detta bidrar även till att stärka platsens egen arbetsmarknad och myndigheterna här, då det finns flera statliga myndigheter i Karlstad så som Myndigheten för psykologiskt förvar, Myndigheten för samhällsskydd och beredskap samt Plikt- och prövningsverket. Karlstadsregionen har även en räddningstjänst där 6 närliggande kommuner samverkar. Räddningstjänsten har mycket kunskap och erfarenheter kring samhällssäkerhet. Vi ser också ett stort värde av ett samarbete med Norge utifrån Sveriges kommande medlemskap i NATO.

NTNU - ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi (IIK). Instituttet ligger ved Fakultet for informasjonsteknologi og elektroteknikk. Instituttet driver med forskning, utdanning og innovasjon innen cybersikkerhet, informasjonssikkerhet, kommunikasjonsnettverk og nettverkstjenester. Instituttet tilbyr studieprogram på doktor-, master-, og bachelorgradsnivå innen informasjonssikkerhet og kommunikasjonsteknologi. Det er ca. 130 årsverk ved instituttet fordelt på to lokasjoner, Gjøvik og Trondheim, 1000 studenter og 75 PhD-stipendiater.

Instituttet er også vertskap for Center for Cyber and Information Security (CCIS), SFI Norwegian Centre for Cyber Security in Critical Sectors (NORCICS) og Norges nasjonale forskerskole innen data og informasjonssikkerhet (COINS).

Høgskolen i Lillehammer (HINN) er en høyere utdanningsinstitusjon med rundt 1200 ansatte og 16000 studenter fordelt over åtte lokasjoner i Innlandet fylke. Institutt for organisasjon, ledelse og styring tilbyr bachelor- og masterstudier i beredskap og krisehåndtering på lærested Rena, og er en av Norges ledende miljøer på beredskapstrening. Åpningen av Senter for Ledertrening på Rena (SLTR) høsten 2023 vil ytterligere styrke utdanningen og videreutviklinga av beredskapstrening. Integrasjon cybersikkerhetsrelaterte kriser i beredskapstreningen vil være en av flere satsingsområder for det nye senteret.

Vaager Innovasjon er et flerfunksjonelt innovasjonsselskap som både jobber med oppstartsbedrifter (start-ups) og etablerte virksomheter. Selskapet har i dag ni ansatte og i 2022 en omsetning på omtrent 15MNOK. Cyber- og informasjonssikkerhet er et faglig kjerneområde, Vaager jobber systematisk med å kommersialisere cyber- og informasjonssikkerhetsselskaper og integrert dette i arrangementer som eksempelvis den årlige idéakseleratoren Boost It og akseleratorprogrammet KLP Trykktanken Cyber i

samarbeid med CoFounder. Sammen med NTNU er Vaager grunnleggende medlemmer av Norsk Senter for Informasjonssikring (NorSIS) som driver råd og veiledning til innbyggere og SMBer.

Som oversikten viser, består partnerskapet i Cross Border Cyber Capacity av tunge regionale kompetansemiljøer. Bland prosjektpartnere/medsökande partners finns det bred och mångårig erfarenhet av att utveckla, genomföra och administrera projekt. Detta gäller såväl regionala och nationella satsningar som internationella. Med tanke på de olika profilerna och kompetensområdena har gruppen som helhet potential att skapa ett dynamiskt och omfattande ekosystem där varje partner använder sin expertis och signa nätverk för att dela bästa praxis och kunskap men också bidra till utvecklingen av metoder och arbetssätt.

6.3 Organisering og ledelse av Cross Border Cyber Capacity

Cross Border Cyber Capacity är ett samverkansprojekt där projektägarna på norsk och svensk sida kommer att ha det övergripande ansvaret för att säkerställa att projektplanen (se avsnitt 3) följs och att projektets leveranser levereras i linje med tidsplanen. Projektägarna kommer att ha en tydlig uppdelning kring sina ansvarsområden och uppföljning av respektive arbetspaket, dock kommer samtliga AP genomföras genom aktiv samverkan mellan medsökande parter.

Huvudgrupperingarna i projektet är styrgruppen och projektgruppen. Styrgruppen är ett överordnat organ till vilken projektledarna rapporterar, medan projektgruppen övervakar och utför de dagliga praktiska uppgifter.

Styrgrupp

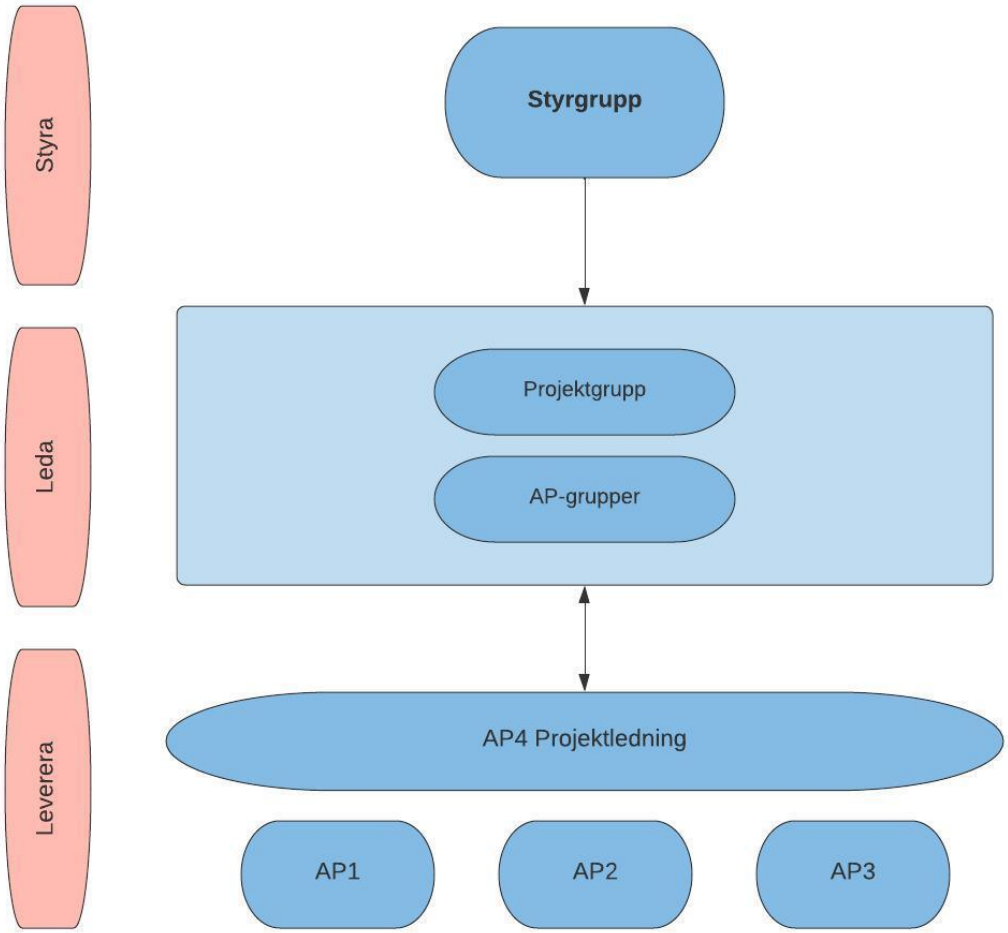
Projektgruppen kommer att tillsätta en styrgrupp med representanter från pentahelix strukturen och från projektdeltagarnas organisationer. Fra norsk side vil representant fra Digital Innlandet, NCCS, NTNU, HINN og Vaager Innovasjon delta. På den svenska sidan kommer projeketets parter delta, men även representanter från Länsstyrelsen i Värmland och Myndigheten för Samhällsskydd och Beredskap (MSB). Alla i styrgruppen har rösträtt i styrgruppens beslut. Styrgruppen kommer att diskutera övervakning och kontroll av projektet; kommunikation och spridning av resultat; kvalitetssäkring; verifiera uppnådda mål; kontrollera avvikelser; budget; konfliktlösning; etc. Styrgruppen sammanträder fyra gånger per år och projektledaren är sammankallande för styrgruppen. Innlandet fylkeskommune og Region Värmland tilbys en observatørrolle i styringsgruppen.

Projektgrupp

Projektgruppen säkerställer en effektiv operativ ledning av alla projektaktiviteter, dagliga samordningsuppgifter och övervakar projektets budget och framsteg, inklusive uppföljning av arbetsplan och indikatorer. Projektgruppen innefattar en norsk och svensk projektledare samt en representant från varje medsökande part/samarbeidspartner. Projektledaren har ledande roll i projektgruppen. Möten kommer att hållas varannan vecka eller oftare vid behov.

AP-grupper

Til hver arbeidspakke etableres operative gruppering som består av relevanta aktörer från partners och leds av AP-ledare (se avsnitt 3). Målene med gruppene er å samverke slik at aktiviteter utføres med relevanta aktörer.



Modell 5: Prosjektorganisering Cross Border Cyber Capacity

Styringskapasitet hos prosjektledelsen

Genom ovannämnda nätverk har **Compare** tillgång till stor bas av expertkompetens inom digitalisering, tech och hållbarhet. Compare har tex. specifikt utsedda coacher med syfte att utveckla och ta vara på det strategiska lärandet utifrån ett hållbarhetsperspektiv. Vi har stor erfarenhet av att leda, genomföra och redovisa projekt oc följa upp satsningarnas mål och indikatorer. Compare har en egen ekonomiavdelning, som i dagsläget hanterar ca. 15 projekt hos bland annat Tillväxtverket, Interreg, Vinnova och ESF. Compares ekonomiavdelning, med Controller i spetsen, är mycket väl insatta i regelverk och har god kunskap om vilka kostnader som är stödberättigade. Vi har en av styrelsen beslutad attestordning, som styr vilka som får godkänna och attestera kostnader för ett visst projekt och vi har också regelbundna uppföljningar där vi kontrollerar att kostnader betalas i tid och att dom är bokförda på rätt projekt. Projektet särredovisas i bokföringen med hjälp av eget projektnummer, egen resultaträkning och egen huvudbok. Personalens faktiska lönekostnader fördelas ut på projekten månadsvis, enligt den tjänstgöringsgrad som personen har i det aktuella projektet.

Cross Border Cyber Capacity har tre svenska partner – Compare, Karlstads kommun och Karlstads universitet. Den svenska delen av partnerskapet har stor erfarenhet av att arbeta tillsammans och vi

har redan inarbetade ruiner för rapportering, gör löpande likviditets-prognoser för att säkerställa att vi hela tiden har en stabil likviditet i verksamheten och vi har en bankkredit på två miljoner, som vi glädjande nog aldrig behövt utnyttja. Likviditeten säkerställs också framför allt genom att vi har några större projekt, bland annat ett tioårigt Vinnväxtinitiativ (hos Vinnova), som genererar stora utbetalningar varje kvartal. Vi har också en basfinansiering på 2,6 Mkr per år från Region Värmland, som utbetalas med 1/12 varje månad.

Digital Innlandet har 5 ansatte med lang og bred kompetanse innen prosjektutvikling- og ledelse, nettverks- og klyngeutvikling, strategisk posisjonering og kommunikasjon. De ansatte har faglig legitimitet innen digitalisering, IT og cybersikkerhet, og innehar inngående kjennskap til nøkkelaktører i økosystemet innen cybersikkerhet lokalt og nasjonalt.

Digital Innlandet er et regionalt nettverk organisert som en forening eid av medlemmene. Blant disse finner vi noen av Innlandets største og mest solide selskaper (som for eksempel Eidsiva-konsernet, Norsk Tipping og Sparebank 1 Østlandet). Størstedelen av inntektene kommer fra prosjekter, men nettverket har i tillegg en meget god medfinansiering fra medlemmene.

Digital Innlandet er eier og vertsorganisasjon for prosjektet The Norwegian Cluster for Cyber Security (NCCS) som er en vesentlig næringssatsing i Innlandet. NCCS er organisert som et definert prosjekt, med egne partnere, egen styringsgruppe og eget prosjektregnskap. Partnerne legger et vesentlig ressursmessig bidrag inn i klyngeprosjektet.

I tillegg til Digital Innlandet er NTNU og Vaager arbeidspakkeledere på norsk side og inngår i prosjektteamet. Aktørene er etablerte samarbeidspartnere, bl.a. gjennom NCCS, og struktur for prosjektsamarbeid, rutiner for rapportering m.m. er allerede etablert. I tillegg er HINN og NCCS med som partnere på norsk side.

Digital Innlandet er en forholdsvis liten virksomhet med en oversiktlig økonomi. En fast, ekstern regnskapsressurs er tilknyttet foreningen, og det avholdes ukentlige møter med denne. Rapportering på prognose opp mot budsjett og soliditet er faste saker på agendaen i styremøtene. Foreningen er solid, men har en bankkreditt på 1 mill NOK i Sparebank 1 Østlandet.

7. Kommunikasjon, resultatspredning og evaluering

7.1 Kommunikasjon

Cross Border Cyber Capasity kommer att använda kommunikations- och spridningsaktiviteter som verktyg för att maximera projektets effekt. Under första etappen kommer att fokuseras på att synliggöra projektet med målet att skapa en bas av intresserade parter i projektet. Denna fas kommer att löpa under hela projektperioden. Den andra etappen kommer att fokusera på att säkerställa hållbarheten för projektets resultat genom skapandet av en exploateringsstrategi. För att säkerställa att projektet synliggörs kommer vi utföra ett antal aktiviteter och kanaler:

Grafisk profil: För att stödja spridningsaktiviteterna och skapa igenkänning kommer logotyp; mallar för presentationer och dokument (f.eks. posters; infoblad och broschyrer) utvecklas. Stor del av materialen kommer att produceras i digitalform för att minska klimatpåverkan och spara resurser.

Webbplats: En särskild webbplats kommer att lanseras där regelbundet kommer att finnas information kring projektets progress. Webbplatsen är projektets huvudsakliga och centrala kommunikationsnav och anses vara rätt kanal för att nå alla intressenter och för att kommunicera projektens resultat och aktiviteter regelbundet i enlighet med dess framsteg.

Sociala nätverk: Projektägarna kommer att använda våra upparbetade befintliga kanaler för att sprida information om projektet till allmänheten. Medsökande partners og samarbeidspartnere kommer också att använda sina organisationers befintliga kanaler för att sprida resultat och information. Sociala nätverk kommer att användas för att flankera spridningsinsatser för att nå en bredare publik och att underlätta dialogen med relevanta intressenter.

Nyhetsbrev: Ett periodiskt nyhetsbrev kommer att släppas med information kring projektet.

Akademiska/vetenskapliga publikationer: Alla akademiska partners kommer att uppmuntras till att publicera projektresultaten i form av rapporter och presentera dem vid relevanta konferenser.

Konferenser och evenemang: Projektets aktiviteter och resultat kommer att kommuniceras på relevanta internationella, nationella och regionala konferenser och evenemang.

Workshops och seminarier: Cross Border Cyber Capacity kommer att anordna workshops/seminarier för att öka synligheten av projektets progress och resultat.

Interregs logotyp kommer att synliggöras på varje kommunikationsmaterial.

Målgrupperna är olika i sin natur och ska därför nås genom olika kanaler och aktiviteter. De mest lämpliga kanalerna väljs ut för att nå varje målgrupp.

Målgrupp	Kommuikations kanal
SME	Befintliga nätverk; sociala nätverk
Beslutsfattare, myndigheter	Direkt kontakt; kongresser
Allmänhet	Sociala nätverk; websida; pressmeddelande
Forskare /Akademiker	Pressmeddelande; nyhetsbrev; publikationer, konferanser
Blandade intressentgrupper	Konferenser; event; websida

Tabell 1: Oversikt over målgrupper og kommunikasjonskanal Cross Border Cyber Capacity

7.2. Resultatspridning

Syftet med resultatspridningen är att förstärka de socioekonomiska effekterna av projektet och dess resultat. Vi kommer att säkerställa det genom att skapa medvetenhet och kommunikation kring projektets aktiviteter och resultat samt säkerställa kunskapsdelning, intressentengagemang och hållbarhet bortom projektets livstid. För detta ändamål har tre huvudmålgrupper för spridning identifieras: offentlig sektor; akademi; och diverse intressenter (entreprenörer, investerare, mm.). För att sprida resultanterna till de olika målgrupperna kommer vi använda oss av olika kanaler (se tabell1) och verktyg. Alla partners kommer vara involverade i resultatspridningen och utformningen av nästa steg. Compare och Digital Innlandet som projektledare och ansvariga för AP4 kommer att utforma strategin och fördela arbetsuppgifter till projektets parter. Redan under projektperioden kommer vi arbeta med att skapa en handlingsplan för nästa steg (AP3). Det finns stor potential där olika organisationer såsom kommun och akademi kan samarbeta kring utbildningsfrågor, policyfrågor och säkerhetsfrågor samt datadelning men hur ett sådant arbete kan ske i praktiken och i vilken grad är en fråga som kommer att besvaras under projektets gång. Alla partner har själva varit med och önskat samarbete kring byggandet av samverkansstrukturer vilket ökar chanserna till långsiktigt ihållande arbete med frågan.

8. Risikovurdering

Riskbeskrivning	*Sannolikhet*	*Allvarlighets grad*	Åtgärder
R.1 Partner lämnar projektet	Låg	Hög	Projektteamet arbetar aktivt för att förhindra konflikter och hålla engagemanget hos partners och aktörer.
R.2. Förseningar i projektleveranser	Låg	Medium	Förseningar och misslyckanden från partners övervakas regelbundet genom ledningsprocedurer och verktyg (t.ex. intern rapportering, regelbundna möten, mm.).
R.3 Projektet skapar inte tydlig handlingsplan	Låg	Hög	Kontinuerlig utvärdering för att se att projektet är i rätt riktning och följer tidsplanen.
R.4 Fördröjd projektstart	Medium	Medium	Tydliga aktiviteter i början av projektet som samordnas tillsammans mellan AP lead och projektledare.
R.5 Avhopp av resurs	Låg	Låg	Respektive aktör har ansvar till att säkerställa att resurs finns för genomförandet av projektet. Vid behov av byte ska respektive partner se till att ersättaren får information för projektet.
R.6 Etiska och laghinder	Låg	Hög	Projektet kommer att anlita specialister för att säkerställa att lagstiftningar följs. Projektaktörer
R.7 Lågt deltagande av helix aktörerna i de planerade aktiviteterna	Låg	Medium	Partnerna har starka kopplingar som täcker de olika målgrupperna. En stark kommunikationskampanj och informationskampanj används för att nå intressenter, inklusive flera direktsamtal för att främja workshops och deltagande.

9. Budsjett og finansieringsplan

I tillegg til budsjett og finansieringsplan etter Interregs mal og retningslinjer for norsk og svensk side, er det utarbeidet et samlet budsjett for prosjektet. Budsjettet bygger på mål og aktiviteter beskrevet i del 2 og 3 i denne prosjektbeskrivelsen og det felles budsjettet viser en oversikt over kostnader fordelt på arbeidspakker (se vedlagte budsjett).