

Frede A. Stenslie

Utvikling og stabilisering av innovasjonsnettverk

En casestudie av klyngeprosjektet Security Valley

Trondheim, juni 2011

NTNU
Norges teknisk-naturvitenskapelige
universitet
Institutt for sosiologi og statsvitenskap
Fakultet for samfunnsvitenskap og teknologi ledelse



Utvikling og stabilisering av innovasjonsnettverk

En casestudie av klyngeprosjektet Security Valley

Frede A. Stenslie

Medier, kommunikasjon og informasjonsteknologi
Oppgaven levert: juni 2011
Hovedveileder: Hendrik Storstein Spilker

Forord

Det begynte med nysgjerrighet og en faglig interesse for nyskaping, kommunikasjon og aktørrelasjoner i innovasjonsnettverk. Et halvt år, tre blyanter og en PC-kollaps senere foreligger masteroppgaven. Det har til tider vært en påkjenning, men det har vært gøy! Arbeidet med masteroppgaven har vært en faglig utfordring, og det har gitt meg både påfyll av ny kunnskap, og dypere innsikt i et tema jeg allerede kunne mye om. Det ble under arbeidet tidlig klart at jeg måtte inn på et teoretisk felt rundt innovasjon og næringsklynger som i utgangspunktet ligger utenfor min fagbakgrunn. Det har likevel vært svært givende å se hvordan kommunikasjonsteori kan bidra til en forståelse av klynge- og nettverkssamarbeid hvor relasjonen mellom mennesker, utviklingen av holdninger og tolkningen av budskap er viktige variabler. I tillegg er det alltid en glede å få arbeide med noe som ligger utenfor pensumlitteraturen og lesesalen, særlig når man ser at alle timene bak fagbøkene faktisk er av stor verdi.

Jeg vil først og fremst takke Hendrik Spilker ved Institutt for sosiologi og statsvitenskap for dyktig og grundig veiledning i denne masteroppgaven. Takk til Geir Olav Glomstad, daglig leder i Gjøvik Kunnskapspark, som har åpnet opp bedriften og gitt meg en inngangsport til nettverket i og rundt GKP. Mange takk til alle informanter som ville stille opp og dele av sin erfaring, og spesielt tre anonyme som har stilt seg tilgjengelig for mine spørsmål gjentatte ganger. På det personlige plan vil jeg takke mine foreldre for all støtte gjennom studietiden, og gi en ekstra takk til mamma for utrettelig korrekturlesing. Tusen takk til Karina E. Dæhlin som har vært min største støtte i hektiske tider! Sist men ikke minst, takk også til medstudentene på Medier, kommunikasjon og informasjonsteknologi for mye moro og et godt faglig miljø.

Sammendrag

Denne masteroppgaven er et casestudium av den distribuerte informasjonssikkerhetsklyngen Security Valley med kjerneområde i Gjøvik. Masteroppgaven baseres på dette caset for å studere stabiliseringen av nettverk for samarbeid og innovasjon. Det benyttes en kommunikasjonsfaglig innfallsvinkel for å fokusere på hvordan aktørrelasjoner og kommunikasjonen mellom aktører er viktig for å skape et solid og bærekraftig samarbeidsnettverk på tvers av ulike bedrifter og organisasjoner. Videre viser også studien hvordan virkemiddelapparatets klyngeutviklingsprogrammer har implikasjoner for stabiliseringen av aktørrelasjoner og kommunikasjon innenfor nettverket. Stabiliseringen av nettverk for samarbeid og innovasjon ser på den ene siden i stor grad ut til å være avhengig av en god balanse mellom ekstroversjon og introversjon. En ekstrovert klynge kan gå på bekostning av stabilisering av aktørrelasjoner i kjerneområdet, og slik sett bli et luftslott. En introvert klynge vil risikere lock-in, og heller ikke kvalifisere til videre støtte fra virkemiddelapparatet. På den andre siden ser stabilisering ut til å være betinget av en kommunikasjon som inkluderer elementer av hva som tradisjonelt tenkes som eksternkommunikasjon og internkommunikasjon for å skape koherens mellom eksternt og internt budskap. En felles forståelse av prosjektet, dets formål og omfang vil styrke identiteten og utvikle sosial kapital blant aktørene i nettverket, noe som sees som vesentlig for et fruktbart samarbeid.

Innholdsfortegnelse

1. Introduksjon og bakgrunn	1
1.1 Innovasjon og kommunikasjon i kunnskapsnettverk	1
1.2 Gjøvik Kunnskapspark og Security Valley	3
1.3 Leserveiledning	5
2. Teoretisk grunnlag	7
2.1 Nettverkssamfunnet: ny økonomi, ny organisering	7
2.2 Forståelsen av innovasjon – lineær kontra dynamisk	9
2.3 Regionale innovasjonssystemer	10
2.4 Porters diamant og sosial kapital på flere nivå	11
2.5 Sosial kapital, IKT og medierikhet	13
2.6 Nærhetsdimensjoner, lokal buzz og globale pipelines	14
2.7 Autokommunikasjon: kommunikasjonslogikken i nettverksorganisasjonen	17
3. Forskningsmetode	21
3.1 Kvalitativ metode og casestudium	21
3.2 Grounded theory	23
3.3 Datainnsamling og intervjuguide	24
3.4 Anonymisering, analyse og bearbeiding av data	26
3.5 Kvalitetskriterier	27
4. Innovasjonsnettverk for et innovativt klima i Innlandet?	29
4.1 Et <i>innovativt klima</i> – helhetlig tankegang rundt regionale innovasjonsnettverk ..	29
4.2 Informasjonssikkerhet i Innlandet 2000 – 2001	31
4.3 Bluelight – regionalt kompetansenettverk for informasjonssikkerhet	32
4.4 Exit Bluelight – enter Security Valley	36
4.5 Security Valley – internasjonalt klyngeprosjekt for informasjonssikkerhet	37
5. Fra Bluelight til Security Valley – hva skjedde?	43
5.1 Aktørers behov vs. samarbeidsrammeverk: ufarlig kompetanse, farlige penger ..	43

5.2	Tillitsbygging og IKT i distriburte nettverk	45
5.3	IKT i Bluelight og Security Valley – to strategier.....	48
5.4	Identitet og autokommunikasjon	49
5.5	Synliggjøring: Proof of the pudding eller å kommunisere visjon?.....	50
5.6	Fasilitering vs. prosjektledelse	52
5.7	Koblingen til HiG	54
5.8	Tidsperspektivet.....	55
5.9	Bottom up vs. Top down	56
6.	Innovasjonsnettverk vs. innovasjonsinfrastruktur	59
6.1	Bredt samarbeidsprosjekt vs. produktfokus.....	60
6.2	Gjøvik Kunnskapspark sin egeninteresse vs. gründeres interesser	62
6.3	Geografisk omfang	64
6.4	Et feilslått innovasjonsnettverk?.....	66
7.	Svaner og kalkuner: stabilisering av innovasjonsnettverk.....	69
7.1	Betydningen av temporale forhold og byggingen av enterprise eller bureaucracy 69	
7.2	Påvirkningen av institusjonelle forhold på geografisk nærhet	70
7.3	En stabiliserende triade: autokommunikasjon, consistency og sosial kapital	71
7.4	Stabilisering av nettverk – teoretiske og politiske implikasjoner.....	73
	Litteraturliste	75

Figurliste

<i>Figur 1: Klyngeutviklingsmodell. Basert på fremstilling i "Håndbok for Arena-programmet" (Ffowcs-Williams og Cluster Navigator 2004, i SIVA, Innovasjon Norge og Norges Forskningsråd 2006: 12 – 13).</i>	<i>4</i>
<i>Figur 2: Johnstads modell "Porter og den sosiale kapital" (Johnstad 2004: 122).</i>	<i>12</i>

Tabelliste

<i>Tabell 1: Måloppnåelse for Bluelight. Basert på Bergum (2006: 32).</i>	<i>35</i>
<i>Tabell 2: Nøkkelkarakteristikker ved Bluelight og Security Valley.</i>	<i>57</i>
<i>Tabell 3: Nøkkelkarakteristikker ved Security Valley vs. SECTOR</i>	<i>66</i>

Liste over vedlegg

<i>Vedlegg 1: Intervjuguide Bluelight og Security Valley</i>	<i>i</i>
<i>Vedlegg 2: Samtykkeerklæring</i>	<i>vi</i>
<i>Vedlegg 3: Organisasjonskart for Bluelight</i>	<i>vii</i>
<i>Vedlegg 4: Organisasjonskart og medlemsoversikt for Security Valley</i>	<i>viii</i>

1. Introduksjon og bakgrunn

1.1 Innovasjon og kommunikasjon i kunnskapsnettverk

Innovasjon er et flerdimensjonalt og omfattende begrep. Innovasjon knytter seg først og fremst til nyskaping og realiseringen av en idé til nytt produkt, ny prosess eller forbedringer i eksisterende produkter og prosesser (Sørensen 2005). Det politiske fokuset på innovasjon og næringsutvikling gjennom 1990- og 2000-tallet må sees i lys av en globalisert økonomi og regionaløkonomisk politikk for å fremme konkurransekraft i den nye økonomien. Stortingsmelding nr. 25 (2004-2005) *Om regionalpolitikken* vektlegger viktigheten av å tenke innovasjon, verdiskaping og konkurransekraft som en del av regionalpolitikken, noe som også understøttes av utbyggingen av et bredt offentlig virkemiddelapparat for å fremme regional innovasjon. Dette virkemiddelapparatet inkluderer i første rekke Innovasjon Norge, Forskningsrådet og SIVA som sammen med høyskolene og fylkeskommunene alle er sterke aktører innenfor (regional) innovasjon og næringsutvikling. Halvorsen og Lacave (1998) og Halvorsen (2001) skriver at oppblomstringen av forskningsparker og kunnskapsparker (*science parks*) må sees i lys av det politiske og akademiske fokuset på regionale innovasjonssystemer. I Norge er det SIVA som er hovedeier i de fleste forsknings- og kunnskapsparkene. Mens forskningsparkene ble etablert på 90-tallet for å kommersialisere forskningsresultater fra høyskoler og universiteter på det nasjonale plan, har kunnskapsparkene blomstret opp på begynnelsen av 2000-tallet som mer regionalt fokuserte innovasjonsaktører. Både målene og midlene til kunnskapsparkene varierer i noen grad, men generelt kan man si at oppstarthjelp til nye bedrifter og kommersialisering av forskningsresultater via inkubator drift og kobling til finansieringsordninger, samt å skape synergier, spin-offs og klyngeinitiativer mellom regionale kompetanse- og næringslivsaktører er hovedaktivitetene til kunnskapsparkene (Halvorsen og Lacave 1998: 18). Nært knyttet til kunnskapsparker som tilretteleggere for regional innovasjon og næringsutvikling ligger tanken om samarbeid mellom ulike aktører for kunnskapsutveksling og innovasjon i klynger og nettverk (Dahl og Pedersen 2004).

Selv om virkemiddelapparatet er velutbygget og den politiske viljen legger til rette for innovasjon, er ikke veien til langvarig samarbeid, bærekraftige klynger og stabile nettverk lett. Våland (2004) skriver om hvordan industrielle nettverk oppstår i entusiastiske miljøer, men at mange av disse dessverre ender opp som "kalkuner". Metaforen kalkun

viser til intensjonen om å skape noe som aldri ble hva det var ment som. Selv om intensjonene med å skape kalkunen nok var de beste, har den få av egenskapene til en god fugl; den er ikke pen, og den kan ikke fly. En kalkun er med andre ord den rake motsetningen til en vakker svane. Hvordan kan relasjonene, identiteten og kommunikasjonen innenfor et nettverk bidra til å skape svaner, og ikke kalkuner? Denne studien ønsker å peke på ett sett stabiliserende funksjoner innenfor et slikt innovasjons- og kunnskapssamarbeid. Den vil gå spesielt inn på hvordan dynamikken og relasjonene i hjemmebasen er viktig for å sikre bærekraftighet i klynge- og nettverksinitiativer som fordrer internasjonale koblinger. Mens tidligere studier ofte konsentrerer seg om *enten* nyetableringsvirksomheten *eller* nettverksvirksomheten til en kunnskapspark vil denne studien se helhetlig på aktivitetene i en kunnskapspark for å undersøke hvordan disse kan fungere som gjensidig støttende og stabiliserende funksjoner. Begrepet stabilisering viser til langsiktigheten og bærekraftigheten som oppnås når aktørene innenfor prosjektet har en felles forståelse av gjensidige interesser, strategi, mål og arbeidsform (Callon 2001 [1986]). Lundvall og Christensen (2004) beskriver innovasjon som en usikker kommunikasjonsprosess hvor sosial og kulturell nærhet tilrettelegger for måloppnåelse, mens Griffin (2006) viser til Tidd et al. (2005) og Kaufmann og Kaufmann (1996) når hun skriver at innovasjonsprosesser trenger tydelig kommunikasjon, og at god og tydelig kommunikasjon i neste rekke er et av kjennetegnene på en vellykket organisasjon. Det er rimelig å anta at disse mekanismene også er gjeldende i nettverk og klynger. Problemstillingen lyder:

Hvordan kan en kunnskapspark stabilisere et nettverk for samarbeid og innovasjon?

For å svare på problemstillingen vil jeg benytte klyngeprosjektet Security Valley som case for å belyse ulike sider ved et regionalt innovasjonsnettverk. Security Valley var et prosjekt som hadde målsetninger om å etablere en klynge for informasjonssikkerhetsorganisasjoner med kompetansesenter i Gjøvik under prosjektledelse av Gjøvik Kunnskapspark. Prosjektet ble lansert i 2008 og ble uformelt avviklet i 2010. Casen Security Valley illustrerer flere viktige elementer rundt stabiliseringen av regionale innovasjonsprosjekter. Analysen og drøftingene i denne oppgaven er gjort på bakgrunn av intervjudata med informanter hentet fra miljøet i og rundt Gjøvik Kunnskapspark som har hatt befatning med prosjektene Bluelight og/eller Security Valley. Security Valleys søknad om Norwegian Centre of Expertise fra 2009 har i tillegg til nettsiden securityvalley.no gått inn

som supplerende datamateriale. Kapittel 4 er i stor grad basert på følgeforskningsrapporter for prosjektene Bluelight og Security Valley utført av Østlandsforskning (Bergum og Nyhus 2004; Bergum 2006; Bergum 2009).

1.2 Gjøvik Kunnskapspark og Security Valley

Gjøvik Kunnskapspark ble opprettet i 2000 som en av SIVAs kunnskapsparker. Næringsrådet i Gjøvikregionen, Høgskolen i Gjøvik og flere aktører i det lokale næringslivet var pådrivere for etableringen av et innovasjonsselskap for å tilrettelegge for nyskaping og næringsutvikling i kommunene på vestsiden av Mjøsa. SIVA definerer en kunnskapspark som ”Innovasjonsselskap med fysisk og/eller eiermessig tilknytning til en av de regionale høgskolene. Bygger på det internasjonale forskningsparkkonseptet (science park), men legger mer vekt på samspill med regionalt næringsliv”¹. Gjøvik Kunnskapspark er lokalisert i samme område som blant andre Høgskolen i Gjøvik, Norwegian Information Security Laboratory (NISlab), Gjøvik Tekniske Fagskole, Norsk Senter for Informasjonssikring (NorSIS) og Eidsiva Vekst i Gjøvik. Gjøvik Kunnskapspark (GKP) ønsker å ”identifisere, etablere og realisere innovasjonsprosjekter med regional forankring og internasjonalt potensiale”². Hovedfokuset ligger på områdene sikkerhet og teknologi. Kunnskapsparken drifter to inkubatorer. SECTOR (*Security Incubator*) er lokalisert innenfor GKPs lokaler sammen med NorSIS på Gjøvik. I SECTOR ligger hovedfokuset på gründerbedrifter innenfor (informasjons)sikkerhet, men det finnes også flere bedrifter som arbeider innenfor andre bransjer. RISC inkubator (*Raufoss Innovation and Science Centre*) er lokalisert innenfor NCE Raufoss i Raufoss Industripark, og fokusområdet er (industri)teknologi. Siden oppstarten i år 2000 har Gjøvik Kunnskapspark satset parallelt på innovasjonsnettverk og innovasjonsinfrastruktur. Innovasjonsinfrastruktur knytter seg til drift av inkubator, bedriftsrådgivning og tilknyttet aktivitet, mens innovasjonsnettverk går på samarbeidsprosjekter mellom flere etablerte aktører og gründerbedrifter. Prosjektene Bluelight (2002-2007) og Security Valley (2008-2010) er to av flere prosjekter GKP har koordinert på innovasjonsnettverkssiden.

Virkemiddelapparatet representert ved Innovasjon Norge, Norges Forskningsråd og SIVA arbeider for økt regional innovasjon i næringsklynger gjennom utviklingsprogrammene Arena og NCE (*Norwegian Centre of Expertise*).

¹ SIVA, [http://www.siva.no/internett/cms.nsf/\\$all/1266DB357E99C8B4C1257506005C884B](http://www.siva.no/internett/cms.nsf/$all/1266DB357E99C8B4C1257506005C884B) (udatert, hentet 28.03.2011)

² GKP, http://www.gkp.no/index.php?option=com_content&view=article&id=47&Itemid=1 (udatert, hentet 28.03.2011)

Arenaprogrammet er en starthjelp for etableringen av nettverk eller klynger hvor innovasjon og næringsutvikling står sentralt. NCE-programmet kan på mange måter sees som en viderefinansieringsordning av de sterkeste nettverkene/klyngene som blir etablert gjennom Arena³. Både Arena og NCE legger Ffowcs-Williams og Cluster Navigator sin 5-fasers klyngemodell til grunn for forståelsen av klyngeutvikling gjennom følgende 12 trinn:

- 1. Sikre oppslutning**
 - Introdusere klynger som arbeidsform
- 2. Legge grunnlaget**
 - Innledende klyngeanalyse
 - Etablering av ledergruppe
- 3. Skape fremdrift og begeistring**
 - Utvikle felles visjon
 - Identifisere stegene fremover
 - Lage kortsiktig handlingsplan
- 4. Utvide klyngegrunnlaget**
 - Igangsette klyngeinitiativet
 - Formalisering av klyngeorganisasjonen
- 5. Sikre fortsatt drift**
 - Oppgradering av den strategiske agendaen
 - Samarbeid med andre klyngeinitiativ
 - Evaluere og justere strategi

Figur 1: Klyngeutviklingsmodell. Basert på fremstilling i "Håndbok for Arena-programmet" (Ffowcs-Williams og Cluster Navigator 2004, i SIVA, Innovasjon Norge og Norges Forskningsråd 2006: 12 – 13).

Security Valley var et prosjekt som tok sikte på å bygge videre på nettverket som var etablert rundt informasjonssikkerhet som fagområde gjennom prosjektet Bluelight. Gjennom arbeidet med å etablere et sterkt miljø på Gjøvik med *pipelines* til andre nasjonale og internasjonale kompetanseaktører på informasjonssikkerhet ønsket man å etablere en næringsklynge som NCE. Security Valley fikk avslag på sin søknad om NCE i 2009, og den klyngerelaterte aktiviteten opphørte derfor i løpet av høsten 2009 siden det ikke lenger fantes tilstrekkelig finansieringsgrunnlag. I hvilken grad Security Valley klarte å oppfylle kravene til NCE-status gir ikke mine data noen systematisk oversikt over. Denne studien vil i det vesentlige gå inn på aktørrelasjoner og modenhet i utviklingsprosessen når

³Innovasjon Norge, http://ekstranett.innovasjonnorge.no/templates/Page_Meta_56334.aspx (datert, hentet 28.03.2011).

jeg benytter Security Valley som case for å undersøke hvordan dynamikken mellom interne og eksterne dimensjoner i et klyngeinitiativ bidrar til stabiliseringen av innovasjonsnettverk. Slik jeg ser klyngeutviklingsmodellen som ligger til grunn for Arena og NCE gir den liten innsikt i hvordan samarbeid, tillit og sosiale bånd utvikles for å stabilisere klyngen. I tillegg viser den også en lineær og suksessiv forståelse av klyngeutvikling, noe som virker overforenklet ut fra mine intervjuer med informanter innenfor Security Valley.

1.3 Leserveiledning

Oppgaven er bygget opp i syv hovedkapitler. Kapittel 2 vil gi en oversikt over relevant teori og tidligere forskning som vil benyttes i analysen av funnene. Den teoretiske innfallsvinkelen til studien består av et utvalg blant innovasjonsteori, kommunikasjonsteori og teknologisosologi. I kapittel 3 vil jeg redegjøre for forskningsmetode, valg av case og fremgangsmåte. Her vil jeg også drøfte datakvaliteten, de tolkingene jeg har gjort og studiens kvalitet. Kapittel 4 er første analysekapittel hvor jeg vil redegjøre for Gjøvik Kunnskapsparkers satsning på innovasjonsnettverk for informasjonssikkerhet ved å gi en kronologisk gjennomgang av Bluelight og transformasjonen til Security Valley. I dette kapitlet vil jeg også introdusere begrepet *innovativt klima* som forståelsesramme for et lokalt miljø med positive holdninger til innovasjonsarbeid. Bluelight og Security Valley var to prosjekter som hadde den grunnleggende likheten ved at begge var innovasjonsnettverksprosjekter for informasjonssikkerhet under styring av Gjøvik Kunnskapspark. Prosjektene var likevel forskjellige på mange viktige punkter. I kapittel 5 vil jeg gå nærmere inn på disse forskjellene for å etablere en forståelse av hva som skjedde da Bluelight ble transformert til Security Valley. Kapittel 6 tar for seg balansen mellom innovasjonsnettverk og innovasjonsinfrastruktur. Hvordan kan fokus på innovasjonsinfrastrukturen – definert som inkubator for gründerbedrifter – bidra til å stabilisere nettverk for innovasjon og samhandling gjennom å sikre et innovativt klima i det geografiske kjerneområdet? I kapittel 7 vil jeg oppsummere studiens funn og presentere tre hovedmomenter som konkluderer denne studien. Utviklingen fra Bluelight til Security Valley kan fremstilles som en historie om svanen som ble til en kalkun. Jeg argumenterer for en mer nyansert forståelse av denne utviklingen, og vil peke på hvordan historien om Security Valley kan være nyttig for forståelsen av stabilisering av nettverk for samarbeid og innovasjon.

2. Teoretisk grunnlag

I dette kapitlet vil jeg først presentere en mer overordnet nettverksteori for å redegjøre for de grunnleggende elementene i nettverks- og klyngetenkning. Deretter vil jeg gi en kort innføring i forståelsen av innovasjonsbegrepet, og hvordan innovasjon er en del av nettverks- og klyngetenkningen, ved å presentere teori og tidligere forskning rundt regionale innovasjonssystemer. Jeg vil videre greie ut om Johnstads teoretiske argument om at sosial kapital utgjør en *black box* i klyngeteoriene; aktørrelasjonene må forstås som limet som holder et nettverk eller en klynge sammen. Mens både teori omkring regionale innovasjonssystemer og Porters modell, som Johnstad bygger på, setter geografisk nærhet som betingelse som klynger, skal vi se at Boschma (2005) ser geografi som kun én av flere nærhetsdimensjoner for samarbeid. Denne forståelsen deles også av Bathelt et al. (2004) som skriver om hvordan lokal *buzz* og globale *pipelines* er viktige betingelser for suksessfulle klynger. Til slutt vil jeg også redegjøre for hvordan nettverks- og klyngesamarbeid forutsetter en forståelse av organisasjonskommunikasjon som transcenderer de tradisjonelle kategoriene “internkommunikasjon” og “eksternkommunikasjon” for å skape gode aktørrelasjoner og dermed bidra til å stabilisere nettverkssamarbeid.

2.1 Nettverkssamfunnet: ny økonomi, ny organisering

Manuel Castells’ nettverksteori er en nyttig innfallsvinkel til å forstå fremveksten av nettverk og klynger som et politisk, organisatorisk og økonomisk fenomen. Castells (1996: 77) knytter IKT til fremveksten av et nytt nettverkssamfunn, og en ny økonomi hvis karakteristikk er “informational, global, and networked”. Med *informational* – eller informatorisk – mener forfatteren at aktørene i den nye økonomien er avhengig av å kunne generere, prosessere og benytte kunnskapsbasert informasjon for å hevde seg i et marked som går utover grenser i tid og rom som man tidligere forholdt seg til. De gamle grensene har i sin tur blitt oppløst slik at man i den nye økonomien snakker om et *globalisert* marked. For Castells er også alle *komponentene* i markedet, slik som arbeidskraft, kapital, teknologi og ledelse, også globalisert og gjensidig avhengig. Økonomien har gjennom de siste tre – fire tiår utviklet seg som en nettverksorganisering. Med dette mener Castells at interaksjonen mellom aktører i den nye økonomien skjer på globalt plan mellom nettverk av aktører. Denne interaksjonsformen bunner i at informasjonsteknologi har gjort samhandling og kontakt øyeblikkelig og alltidsnærværende (ibid.). IKT bryter opp de

gamle begrensningene i tid og rom, noe som resulterer i fremveksten av nettverkssamfunnet.

En globalisert nettverksøkonomi setter markedskonkurransen i sentrum. Økonomisk konkurransedyktighet knyttes til ønsket om profitt for både kommersielle og politiske aktører i den nye økonomien. Innovasjon, produktivitet og teknologiske fremskritt er middel for å sikre konkurransedyktighet og profitt. Selv om informasjonsteknologi, godt hjulpet av deregulerte handelsbarrierer, skaper en globalisert økonomi, er likevel ikke alle komponenter globalisert. Castells påpeker at det meste av produksjon, sysselsetting og bedrifter fortsatt er bundet til det lokale eller regionale nivået på tross av at den overordnede økonomiske virkeligheten de opererer i er internasjonal (1996: 101). Det er mot dette bakteppet vi må forstå fremveksten av næringsklynger og regionale innovasjonssystemer som verktøy for fremgang i en globalisert og nettverket økonomi basert på kunnskap og informasjon. I denne økonomien forstås også konkurranse og økonomisk vekst som en blanding av sosiale og økonomiske prosesser i nettverk og klynger (Bathelt og Taylor 2002).

Castells (1996) skriver lite direkte om næringsklynger som konsekvens av den nye økonomien. Han bruker imidlertid begrepet *the network enterprise* for å beskrive konsekvensene av den nye økonomien for organisasjonene som er aktører i den. Castells definerer en organisasjon som “a system of means structured around the purpose of achieving specific goals” (Castells 1996: 187). Med referanse til Touraine (1959) viser forfatteren til to grunntyper av organisasjoner: i) organisasjoner som har reproduksjon av sitt virkemiddelsystem som organisatorisk mål; og ii) organisasjoner hvis målsetninger, og endring i målsetninger, former og omformer virkemiddelsystemet (ibid.). Den første organisasjonstypen kaller Castells byråkratier, mens den andre formen er foretak (*enterprise*). Nettverksorganisasjonen defineres som følger: “*that specific form of enterprise whose system of means is constituted by the intersection of segments of autonomous systems*” (Castells 1996: 187). Slik jeg ser det, sier teorien om nettverksorganisasjonen lite direkte om hvordan små og middels store bedrifter med lokal eller regionalt fofeste agerer i den nye økonomien. Likevel vil jeg argumentere for at nettverksorganisasjonen er et nyttig konsept for å forstå organisasjonslogikken i en globalisert økonomi, og for å forstå strategisk allianse som konkurransefortrinn på makronivå. Organisatorisk sett blir det nettverksdrevne *prosjektet* den nye arbeidsenheten, mens de individuelle bedriftene i mindre grad står i sentrum. Informasjonen som deles mellom aktører som opererer på ulike felt i nettverket blir av desto høyere viktighet:

And the most important information, under new economic conditions, is that processed between companies, on the basis of experience from each field. Information circulates through networks: networks between companies, networks within companies, personal networks, and computer networks (Castells 1996:177).

Castells peker på to forutsetninger som avgjør graden av suksess for et nettverk. Disse forutsetningene er i) *connectedness*, altså de strukturelle egenskapene for god kommunikasjon; og ii) *consistency*, som viser til graden av delte interesser mellom nettverkets målsetning og aktørenes målsetninger (1996: 187). Av analysen fremgår hvordan Security Valley var en type nettverksorganisert prosjekt hvor man ønsket å utvikle noe *utover* de organisasjonene som skulle samles under paraplyen Security Valley. Casen vil også illustrere hvordan *connectedness* og *consistency* er gjensidig støttende betingelser, men at gode strukturelle kommunikasjonsegenskaper ikke alltid gir en felles forståelse av *consistency*.

Hos Castells gjennomsyrrer også nettverkslogikken begrepsapparatet omkring geografi og oppbygning av nettverkssamfunnet. Nettverk er bygget opp av *punkter*, *huber* eller *noder* koblet sammen med *linker*. Disse punktene, hubene og nodene kan være byer, mennesker, organisasjoner, regioner eller nasjoner. Linkene består av en kontinuerlig flyt – *flow* – av ting som informasjon, materialer, penger eller mennesker (Bell 2007: 69). I denne oppgaven velger jeg å benytte Castells' begrepsapparat i drøftingen av nettverk.

2.2 Forståelsen av innovasjon – lineær kontra dynamisk

Innovasjon er et omfattende begrep som brukes i mange sammenhenger. En klar definisjon av innovasjon som fenomen og begrep er derfor vanskelig – og lite ønskelig – å gi. Sørensen (2005) skriver om utviklingen av innovasjonsbegrepet fra den schumpeterianske betydningen hvor innovasjon var knyttet til entreprenørvirksomhet i nye produkter, nye produksjonsprosesser, nye markeder, nye kilder for leveranser og nye organisasjonsformer til et begrep som beskriver organiseringen av forskning, virkemiddelapparat, næringspolitikk og finansiering. Sørensen refererer til Freeman (1982: 7) som poengterer at en innovasjon ikke er det samme som en ny idé, men som realiseringen av idéen eller oppfinnelsen som nytt produkt eller ny praksis (Sørensen 2005: 513). Innovasjon må dermed sees i sammenheng med kunnskap, kunnskapsutvikling og kunnskapsdeling, og kan ikke sees som *lineære* årsak – konsekvenshendelser, men snarere som *dynamiske* prosesser hvor en mengde aktører og interesser påvirker utviklingsforløpet (ibid.). Berker (2010) viser til Cheng og Ven (1996) som studerer forholdet mellom orden og

tilfeldigheter i innovasjon ved å teste to motstridende antakelser: a) innovasjon skjer i periodiske sekvenser og utviklingstrinn; og b) innovasjon skjer i form av en rekke tilfeldige hendelser. Cheng og Ven fant at ingen av antakelsene stemte. I stedet viste innovasjonsprosesser seg som et uforutsigbart og dynamisk system uten noen fast orden, men likevel ikke stokastisk og tilfeldig (Cheng og Ven 1996: 607, i Berker 2010: 3). Når det i denne studien snakkes om innovasjon, innovasjonsprosesser og innovasjonsnettverk er dette i forhold til både de politiske og de økonomiske interessene knyttet til innovasjon, og spesielt til regionale innovasjonssystemer. Innovasjon som sosialt, økonomisk og politisk fenomen er dermed knyttet opp til hvordan innovasjon skjer innenfor en kontekst av kommersielle interesser, samfunnsmessige behov, politiske aspirasjoner og offentlige virkemidler. Klyngeteoriene gir en innfallsvinkel til forståelsen av hvordan det dynamiske miljøet rundt en bedrift er avgjørende for bedriftens konkurranseevne.

2.3 Regionale innovasjonssystemer

Beat Hotz-Hart (2000) viser hvordan den økonomiske globaliseringen øker betydningen av stabile og sterke regionale innovasjonsnettverk. Han viser til viktigheten av en sterk regional kunnskapsbase, og en kunnskapsinfrastruktur som sammen med et godt institusjonelt og finansielt rammeverk vil øke konkurransedyktigheten til regioner i den nye økonomien. Hauge et al. (2009) viser til Lundvall (1985) og Freeman (1988) når de beskriver hvordan innovasjonssystemteori ble utviklet som en helhetlig forståelse av innovasjon som betinget av nasjonal kontekst. Senere har man også snakket om regionale innovasjonssystemer som undersystemer av det nasjonale. Regionale innovasjonssystemer kan defineres som “nettverk av offentlige og private aktører hvis aktiviteter og interaksjon skaper, importerer, modifiserer og sprer ny teknologi” (Freeman 1988, i Hauge et al. 2009: 126). Forfatterne foreslår en modell som forklarer regionale innovasjonssystemer er samspillet mellom 4 delsystemer: i) *kunnskapsinfrastrukturen* representerer universitet/høgskole, FoU og ledende teknologibedrifter; ii) *det industrielle system* som innbefatter gründere, bedrifter og klynger/bedriftsnettverk; iii) *regionale myndigheter og virkemidler* slik som for eksempel Innovasjon Norge, fylkeskommunene, og de programmer og ordninger som sorterer under disse; og iv) *annen infrastruktur* som finansieringsordninger, konsulenttenester og informasjon. Inkubator drift kan være eksempel på dette (ibid.: 127 - 128). Samspillet mellom aktører innenfor disse delsystemene er grunnlaget for sosial kapital og kunnskapsflyt og læring som gjensidig avhengige faktorer. Det er innenfor denne rammen av nærings- og distriktspolitisk syn på

regionale innovasjonssystem at vi må forstå utviklingen av innovasjonsnettverk/klynger med drivernode i en kunnskapspark.

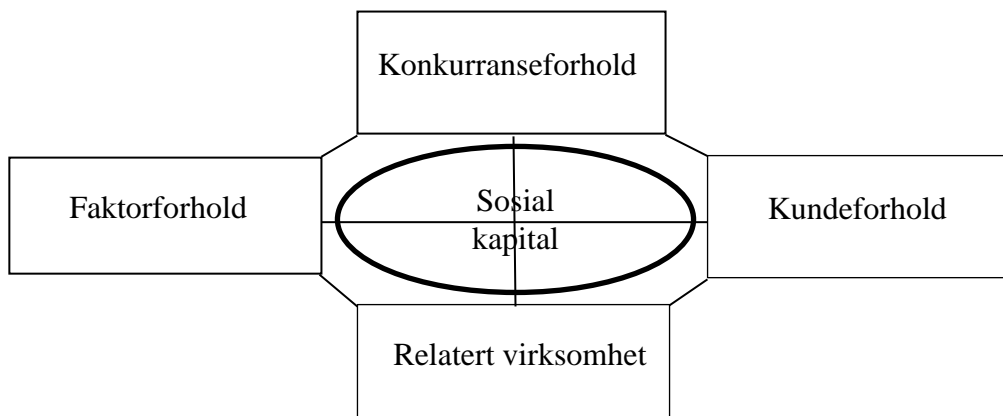
2.4 Porters diamant og sosial kapital på flere nivå

Tom Johnstad (2004; 2009) tar utgangspunkt i Porter (1990; 1998; 2000) i sine teoretiske betraktninger rundt innovasjon og næringsutvikling i Innlandet. Utgangspunktet hos Porter er at alle virksomheter har en "hjemmebase"⁴ som svarer til ulike organisatoriske, geografiske og politiske avgrensninger. En hjemmebase kan eksempelvis være en by, en region eller en nasjon. Virksomheter må sikre sin hjemmebase for å kunne være konkurransedyktige i den globale økonomien, og dette gjør de ved å samarbeide i klynger. Disse klyngene kan forekomme i mange forskjellige næringer, fagfelt, og på ulike geografisk nivå. Sentralt i Porters klyngeteori er diamantmodellen som forklarer samspillet mellom fire faktorer som påvirker bedrifters konkurranseevne. *Faktorforhold* omfatter ressurser, infrastruktur, kapital, teknologi med mer. *Kundeforhold* viser til etterspørsel av produkter eller tjenester på hjemmemarkedet. *Konkurransforhold* gjelder egenskaper ved konkurransesituasjonen, og hvordan man tilpasser seg denne. *Relaterte næringer* viser til beslektet virksomhet og kunnskapsmiljø (Porter 1990, i Reve og Jakobsen 2001: 32 - 39). Disse fire faktorene utgjør tilsammen de dynamiske betingelsene for hjemmebasens konkurranseevne. I denne dynamikken inngår krav fra brukere/kunder, konkurransesituasjonen mellom relaterte bedrifter og koblingen mot eksterne kompetansemiljøer for å nevne noe. I Porters klyngeteori er de sosiale og organisatoriske linkene mellom aktørene som holder klyngen sammen (Johnstad 2009: 68 – 69).

Dynamiske innovasjonsprosesser er komplekse, og krever samarbeid mellom nodene i nettverket. Begrepet *sosial kapital* kan benyttes for å skape bevissthet om hvordan kommunikasjonen innenfor et kunnskapsnettverk bør bidra til å tilrettelegge for en felles sosial plattform å bygge samarbeidet på. Johnstad (2004: 122) viser til Bourdieu (1986), Coleman (1990), og Putnam (1993) når han definerer sosial kapital som "sosiale relasjoner, tillit, normer og sanksjoner mellom personer, grupper eller organisasjoner som fremmer eller hemmer samarbeid til felles beste". Videre skriver Johnstad at sosial kapital finnes i relasjonene mellom aktører, og er en ressurs som oppstår i den sosiale strukturen aktøren er en del av. Sosial kapital virker inn på effekten av andre former for kapital, slik som human kapital (kompetanse), finansiell kapital, og fysisk kapital (eiendom) (Johnstad 2004; 2009).

⁴ Begrepene hjemmebase og kjerneområde viser til en klynges sterkeste geografiske tilhørighet. I Oppgaven brukes begrepet kjerneområde, siden dette begrepet også blir brukt i Security Valleys NCE-søknad (2009).

Han peker videre på at oppmerksomheten rundt sosial kapital som ressurs for samarbeid og innovasjon i nettverk innenfor innovasjons- og klynjelitteraturen i liten grad fokuserer på utviklingen og bestanddelene i sosial kapital. Således fremstilles sosial kapital som et black boxet fenomen uten noen konkret verdi (ibid.). Johnstad konkretiserer sosial kapital ved å se på dens funksjon på ulike analytiske nivå. I et makroperspektiv knytter han sosial kapital til Porters (1990) klassiske klyngeteori, og forklarer sosial kapital som ”limet” som holder kundeforhold, konkurranseforhold, faktorforhold og relatert virksomhet sammen i et nettverk for samarbeid og kunnskapsdeling:



Figur 2: Johnstads modell "Porter og den sosiale kapital" (Johnstad 2004: 122).

På mesonivået består sosial kapital av relasjonene som oppstår mellom aktører og noder i nettverk. Coleman (1988) deler begrepet ”sosial kapital” opp i grunnleggende komponenter for å belyse ulike sider ved det. For det første snakker han om utviklingen av et *sosialt nettverk* som forutsetning for sosial kapital, og dermed tillit. Videre er det viktig å utvikle et sett med *normer og sanksjoner*, og oppnå en felles forståelse rundt disse verdier og regler for medlemmene (ibid.). I videreføringen av dette viser Johnstad til Ostroms (1998) modell for kollektiv handling som viser hvordan faktorer som kommunikasjon, kunnskap om tidligere handling, interesseartikulering og utviklingen av felles normer ligger til grunn for tillit, omdømmevurdering og gjensidighet. Summen av denne påvirkningen utgjør klimaet for samarbeid. Tillit, gjensidighet og omdømme står i gjensidig påvirkningsforhold til hverandre, enten positivt eller negativt.

Halpern skriver om de tre *sub-typene* i sosial kapital; *bonding*, *bridging* og *linking* (Halpern 2005, i Johnstad 2009: 75). Bonding (sammensveising) viser til de tette bånd som oppstår mellom mennesker innenfor relativt homogene grupper. Det er disse sterke båndene som kan bidra til en solid fellesskapsfølelse innenfor en bedrift. Bridging

(brobygging) går på horisontale bånd mellom grupper, bedrifter og organisasjoner, og er ofte av svakere karakter. Bridging er ikke nødvendigvis et institusjonalisert fenomen, men kan like gjerne skje via enkelte nøkkelpersoner, informasjonskanaler og kontakter. Bridging og bonding har tidligere blitt beskrevet av Robert A. Putnam, som karakteriserer bonding som den innadrettede kontakten i et sosialt nettverk, mens bridging er den utadrettede kontakten (Putnam 2000, i Bø og Schiefloe 2007). Linking går på å knytte vertikal kontakt mellom grupper, institusjoner eller bedrifter som står i et asymmetrisk maktforhold til hverandre (Halpern 2005, i Johnstad 2009: 76). Sosial kapital er ikke et fast og uforanderlig fenomen, men snarere noe som utvikles over tid, og som kan forsterkes eller forvitres. Johnstad (2009: 77) påpeker at ”I klyngesammenheng er det viktig å få til overgangen fra samarbeid (bridging) til samhandling (bonding), der samhandling er en mer utviklet og dypere form for samarbeid”.

På mikronivå knytter Johnstad sosial kapital til sosialt entreprenørskap for å vise hvordan enkeltindivider – *ildsjelene* – kan skape engasjement og mobilisere til innovasjon innenfor lokale forutsetninger. Dette handler også om hvordan bedriftsmiljøet fasiliterer for visjoner, initiativ og godt lederskap (Johnstad 2009). Johnstad ser sosial kapital i innovasjon som en trenivåmodell hvor ildsjeler og entreprenørskap på mikronivået må sees i sammenheng med mesonivået, hvor omdømme, tillit og gjensidighet er forutsetning for samarbeid. Dette utgjør igjen ”black boxen” som er limet i klyngeteoriene på makronivået (ibid.: 81).

2.5 Sosial kapital, IKT og medierikhet

Johnstad (2004: 123) ser sosial kapital som ”basisen for den generaliserte tillit vi finner mellom individer, bedrifter og organisasjoner”. Våland (2004) fokuserer på at gode nettverk bygger på en kjennskap til hverandre, og erkjennelse av gjensidighet mellom nodene i nettverket. Dette oppnås ved å tilrettelegge for en god informasjonsflyt innenfor nettverket, det vil si regelmessig og effektiv kommunikasjon (ibid.). Samtidig peker andre studier på at uformelle kanaler og personlige kontakter ofte er vel så viktig for informasjon og kunnskapsdeling som de formelle knutepunktene (Dahl og Pedersen 2004). Steinfield et al. (2010) undersøker antakelser om sosial kapital, kunnskapstilgang, tillit og IKT-bruk som gunstig i næringsklynger. Forskerne konkluderer med at kunnskapsdeling innenfor klynger, og særlig koblingen mellom forskningsinstitusjoner og små bedrifter, sikrer suksess. IKT-bruk forsterker human kapital, og komplementerer andre strategier for utvikling av sosial kapital som forutsetning for kunnskapsdeling (ibid.).

Medierikhetsteori bygger på antakelsen om forskjellige mediers kapasitet til å kommunisere ulikt innhold. Hovedtanken er at usikkerheten er omvendt proporsjonal med informasjonsbredden i den valgte kommunikasjonsformen. Informasjonsbredden, eller mer spesifikt et mediums potensial til å fasilitere felles forståelse, kan forstås som høy- eller lav rikhet i mediet (Draft et al. 1987). Men henblikk på virtuelle team og distribuert samarbeid knytter Bergum (2004) interaksjon, relasjonsbygging og tillit til valg av medie- og kommunikasjonskanaler. Særlig fokuserer han på et bevisst valg av kommunikasjonskanal i forhold til hvilken fase samarbeidet er i. Han vektlegger at et minimum av synkron toveiskommunikasjon er å foretrekke i alle faser, men at dette er ekstra viktig i startfasen, da tillit skal bygges mellom aktører som ikke tidligere har noe forhold til hverandre. Ansikt-til-ansikt-kommunikasjon er i slike tilfeller foretrukket (ibid.). Bergum (2004) mener at utviklingen av en felles kultur, motivasjon og tillit mellom noder i et kunnskapsnettverk forutsetter at kommunikasjonen foregår gjennom flere kanaler. Man kan tenke seg at det vil være kontraproduktivt å redusere kommunikasjonen til kun rutinemessige beskjeder og informasjonsdeling via tegnfattige og asynkrone medier. Våland (2004: 5) påpeker at elektronisk basert kommunikasjon ”kan neppe erstatte tillitsbygging gjennom sosiale og uformelle relasjoner, som er en viktig faktor i utviklingen av nettverket”.

2.6 Nærhetsdimensjoner, lokal buzz og globale pipelines

Mens Johnstad (2009) med referanse til Halpern (2005) fokuserer på bonding, bridging og linking for å bygge relasjoner for stabile klynger og nettverk, kan også teori rundt ulike dimensjoner av nærhet være nyttig for å få innsikt i betingelsene for nettverk for samarbeid og innovasjon. Teori rundt nærhetsdimensjoner skiller seg også fra det geografisk-økonomiske perspektivet og agglomerasjonsteorien som står sentralt i både Porters klyngeteori og i tanken om regionale innovasjonssystemer. Boschma (2005) peker på at geografisk nærhet er kun én av flere typer nærhet som ligger til grunn for dannelsen av klynger. Boschmas hovedargument er at den geografiske nærheten må sees i forhold til andre nærhetsdimensjoner fordi samlokalisering i seg selv er relativt lite viktig, men at det legger til rette for andre typer nærhet. Nærhet på ulike plan er også et tveegget sverd: For mye nærhet kan lede til en introvert klynge uten de nødvendige markedskoblingene, fleksibilitet og utviklingspotensial (*lock-in*), mens en for ekstrovert klynge ikke vil virke samlende for medlemsaktørene (Boschma 2005). Nettopp balansen mellom fundamenteringen internt i klyngen og de nødvendige koblingene utenfor klyngen er tema

for Bathelt et al. (2004) og Bathelt og Taylor (2002) som beskriver hvordan lokal *buzz* og globale *pipelines* legger til rette for kunnskapsutvikling og vekst i nettverk og klynger.

På bakgrunn av tidligere teori identifiserer Boschma fem nærhetsdimensjoner: kognitiv, organisatorisk, sosial, institusjonell og geografisk nærhet. Kognitiv nærhet viser til det aktuelle kunnskapsområdet som ligger til grunn for klyngen eller nettverket, og den gjør at læring, kunnskapsdeling og dermed innovasjon er lettere å gjennomføre. *Kognitiv nærhet* er nært knyttet til evnen til å kommunisere og forstå budskap likt (Boschma og Lambooy 1999, i Boschma 2005: 63). Selv om kognitiv nærhet er en forutsetning for effektiv læring og kunnskapsdeling, peker forfatteren likevel på tre forhold som gjør det nødvendig å opprettholde en viss kognitiv avstand. For det første krever læring og kunnskapsutvikling komplementære kunnskapsbaser hos menneskene innenfor klyngen eller nettverket. For det andre vil for stor kognitiv nærhet kunne føre til lock-in på grunn av manglende orientering utenfor området man arbeider i. For det tredje hevder Boschma at kognitiv nærhet vil kunne føre til deling av informasjon som er ugunstig for en bedrifts konkurransevne (Boschma 2005: 64).

Organisatorisk nærhet er viktig for evnen til koordinering og deling av kunnskap mellom aktørene i et nettverk. Forfatteren definerer det som følger: “(...) the extent to which relations are shared in an organizational arrangement, either within or between organizations. To be precise, this involves the rate of autonomy and the degree of control that can be exerted in organizational arrangements” (Boschma 2005: 65). Organisatorisk nærhet antas å være gunstig for kunnskapsutveksling og innovasjon. Likevel kan for tette organisatoriske bånd føre til lock-in i bestemte eller typiske relasjoner, og en generell introvert holdning som resulterer i lite fleksibilitet, og liten grobunn for innovative ideer (ibid.).

Sosial nærhet vedrører i hvilken grad sosiale relasjoner mellom aktører i nettverk er etablert som forutsetning for læring og handling. Sosial nærhet svarer i grove trekk til det som ovenfor er referert til som sosial kapital, og spesielt det som går på tillit i relasjoner på et analytisk mikronivå. Boschma er enig i at de sosiale relasjonene må være veletablert for å fremme innovasjon og kunnskapsdeling i klynger og nettverk, men peker samtidig på at for sterk tillit og sosial atferd kan undertrykke opportuniste, og dermed tap av utviklingsmuligheter (Boschma 2005: 66).

Institusjonell nærhet omhandler den delte forståelsen av “*the institutional rules of the game*”, kultur, vaner og normer som deles mellom aktører i et samarbeid (Boschma 2005: 68). Den institusjonelle nærheten ligger til grunn for å skape en overordnet stabilitet i

samarbeid hvor kunnskapsdeling og innovasjon står sentralt. På den annen side kan også institusjonell nærhet bidra til et låst system. Boschma peker på at tre faktorer må balanseres: i) *stabilitet*, det vil si å redusere usikkerhet og opportunisme; ii) *åpenhet* til å skape muligheter; og iii) *fleksibilitet* til å eksperimentere med nye institusjoner (Boschma 2005: 68).

Boschmas siste nærhetsdimensjon er den geografiske. *Geografisk nærhet* har blitt gjort mindre viktig gjennom mer utstrakt bruk av IKT. Kognitiv nærhet er en forutsetning for utvikling og læring i nettverk og klynger, men verken den kognitive, eller sosiale nærheten trenger å være stedbunden. Likeledes forutsetter heller ikke institusjonell og organisatorisk nærhet samlokalisering. Boschma påpeker imidlertid at IKT ikke løser alle nærhetsproblemer, siden ansikt-til-ansikt-kontakt er viktig for etableringen av tillit og overføring av *taus kunnskap*. Det antas likevel at geografisk nærhet vil bidra til å styrke de positive effektene ved de andre nærhetsdimensjonene, så lenge det ikke bidrar til en geografisk lock-in. Dette viser til den nødvendige balansegangen mellom å sikre et indre miljø i nettverket eller klyngen samtidig som at relasjoner mot eksternt marked og eksterne organisasjoner må opprettholdes. Bathelt et al. (2004) sin teori om lokal buzz og globale pipelines er en nyttig innfallsvinkel for å forstå denne balansegangen.

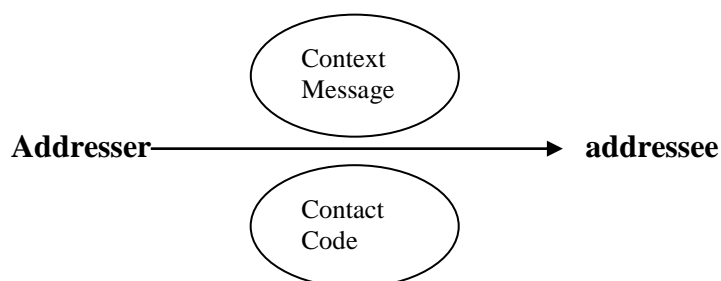
Bathelt et al. (2004) er kritisk til å forstå innovasjon, kunnskapsdeling og læring som avhengig av samlokalisering når man snakker om nødvendigheten av å dele taus kunnskap. Likeledes antas at kodifisert kunnskap ikke i samme grad er avhengig av samlokalisering, og at den dermed er av en mer globalisert karakter. Dette må igjen sees i forhold til utviklingen i informasjonsteknologi som skaper den globaliserte økonomien og nettverksorganiseringen (Castells 1996). Bathelt et al. (2004) skriver at en klynges suksess avhenger av å kunne kombinere den stedbundne tause kunnskapen med kodifisert kunnskap som er tilgjengelig utenfor klyngens geografiske område. Forfatterne bygger på tidligere forskning når de benytter begrepet *local buzz* for å beskrive strømninger i et geografisk avgrenset miljø for kunnskapsdeling, læring, teknologiutvikling og innovasjon (Storper og Venables 2002; Owen-Smith og Powell 2002; Grabher 2002, i Bathelt et al. (2004: 38). Forfatterne definerer lokal buzz som “the information and communication ecology created by face-to-face contacts, co-presence and co-location of people and firms within the same industry and place or region” (Bathelt et al. 2004: 38). Utviklingen av buzz krever – som også Boschma påpeker – en kognitiv nærhet, men også delt kultur og vaner som stimulerer til fremveksten av institusjonell nærhet (ibid.). Konkret oppstår buzz når informasjon deles i uformelle og formelle samtaler, i tilfeldige møter, over lunsjbordet,

verktøybenken eller i styrerommet. Buzz kan styrkes eller svekkes av de sosiale mønstrene i en klynge eller et nettverk, og er således avhengig av sosial kapital for å fungere godt.

Behovet for kommunikasjon og kunnskapsdeling utenfor en klyngeområde bør ivaretas av hva Bathelt et al. (2004) med referanse til Owen-Smith og Powell (2002) kaller *pipelines*. Pipelines er koblinger mellom aktører innfor klynger og aktører utenfor klynger som på ett eller annet vis kan bidra positivt til utvikling hos klyngeaktøren. Kommunikasjon og informasjonsdeling via pipelines fungerer på mange måter motsatt av den lokale buzzen. Mens buzz er tilfeldig og usystematisk, er kommunikasjon via pipelines tilmålt og strukturert. Pipelines er viktig for å forhindre lock-in og introversjon i klyngen og dermed sikre konkurransedyktighet. Likevel kan også for sterke og omfattende eksterne relasjoner true den interne dynamikken i klynger. Dette skjer når oppmerksomheten rundt globale pipelines går på bekostning av opprettholdelsen av buzz mellom aktørene i kjerneområdet. Konsekvensen blir at incentivene som ligger i å etablere seg og arbeide innenfor klynger blir borte når buzzen stilner. Resultatet blir hva Bathelt et al. (2004: 48) kaller *hollow clusters*, altså klynger uten noen god intern dynamikk: “A cluster which is more or less empty because its important actors are constantly travelling the world in order to build and maintain an extensive pipeline system will run an obvious risk of becoming less vibrant” (Bathelt et al. 2004: 48).

2.7 Autokommunikasjon: kommunikasjonslogikken i nettverksorganisasjonen

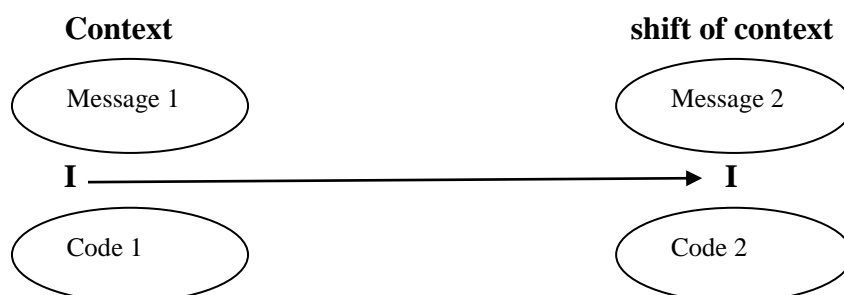
Klassiske kommunikasjonsmodeller tar ofte utgangspunkt i oversendelsen av et budskap fra en sender til en mottaker. Et eksempel er Jakobsons (1964) modell som inkluderer kontekst og kode for å si noe om hvordan kulturell koding og kontekst bestemmer tolkningen av budskapets innhold (Jakobson 1964, i Lotman (1990: 20):



Lotman (1990) tar utgangspunkt i denne kommunikasjonsmodellen når han forklarer at de typiske modellene viser til en kommunikasjonsretning som går fra ”jeg” til ”ham/henne”. Lotman benytter begrepet *autokommunikasjon* når han snakker om en alternativ kommunikasjonsretning, nemlig den kommunikasjonen som går fra ”jeg” til ”jeg”. På

samme måte som i en ”jeg-til-ham/henne-modell” kan innholdet i budskapet bli endret gjennom kommunikasjonsprosessen, siden tolkningen av budskap er kontekstavhengig.

Autokommunikasjonsmodellen kan dermed fremstilles på denne måten (Lotman 1990: 22):



Cheney og Christensen (2001) kobler Lotmans semiotiske begrep om autokommunikasjon til organisasjonskommunikasjon. Forfatternes utgangspunkt er at det i moderne organisasjoner er problematisk å definere grenser for organisasjonens omfang, og at det dermed vanskelig kan trekkes et klart skille mellom hva som ligger eksternt for organisasjonen og hva som er internt i organisasjonen. Mens den tradisjonelle organisasjonskommunikasjonen har vært fokusert rundt *internkommunikasjon* eller *eksternkommunikasjon*, har organisasjoner i det (post)moderne samfunnet måttet vie mer oppmerksomhet til å kommunisere likt på kryss av internt og eksternt publikum: ”Many organizations have begun to realize the difficulties of convincing an external audience about their deeds (...) if the internal audience does not accept the message – and vice versa” (Cheney og Christensen 2001: 232). Forfatterne knytter videre en samstemt ekstern- og internkommunikasjon til utviklingen av organisasjonens identitet: Uten konsistent kommunikasjon internt og eksternt vil organisasjonen miste ”selvfølelsen”, som i neste rekke er viktig for troverdigheten både utenfor og innenfor organisasjonen (ibid.). Det påpekes at mens utvikling eller opprettholdelse av identitet ofte ikke er et eksplisitt mål med kommunikasjon, er det en integrert del av det organisasjonen ønsker å fremstå som; hva den ”er”, ”står for”, eller ”vil være” (Cheney og Christensen 2001: 232).

Kommunikasjonen i et nettverk bestående flere organisasjoner befinner seg et sted i mellom det kommunikasjonslitteraturen typisk har definert som grenser for intern- og eksternkommunikasjon. En bedrifts kontakt med en annen er i et henseende eksternt, siden den går utenfor det bedriftsinterne nivået, men likevel internt, siden bedriftene befinner seg innen samme nettverk - og også ofte er samlokalisert. I tillegg kan distribuerte

organisasjoner og kundemedvirkningsprosesser bidra til å ytterligere utdeliggjøre skillet mellom hva som er internt og eksternt for en organisasjon. Cheney og Christensen (2001) knytter tvetydighet i nettverksorganisasjonens ytre grenser til bedrifters behov for identitet og en følelse av "self":

To uphold a sense of "self" while being flexible or existing as part of a larger network, organizations of today seek to integrate internal and external dimensions of their activities with the overall purpose of communicating one identity, although they may indeed pursue variations on a central theme (Cheney og Christensen 2001: 245).

En måte å kontinuerlig inkludere en internt rettet kommunikasjon med sikte på å skape en felles identitet i nettverket, er i følge Cheney og Christensen å integrere dette i kommunikasjon som er eksternt rettet. Forfatterne eksemplifiserer dette med å vise til samarbeidet mellom oljeprodusentene BP, Norol, Shell, Chevron, Statoil, Texaco, Q8 og Total som i sin reklame bruker Walt Disneys TV-show "From all of us to all of you" som samlende slagord både for samarbeidspartnerne og forbrukerne. I videreføringen av dette argumenteres det for at det selvforsterkende, og dermed identitetsbyggende, elementet i kommunikasjonen i slike tilfeller kan være like viktig som det substansielle *budskapet* som kommuniseres. Cheney og Christensen viser til dette som *auto-communication* siden kommunikasjonen først og fremst tar sikte på å fremkalle verdier, identiteter og normer som ligger internt i en distribuert organisasjon eller et nettverk, men likevel er en integrert del av organisasjonens eksternkommunikasjon (ibid.). I videreføringen av dette kan man se organisasjonsidentitet som eksempel på Cooleys (1902) "looking-glass-self": Organisasjonen betrakter seg selv etter hvordan den viser seg utad. På dette punktet er det vesentlig å huske Lotmans poeng: Også i en "jeg-til-jeg" kommunikasjonsmodell kan innhold endres og refortolkes. Dette betyr at dersom organisasjonen kommuniserer noe utad som aktørene innad ikke gjenkjenner seg i, oppstår en identitetskrise for organisasjonen.

Den grunnleggende forståelsen av nettverks- og klyngeutvikling som er presentert i dette kapittelet er viktig for å forstå Security Valley som forsøket på å etablere en klynge innenfor det rådende regional- og innovasjonspolitiske klima. Mer spesifikt vil teoriene som er presentert her underbygge tolkningene gjort i analysen, hvor den nettverksinterne dynamikken studeres i nærmere detalj for å undersøke stabiliseringen av innovasjonsnettverk.

3. Forskningsmetode

Redegjørelsen for forskningsmetodikk er viktig for å belyse hvordan studien er bygget opp, og for å skape gjennomsiktighet i prosessen. Metodevalg vil kunne ha stor påvirkning på konklusjonene som trekkes, og er således knyttet til studiens kvalitet. I dette kapittelet vil jeg redegjøre for fremgangsmåte, ta opp aktuell metodekritikk på teoretisk grunnlag og vurdere kvalitetskriteriene for kvalitativ forskning.

3.1 Kvalitativ metode og casestudium

Kvalitativ metode omhandler den arbeidsformen i forskningen som baserer seg på ikke-kvantifiserbare data. Kvalitative metoder er først og fremst egnet for å utvikle en bred forståelse av de sosiale fenomener som inngår i studiens temaområde, og er således velegnet for prosess- og meningsfortolkning (Thagaard 2003). Kvale (2001) argumenterer for hvordan denne dynamiske holdningen til datamaterialet ivaretas gjennom å bruke det kvalitative forskningsintervju som metode. I denne oppgaven har jeg benyttet semi-strukturerte forskningsintervjuer som datainnsamlingsmetode.

Andersen (1997) beskriver case-begrepet innenfor samfunnsvitenskapelig forskning som komplisert og vanskelig definerbart. Han viser til hvordan casestudier i mange tilfeller oppfattes som ikke-vitenskapelige, eller kun verdifullt som støtteforskning til bredere undersøkelser. Casestudium kan defineres som en dypere studie i ett eller få ”tilfeller”. Andersen (1997: 15) viser til Yin (1981: 59) som beskriver casestudiet som studiet av et ”a) contemporary phenomenon in its real-life context, especially when, b) the boundaries between phenomenon and context are not clearly defined”. Videre peker han på at casestudier ofte vil starte induktivt på den måten at hypoteser og forskningsspørsmål oppstår underveis i arbeidet, og at generering av teori ofte er hensikten bak studien (Andersen 1997). Dette ligger tett opp til en generell oppfatning av grounded theory som forskningsmetodikk. Dette skal vi komme tilbake til. Først vil jeg beskrive utviklingen av Security Valley som mitt case.

I arbeidet med denne masteroppgaven startet jeg med kun en vag idé om hva jeg ville forske på. Jeg ville vite noe om kommunikasjon i innovasjonsprosesser, og om hvordan nettverk er avhengige av god aktørdynamikk for å fungere. Likevel følte jeg ikke at jeg kunne utlede konkrete hypoteser på bakgrunn av temaområdet og den teoretiske kunnskapen jeg satt inne med. Jeg kjente imidlertid til Gjøvik Kunnskapspark som hadde administrert informasjonssikkerhetsnettverket Bluelight, og jeg hadde også en viss kjennskap til prosjektet Security Valley. I samtale med daglig leder i kunnskapsparken fikk

jeg tidlig vite at Security Valley hadde havarert på grunn av økonomiske problemer, og at det ble ansett som en tapt sak. GKP var mer interessert i å vite på hvilken måte de kunne utvikle en mer solid kobling mellom inkubatorvirksomheten sin og det lokale næringslivet uavhengig av det direkte fokuset på informasjonssikkerhet. Dette gjorde min innfallsvinkel til masterprosjektet klarere: Jeg ønsket å finne ut hva aktørene innenfor nettverk for innovasjon og kunnskapsdeling tenkte om ulike sider ved arbeidet i et slikt miljø. Jeg ville heller ikke gi helt slipp på ideen om å studere Security Valley. I intervjuguiden til de første intervjuene gikk jeg relativt bredt ut og stilte spørsmål fra ulike teoretiske innfallsvinkler. De fleste spørsmålene gikk generelt på arbeid innenfor kunnskapsnettverk og på GKP som innovasjonsbedrift. Noen av spørsmålene gikk også på informantenes opplevelse av nettverkssatsningen på informasjonssikkerhet, spesielt på Security Valley. Det var disse spørsmålene jeg opplevde at jeg fikk best data på, og disse gjorde meg mer nysgjerrig på prosjektet Security Valley. Etter hvert fokuserte jeg sterkere på Security Valley, og bestemte meg for å benytte dette som mitt case. Intervjuguiden ble dermed også mer spisset mot å hente informantenes erfaring med Security Valley. Antakelsen bak dette var at ved å se på utfordringer ved Security Valley-satsningen vil man kunne hente ut erfaring som ligger hos aktørene om hvordan samarbeid innenfor innovasjonsnettverk bedre kan tilrettelegges.

Casestudium som metodikk har blitt kritisert på ulike grunnlag. Flyvberg (2004) peker på fem vanlige misforståelser omkring casestudium: i) generell teoretisk kunnskap (kontekstuavhengig) er mer verdt enn konkret, praktisk (kontekstavhengig) kunnskap; ii) man kan ikke generalisere ut fra ett enkelt case; iii) casestudier er mest velegnet til å generere hypoteser, mens disse bedre kan testes med andre forskningsmetoder; iv) casestudien har en fordreining (*bias*) mot verifisering av forskerens antakelser; v) det kan vanskelig utledes teori fra ett enkelt case (Flyvberg 2004: 391). Muligheten for generalisering ut fra casestudier vil vi komme tilbake til i forbindelse med diskusjonen av kvalitetskriteriene for kvalitativ forskning. Av dette vil jeg også vise hvordan casestudiet er velegnet til både å utvikle og teste hypoteser på en kvalitetsmessig god måte. Som tilsvar på den øvrige kritikken viser Flyvberg til at generalisert teoretisk kunnskap ofte ikke er beskrivende for samfunnsforskning, siden menneskelig handling ikke kan beskrives innenfor avgrensede rammer. Casestudier har heller ingen større fordreining mot verifisering enn andre forskningsmetoder. Når det gjelder kritikken om at det vanskelig kan utledes generalisert teori fra casestudier er dette en kritikk som faller på siden av

saken, siden casestudier ofte bør leses som narrativer om spesifikk kunnskap (Flyvberg 2004). Dette er også tilfellet for denne casestudien av Security Valley.

3.2 Grounded theory

Dey (2004) beskriver utviklingen av grounded theory som metodologi. Grounded theory bygger på fire grunntanker: i) ideer og fenomener skal *oppdages* gjennom empirien og teori skal genereres gjennom empiri. Det er altså ikke testingen av ulike teoretisk funderte antakelser som er utgangspunktet for en studie; ii) i grounded theory benytter man *teoretisk sampling*, det vil si at informanter velges suksessivt etter hvilke empiriske interesseområder som forskeren finner i tidligere intervjuer. Dette betyr at analyse og datainnsamling er ikke er adskilte prosesser; iii) grounded theory er først og fremst en kvalitativ metode, og baserer seg gjerne på intervjuer som i starten av datainnsamlingen er åpne, mens de fokuseres mer i løpet av prosessen; iv) analyse skjer ved å kode data inn i kategorier, for så å sammenlikne disse; v) datainnsamlingen avsluttes når det oppstår metning, det vil si når ny kunnskap ikke lenger genereres i intervjuene (Dey 2004: 81). Min forskningsmetode i denne studien er i stor grad i tråd med grounded theory retningen. Jeg har ikke bevisst fulgt en slik forskningsmetode, noe som vil si at jeg ikke rigid har fulgt retningslinjene gitt av denne metoderetningen i min forskning. Jeg skal likevel gå inn på noen elementer ved grounded theory som er relevant i denne sammenhengen.

Som vi allerede har vært inne på er det ikke vitenskapsteoretisk uproblematisk å generalisere ut fra (induktive) casestudier. Ved å tenke grounded theory kan man argumentere for at denne kritikken i liten grad er treffende for denne studien. Dey (2004) hevder, på tross av hva som er en gjennomgående oppfattelse i metodelitteraturen, at grounded theory ikke er en induktiv forskningsmetode. I stedet vil det være mer nyttig å tenke på grounded theory som en abduktiv metode. Det vil si at det ikke er generalisering som først og fremst er ønskelig. Derfor benytter man også en teoretisk kontra representativ sampling. Dey forklarer det slik: "Unlike deduction, the result does not follow logically from the premises: abduction offers a plausible interpretation rather than producing a logical conclusion" (Dey 2004: 91). Det kan lett oppfattes slik at grounded theory sier at forskeren ideelt sett ikke bør ha noen teoretisk ballast med seg inn i forskningsprosessen. Dey presiserer dette: Teoretisk kunnskap hos forskeren er bra og nødvendig, men det er uheldig dersom forskeren lar seg *styre* av teori (ibid.). Som nevnt utformet jeg de tidlige intervjuguidene på bakgrunn av teori og begreper jeg hadde en antakelse om at kunne være

relevante. Gjennom prosessen med datainnsamling og etterarbeid kom ny teori og nye begreper til, mens annen teori og begreper falt bort. Et eksempel på dette er begrepsparet *innovasjonsnettverk* og *innovasjonsinfrastruktur* som kom opp under et intervju. Disse viste seg å bli en bærende del i denne studien. Hvordan kan man bruke spenningen mellom disse begrepene til å si noe om stabilisering av innovasjonsnettverk?

Denne studien er ikke utført i samsvar med grounded theory når det gjelder utvalgsstrategi. Mens teoretisk utvalg er sentralt i grounded theory, har mitt utvalg vært gjort i forkant av datainnsamlingen. På grunn av tidspresset ble intervjuer med de 10 første informantene avtalt før jeg startet datainnsamlingen. De tre siste intervjuene ble imidlertid avtalt etter at jeg hadde funnet oppgavens fokus. Jeg har også innhentet skriftlig data underveis i prosjektet. En nærmere presentasjon av datagrunnlaget følger i de neste delkapitlene.

3.3 Datainnsamling og intervjuguide

Datainnsamlingen er gjort ved intervjuer med informanter i et strategisk utvalg. I strategiske utvalg er informantene trukket på grunnlag av antakelsen om at de har informasjon som er nyttig i forhold til prosjektets problemstilling (Thagaard 2003). Jeg ønsket å snakke med informanter som på ulik måte hadde erfaring med arbeid innenfor innovasjonsnettverk, og som spesielt kunne belyse caset. Informanter er hentet fra ledelse og inkubatorbedrifter innenfor Gjøvik Kunnskapspark, Høgskolen i Gjøvik og andre bedrifter og aktører som har vært involvert i Bluelight og/eller Security Valley. Disse kategoriene er ikke gjensidig utelukkende. Det er gjennomført 13 intervjuer, hvorav ti har vært personlige møter og tre på telefon. Jeg har ikke jobbet ut fra noe ”tak” på antall informanter, men valgte å avslutte datainnsamlingen da jeg opplevde et metningspunkt i informasjonen. Følgende er en kort anonymisert presentasjon av informantene som har deltatt i datainnsamlingen:

- **Jens** har god kjennskap til nettverkene Bluelight og Security Valley, samt delprosjekter og samarbeidspartnere innenfor disse nettverkene.
- **Idar** har god kjennskap til både innovasjonsnettverksaktiviteten og innovasjonsinfrastrukturen innenfor Gjøvik Kunnskapspark.
- **Kalle** arbeider i en av de sentrale bedriftene i nettverket, og har erfaring med innovasjonsvirksomhet. Han kjenner også godt til innovasjonsnettverksaktiviteten i Gjøvik Kunnskapspark.

- **Tom Anders** kjenner også godt til nettverkene for informasjonssikkerhet, først og fremst Security Valley, men også Bluelight. Han har også god oversikt over innovasjonsinfrastrukturen i GKP.
- **Tore** er først og fremst en fagperson innenfor informasjonssikkerhet i en relatert organisasjon, men kjenner også godt til Bluelight og Security Valley.
- **Trond** arbeider med informasjonssikkerhet i en organisasjon utenfor kjerneområdet. Han har en viss kjennskap til Security Valley, men var først og fremst involvert i nettverket gjennom delprosjekter.
- **Linn** er først og fremst fagperson innenfor regional innovasjon, og arbeider i en relatert organisasjon.
- **Cato, Jan Petter, Stine Mette, Stein Ove, Jarle og Karl** representerer småbedrifter som er/var relatert til inkubatorvirksomheten til GKP. Disse informantene har i varierende grad kjennskap til Bluelight og Security Valley.

Intervjuene har, med ett unntak, hatt en varighet på mellom 25 og 45 minutter. Jeg har fått god hjelp fra daglig leder i Gjøvik Kunnskapspark til forslag til hvem jeg kunne kontakte for intervju. Noen av disse forslagene er fulgt opp, andre er det ikke. GKP har ingen komplett oversikt over mitt utvalg av informanter. I tillegg har NCE-søknaden fra Security Valley blitt gjort tilgjengelig for meg gjennom GKP. Jeg har også basert analysen på informasjon hentet fra nettsiden securityvalley.no, samt feltnotater fra telefonsamtaler og e-postutvekslinger med relevante personer.

I utgangspunktet ønsket jeg at intervjuguiden skulle legge rammene for et semi-strukturert intervju for å gi rom mest mulig ny data. Som nevnt hadde jeg på tidspunktet da datainnsamlingen startet et bredt interesseområde. Jeg ønsket å vite noe om hvordan kommunikasjon bidrar til å stabilisere et nettverk for kunnskapsdeling og innovasjon. På grunn av dette gikk jeg også relativt bredt ut i valget av informanter. Jeg ønsket å snakke med noen som hadde erfaring innenfor innovasjonsledelse, noen som hadde erfaring fra innovasjonsnettverkene Bluelight og Security Valley, noen som hadde erfaring som gründere/inkubatorbedrift og noen som jobbet på forskningssiden. Dette betydde at ikke alle spørsmålene jeg hadde var relevant for den enkelte informant. Intervjuguiden ble dermed tilpasset i henhold til dette. Intervjuguiden som lå til grunn for de første ti intervjuene var på rundt 30 spørsmål delt i tre hovedkategorier: 1) Deg og ditt arbeid/din bedrift innenfor Gjøvik Kunnskapspark/Security Valley, 2) Hvordan hankses med

usikkerhet i innovasjon, 3) Kommunikasjon, kunnskapsdeling og innovasjon. De to siste intervjuguidene inneholdt 17 spørsmål uten noen tematisk strukturering. Intervjuguidene finnes i vedlegg 1. Ett intervju ble på grunn av tidsknapphet gjennomført ustrukturert uten intervjuguide.

Som en konsekvens av den eksplorerende innfallsvinkelen til området jeg ønsket å studere, avgrenset jeg intervjuguiden rundt en del teorier og begreper som jeg antok at kunne være relevante å snakke med mine informanter om. I ettertid ser jeg at dette gjorde intervjuguiden for omfattende, og at det på grunn av dette oppstod tidspress på meg som intervjuer i intervjusituasjonen. Dette ga meg mindre mulighet til å følge opp interessante vendinger i intervjuene. Når det er sagt, opplevde jeg ikke intervjuene som svært strukturerte. Jeg gav rom til informantene til å følge sine resonnementer, og stilte oppfølgingsspørsmål der jeg syntes det var nødvendig. Rekkefølgen på spørsmålene i intervjuguiden ble også avveket ved de fleste intervjuene nettopp for å følge opp informantens svar og resonnementer. I de tre siste intervjuene hadde jeg et klarere fokus på hva min oppgave skulle dreie seg om, og intervjuguiden var dermed mer fokusert. Som en konsekvens opplevde jeg at jeg hadde bedre tid i intervjusituasjonen, og at det var større rom for å gå utenfor de konkrete spørsmålene jeg hadde i intervjuguiden.

3.4 Anonymisering, analyse og bearbeiding av data

Flere av informantene er hentet fra bedrifter i og rundt den fysiske lokasjonen til Gjøvik Kunnskapspark. I et relativt lite kontormiljø som GKP er det vanskelig å sikre full diskresjon rundt deltakelse som informant. Det er likevel kun jeg som har den fulle oversikten over informantene som har deltatt i datainnsamlingen. Jeg har gitt skriftlig informasjon om informert samtykke til mine informanter, og behandlet sammendragene fra intervjuene anonymt⁵. Transkripsjoner og lydopptak fra intervjuene har blitt behandlet konfidensielt. Alle siteringer som fremkommer i denne teksten er anonymisert.

Alle intervjuer er transkribert. For analytiske formål har jeg valgt å utarbeide tematiske sammendrag av hvert av intervjuene. I prosessen fra transkripsjon til sammendrag har jeg gjort en utvelgelse av hvilke data som er relevant for den videre analysen, og sortert disse tematisk. Jeg har brukt en enkel manuell fargekoding for å skille og sammenlikne analysekategorier.

⁵ Samtykkeerklæring finnes i vedlegg 2.

Gjennom Gjøvik Kunnskapspark har jeg fått tilgang til søknaden om status som Norwegian Centre of Expertise for Security Valley. Søknaden er i stor grad benyttet som sekundærdata, og for å få oversikt over visjon, målsettinger og organisasjon innenfor Security Valley. Jeg har ikke hatt noen konkret analysemetode for bruken av dokumenter som datagrunnlag i denne masteroppgaven. Følgeforskningen på Bluelight utført av Svein Bergum ved Østlandsforskning AS har også blitt flittig brukt på ulike stadier av prosjektet. Disse har vært viktige for å gi en grunnleggende forståelse av samarbeidsform, visjon og klima rundt nettverk for informasjonssikkerhet i Innlandet. Heller ikke disse rapportene har vært gjenstand for noen systematisk innholdsanalyse. Sist men ikke minst har også securityvalley.no vært en viktig ressurs for å få innblikk i arbeidsform og aktivitet i nettverket. Jeg har ikke gjort noen systematisk innholdsanalyse av nettsiden.

3.5 Kvalitetskriterier

Begrepene reliabilitet, validitet og generaliserbarhet viser til ulike kvalitetskriterier ved forskning. Reliabilitet omhandler hvorvidt gjentatte tester av samme fenomen med samme måleinstrument gir samme resultat. Validitet går på om studien klarer å måle det den ønsker å måle (Ringdal 2007). Formålet med denne studien er å finne ut hvordan man kan stabilisere nettverk for kunnskapsdeling og innovasjon. Dette illustreres ved å analysere ulike sider ved innovasjonsnettverket/næringsklyngen Security Valley. Først og fremst er det viktig å drøfte begrepsvaliditeten. Nøkkelbegrepene i denne studien er innovasjon, klynge, nettverk, kompetanse, kunnskapsdeling og kommunikasjon med mer. Spørsmålet blir da i hvilken grad min oppfattelse av disse begrepene stemmer over ens med informantenes tolkning. Stort sett opplevde jeg en delt forståelse av begrepsbruken mellom intervjuer og informant. I den grad det har vært usikkerhet har jeg presisert begrepsbruken. Ordet "kunnskapsnettverk" har jeg opplevd som problematisk, og dermed gått bort fra å bruke det. I kvalitativ forskning er vurderingen om begrepsvaliditet nødvendigvis knyttet til vurderingen av umiddelbar validitet (*face validity*). Umiddelbar validitet knytter seg til den skjønsmessige vurderingen av om spørsmålene fanger opp begrepene og fenomenene forskeren er interessert i (Ringdal 2007). Reliabilitet og validitet kan være vanskelig å drøfte i forhold til kvalitative undersøkelser. Dette gjelder i høyeste grad også generaliserbarheten, som vi har vært inne på. I det følgende vil begrepene troverdighet, bekreftbarhet og overførbarhet drøftes som kvalitetsindikatorer for denne oppgaven.

Thagaard skriver at *troverdigheten* til en undersøkelse knytter seg til både "kvaliteten av den informasjonen prosjektet baserer seg på, og til vurderinger av hvordan

forskeren anvender og videreutvikler informasjon fra felten” (Thagaard 2003: 178). Troverdigheten må vurderes ut fra forskerens redegjørelse for utviklingen av de data og funn som presenteres i prosjektrapporten. Jeg har benyttet dette kapitlet for en slik redegjørelse. Oppsummert kan man si at informasjonskvaliteten har blitt ivaretatt ved en skjønnsmessig vurdering av begrepsvaliditeten, de teoretiske rammene for intervjuguiden og måten rådata har blitt behandlet på. Videreutviklingen av informasjon er gjort ved å kategorisere og kode data for analyse i henhold til gjeldende standarder (se for eksempel Strauss og Corbin 1990). *Bekreftbarhet* er knyttet til at forskerens tolkning av data skal kunne etterprøves og bekreftes av annen forskning. Dette går på vurderingen om de tolkninger som er gjort er mer relevante enn andre plausible tolkninger av funnene som ligger i datamaterialet. For å sikre dette har jeg samarbeidet aktivt med min veileder gjennom analyseprosessen, og jeg har også gått tilbake og snakket med tre av mine informanter for å spørre om deres synspunkt på de tolkningene som er gjort. Grunnlaget for bekræftbarheten er ivaretatt gjennom min redegjørelse av prosjektets fremgangsmåte i dette kapitlet.

Som vi har vært inne på er det ikke uproblematisk å generalisere ut fra en studie av et enkelt case. Flyvberg påpeker at dette ikke nødvendigvis er en sannhet, og at det heller ikke er ønskelig å generalisere ut fra case:

One can often generalize on the basis of a single case, and the case study may be central to scientific development via generalization as supplement or alternative to other methods. But formal generalization is overvalued as a source of scientific development, whereas "the force of example" is underestimated (Flyvberg 2004: 395).

Fra dette følger også at casestudier har verdi utover generering av hypoteser til oppfølging i senere studier. Dey (2004) omgår generaliseringsproblemet ved å understreke at forskning innenfor grounded theory metodikk ikke har som formål å generalisere, siden den verken er fundert på deduksjon eller induksjon, men snarer abduksjon. Mer verdifullt som kvalitetsmål for denne masteroppgaven er derfor Thagaards (2003) begrep *overførbarhet*. Overførbarhet innebærer en rekontekstualisering ved at den teoretiske forståelsen som er knyttet til ett enkelt prosjekt settes inn i en videre sammenheng. På den måten kan en enkelt undersøkelse bidra til en mer generell teoretisk forståelse (ibid.). Overførbarhet må dermed sees i sammenheng med bekræftbarheten, som jeg har redegjort for ovenfor.

4. Innovasjonsnettverk for et innovativt klima i Innlandet?

Innovasjon er nærmest som et politisk buzzword å regne, og er svært aktuelt i forhold til distriktspolitikken. Dette viser seg særlig gjennom det offentlige virkemiddelapparatet som skal ivareta den helhetlige tenkningen rundt spredt innovasjon (Hauge et al. 2009), og de SIVA-eide kunnskapsparkene er et vesentlig virkemiddel for å koble næringsliv, gründere og høyskolemiljøer. I dette kapittelet vil jeg først presentere begrepet *innovativt klima* som oppstod i ett av intervjuene som et begrep for å beskrive den overordnede holdningen til innovasjon og samarbeid innenfor det regionale innovasjonssystem i Innlandet generelt, og Gjøvik-området spesielt. Jeg vil også gi en kronologisk presentasjon av innovasjonsnettverkene Bluelight og Security Valley, og til slutt reise noen spørsmål rundt hvorvidt og hvordan Security Valley kan sies å ha bidratt til å skape og utvikle et lokalt og regionalt innovativt klima. Hvor viktig er den overordnede *holdningen* blant innovasjonsaktører til betydningen av samarbeid og innovasjon, og hvordan har gode holdninger til klynge- og nettverkssamarbeid blitt realisert gjennom Bluelight og Security Valley?

4.1 Et *innovativt klima* – helhetlig tankegang rundt regionale innovasjonsnettverk

Gjennom mine intervjuer til denne studien ble jeg klar over at tanken rundt regional og lokal innovasjon og næringsutvikling var godt forankret i aktørene innenfor nettverket av bedrifter og organisasjoner jeg har hentet mine informanter fra. Det var derimot delte meninger om hvorvidt det finnes en helhetlig tilnærming til regional innovasjon på tvers av næringsliv og innovasjonsaktørene i Innlandet, og spesielt i Gjøvik-regionen. Flere informanter forteller at på tross av at koblingen mellom høyskole og kunnskapspark fungerer tilfredsstillende oppleves det som vanskelig å aktivisere lokalt næringsliv i tilstrekkelig grad for å delta i innovasjonsprosesser. Daglig leder i Gjøvik Kunnskapspark beskrev det slik:

Du kan si at mandatet eller oppdraget til en kunnskapspark er definert fra SIVA sin side (...) at man skal være et bindeledd mellom høyskole og næringsliv. Og vi føler at vi er gode på høyskolen, men vi er ikke gode nok på næringslivet. Og til dels kan du si at vi er det på Raufoss innenfor industriparken der, men vi er alt for tynne på de øvrige. (...) Og hos næringslivet tror jeg man har mer sånn skuldertrekk. Som jeg nevnte tidligere, vi har for så vidt ikke klart å ufarliggjøre oss eller tillitsgjøre oss helt overfor næringslivet. At vi kan være et godt instrument for dem. Så det er kanskje det området vi har minst tillit på da, for å bruke det begrepet. Men det går på manglende kompetanse igjen på hva vi holder på med.

Informanten knytter tillitsgjøring til utviklingen av fruktbare relasjoner til det lokale næringslivet. Han peker på behovet for økt kompetanse omkring regionale

innovasjonsaktører og hvordan disse tilrettelegger for innovasjon mellom lokalt næringsliv, gründerbedrifter og de regionale høyskolene. Flere av informantene understreker viktigheten av å ha gode faglig fokuserte prosjekter gående over flere år for å skape et klima for innovasjon. En gjennomgående oppfattelse er at prosjektbasert samarbeid mellom næringslivsaktører, høyskole og gründere øker den gjensidige tilliten mellom aktører som er viktige i det regionale innovasjonssystemet.

Begrepet *innovativt klima* oppstod i ett av intervjuene som en forståelsesramme rundt å ha gode betingelser for lokal/regional innovasjon og innovasjonsnettverk. I følgende sitat peker informanten på det jeg opplever som den samme problemstillingen som daglig leder i Gjøvik Kunnskapspark belyser; nettopp at det er vanskelig å tillitsgjøre seg blant lokalt næringsliv. Mens informanten i forrige sitat peker på manglende kompetanse rundt kunnskapsparken som innovasjonsbedrift som forklaringsvariabel, peker informanten Linn på holdninger i næringslivet som avgjørende for å skape et innovativt klima:

Jeg tror klima har veldig mye å si, jeg! At det er et klima som fremmer innovativ tenkning. Og det er undervurdert i mange sammenhenger. (...) Men jeg tror problemet er likt både på Lillehammer, Gjøvik og Hamar. At vi har et næringsliv som ikke nødvendigvis er fryktelig opptatt av innovasjon. Mer av kostnadsinnsparinger, effektivisering og rasjonalisering. Og det er ikke noe galt i det, men det er dette med klima igjen. Og jeg tror at det er litt sånn at man setter seg på gjerdet litt og ser ut i manesjen: ”Hva er det de driver og roter med nå da tro?” Også melder man seg på hvis det skjer noe veldig stort der, og det virker vellykket. Man bidrar liksom ikke i utgangspunktet til å få det vellykket ved å involvere seg.

Sitatet setter ord på hva jeg gjennom en rekke intervjuer og telefonsamtaler har oppfattet at er en del av problemet med å stabilisere innovasjonsnettverk som bidrar til det helhetlige innovative klimaet i området. Når det gjelder selve begrepet *et klima som fremmer innovativ tenkning* – eller et *innovativt klima*, som jeg noe forenklet velger å kalle det – viser det til noe av det samme som Hauge et al. (2009: 127) i sin modell for regionale innovasjonssystemer viser til som ”sosial kapital og kultur”. Hos Hauge et al. er sosial kapital og kultur ”limet” som binder *kunnskapsinfrastruktur, regionale myndigheter og virkemidler, det industrielle system og annen infrastruktur* sammen i et regionalt system for kunnskapsflyt og læring. Begrepet innovativt klima oppfatter jeg at i tillegg har et normativt element som går på den overordnede *holdningen* blant næringsliv, innovasjonsbedrifter, gründere, offentlige organisasjoner og andre som arbeider med regional innovasjon. Dette ligger også tett opp mot buzz-begrepet som kan forstås som kommunikasjonen som tilrettelegger for et pulserende og inspirerende miljø (Bathelt et al. 2004). Begrepet innovativt klima ble brukt i flere av de senere intervjuene for å snakke om

hvilke holdinger, fokusområder og aktører som er viktige for å skape vellykkede innovasjonsnettverk. I de neste delkapitlene vil jeg redegjøre for hvordan en rekke næringslivs- og kompetanseaktører har bidratt til å utvikle et innovativt klima rundt informasjonssikkerhet i Innlandet fra år 2000 frem til i dag.

4.2 Informasjonssikkerhet i Innlandet 2000 – 2001

Bakgrunnen for satsningen på informasjonssikkerhet i Innlandet er en kompleks og vanskelig historie å få oversikt over i detalj. Svein Bergum i Østlandsforskning var i perioden høsten 2002 til 2006 observatør i Arena Informasjonssikkerhet, bedre kjent som Bluelight. Bergum presenterer i sine rapporter et svært grundig arbeid rundt kartlegging og analyse av de ulike fasene av samarbeidet rundt informasjonssikkerhet i Innlandet. Dette kapittelet vil i stor grad basere seg på Bergums rapporter og artikler.

Før starten på 2000-tallet var informasjonssikkerhetsmiljøet i Innlandet i liten grad kartlagt, og det fantes liten kommunikasjon mellom de ulike aktørene. Bergum og Nyhus (2004: 11) refererer til Ericsson et al. (2002) sin kartlegging av IKT- og mediesektoren i Innlandet når de fordeler de noe over 40 aktørene innenfor informasjonssikkerhet pr. 2001 i fire kategorier: i) leverandører; ii) store brukergrupper; iii) offentlig virksomhet; iv) andre små og mellomstore bedrifter. Informasjonssikkerhetsbedrifter sees som en del av IKT-bransjen, og gjelder spesielt den virksomhet som vedrører ”beskyttelse mot brudd på konfidensialitet, integritet eller tilgjengelighet av den informasjon som blir behandlet i et system, eller beskyttelse av informasjonssystemer og nett i seg selv” (Fornyings- og administrasjonsdepartementet 2007: 5). Etableringen av et kompetansenettverk for informasjonssikkerhet i Innlandet synes å ha skjedd på bakgrunn av flere sammenfallende faktorer som til sammen skapte et gunstig miljø for opprettelsen av et slikt kompetansenettverk. En informant pekte spesielt på den samfunnsmessige utviklingen av en ny teknologihverdag som bakgrunnen for etableringen av et samlet miljø rundt informasjonssikkerhet i Innlandet. Bergum (2006) deler i sin evalueringsrapport Bluelight-prosjektet opp i tre faser; forstudiet, forprosjektet og hovedprosjektet. Dette delkapittelet vil følge denne kronologien og i tillegg presentere Security Valley, som på mange måter kan sees som videreutviklingen av Bluelight etter 2007.

Kartleggingen av IKT- og mediesektoren i Innlandet ble utarbeidet på oppdrag fra SND (nå Innovasjon Norge) i forbindelse med forprosjektet Regionale Innovasjonspiloter, Innovasjon Innlandet (Bergum og Nyhus 2004). Disse undersøkelsene lå til grunn da det i

2000 og 2001 ble startet samtaler rundt behovet for kompetanseheving mellom ulike aktører innenfor informasjonssikkerhet i Innlandet. På denne tiden var det ikke lagt planer for etableringen av noe mer generelt nettverk. På bakgrunn av intervjudata som ligger til grunn for ØF-rapporten *Evaluering av Bluelight*, beskriver Bergum begynnelsen av samarbeidet slik:

Det er litt nyanser mellom informantene med hensyn til når startskuddet for nettverket var, og ”hvem som tok hvilke telefoner”. Hos enkelte i Telenor, Jørstadmo-miljøet og hos leverandøren Thales, hadde det i lenger tid vært snakket om ”å få til noe innen informasjonssikkerhet i Innlandet”. Den som flest nevner som en nøkkelperson i starten er sikkerhetsdirektør Jan Erik Svensson i Telenor (Bergum 2006: 21).

På våren 2000 hadde også SND sett at informasjonssikkerhet hadde dukket opp som ett av flere satsningsområder som var utpekt av en regional arbeidsgruppe. Dette var samme år som Jan Erik Svensson i Telenor første gang hadde tatt kontakt med SND i forbindelse med informasjonssikkerhet som potensielt satsningsområde (Bergum 2006).

På samme tid som SND foretok kartleggingen av informasjonssikkerhet som mulig satsningsområde, ble Gjøvik Kunnskapspark opprettet. Daværende daglig leder i GKP hentet inn Svein Pettersen som hadde kompetanse på informasjonssikkerhet, og som tidligere hadde jobbet sammen med Svensson i Telenor. Pettersen ble fra starten av forprosjektet i 2001 prosjektleder for Bluelight. Forprosjektet handlet i det vesentligste om samarbeid for etableringen av et masterstudium i informasjonssikkerhet ved Høgskolen i Gjøvik. Prosjektgruppen ble etablert høsten 2001 og hadde finansiering fra Kommunal- og regionaldepartementet. Våren 2002 ble studieplanen for masterstudiet i informasjonssikkerhet vedtatt, og de første studentene begynte allerede høsten 2002 (Bergum 2006). Tilretteleggingen av masterstudiet var starten på etableringen av et tungt fagmiljø på informasjonssikkerhet på HiG. Dette fagmiljøet har videreutviklet seg, og vært sterkt involvert i prosjektet Bluelight og delvis i Security Valley.

4.3 Bluelight – regionalt kompetansenettverk for informasjonssikkerhet

Hovedprosjektet var fra høsten 2002 knyttet opp mot Arenaprogrammet til Innovasjon Norge, SIVA og Norges Forskningsråd. Arenaprogrammet skal bidra til å styrke næringsklynger gjennom finansiering fra Innovasjon Norge over en treårsperiode. Programmet legger vekt på en styrking av aktuelle næringsområder gjennom et aktivt nettverkssamarbeid mellom næringsliv, kunnskapsmiljøer og offentlige instanser⁶.

⁶ Innovasjon Norge, http://ekstranett.innovasjonnorge.no/templates/Page_Meta_56170.aspx (udatert, hentet 17.02.2011).

Hovedprosjektet på informasjonssikkerhet gikk fra 2002 under betegnelsen Arena Informasjonssikkerhet. Det ble da opprettet en styringsgruppe som skulle ta seg av de strategiske oppgavene. Det ble også organisert en drivernode som skulle utføre de strategiske arbeidsområdene definert av styringsgruppen. Fra 2004 besluttet styringsgruppen å fjerne drivernoden, og i stedet utføre arbeider som delprosjekter (Bergum og Nyhus 2004)⁷. Bergum (2006) beskriver Bluelight som et samarbeid som i både arbeidsform og fokus utviklet seg gjennom årene som arenaprojekt. I 2003 fokuserte man bredere enn tidligere, og endret også navnet til Bluelight som skulle gi assosiasjoner til sikkerhet i betydningen “policing”:

[det var] mye fokus på visjoner, målsettinger, aktivitetsplaner for nettverket, samt en ”brandingprosess”. (...) Begrepet ”NIS-nettverket: næringsklynge for informasjonssikkerhet” var for komplisert. Etter en kreativ prosess, ble begrepet ”Bluelight” tatt i bruk i midten av 2003, med undertittel: ”enabling security”(Bergum 2006: 22).

Arbeidet som fortsatte i 2004 var fortsatt preget av samarbeid på kompetansesiden, og i mindre grad rettet mot kommersielt arbeid. Hovedoppgavene for dette året gikk på etablering og utvikling av foreningen Kommunal Informasjonssikkerhet (KinS), og å ivareta samfunnsrettede oppgaver som informasjonsarbeid via nettsiden bluelight.no, relasjonsbygging til brukergrupper og det offentlige. Man arbeidet også med synliggjøring av nettverket via mediedekning av de viktigste aktørene, og man startet å diskutere muligheten for å få status som Norwegian Centre of Expertise (NCE). Ved HiG arbeidet man med å videreutvikle masterstudiet og Norwegian Information Security Laboratory (NISlab), som er betegnelsen på forskningsmiljøet ved Avdeling for Informatikk og Modellteknikk (ibid.).

I 2005 var Bluelight involvert i flyttingen av Norsk Senter for Informasjonssikring (NorSIS) fra Trondheim til Gjøvik. NorSIS sorterer under Fornyings-, administrasjons- og kirkedepartementet, og driver opplysning, rådgivning og holdningsskapende arbeid innenfor informasjonssikkerhet. Sammen med utviklingen av NISlab og etableringen av bachelor og PhD i informasjonssikkerhet ved HiG, vokste kompetansemiljøet på Gjøvik ytterligere. På den kommersielle siden etablerte man inkubatoren Security Incubator (SECTOR) innenfor Gjøvik Kunnskapspark, og det ble arbeidet med selskapet Security Partner som ble opprettet sent i 2004. Security Partner skulle samle inn best practice innenfor blant annet risikoanalyse fra andre næringsaktører i nettverket, og selge konsulenttjenester. Security Partner slo aldri an, og ble ikke videreført. Informanten Idar

⁷ Organisasjonskartet for nettverket finnes i vedlegg 3.

forklarte at det var fordi *“det begynte liksom å bli litt penger og den type ting inni bildet. Nettverket fungerte egentlig kun når det var fundamentale utfordringer og mer essensielle ting å jobbe med, som kompetanse”*. I tillegg ble det avholdt workshops som blant annet tok for seg et samarbeidsprosjekt med Nammo AS, og produktet ”sikkerhetskortet”. Man ønsket også å utvikle prosjekter og gå inn på anbud i fellesskap. I 2005 begynte man også å tenke internasjonalt. Først og fremst gjennom tilknytningen til selskaper som Thales, PricewaterhouseCoopers og Ibas, men også gjennom en studietur til Silicon Valley (Bergum 2006).

Perioden som arenaprosjekt skulle opprinnelig avsluttes i årsskiftet 2005/2006. Innovasjon Norge bevilget likevel midler til et halvt års ekstra drift. De viktigste arbeidsoppgavene som var på agendaen i 2006 var hva Bergum (2006: 24) beskriver som ”kritiske nettverksaktiviteter”, mer presist; sterkere tilknytning mellom NorSIS og NISlab inn mot Bluelight, samt å ta inn nye aktører og utvikle en større mulighet for uformelle møtepunkter. Det ble også gått inn for videreføring av arbeidet med SECTOR og prosjektet med Nammo fra 2005. Mye av arbeidet gikk også på å videreføre Bluelight på permanent basis uten arenastøtte. Ved utgangen av arenaperioden i midten av 2006 overtok Christian Meyer, som hadde vært involvert i prosjektet i en tid, som prosjektleder for Bluelight mens Svein Pettersen gikk over i stillingen som daglig leder i Gjøvik Kunnskapspark.

Bluelight var basert på fem delprosjekter: i) utdanning ved etablering av master- og bachelorstudium ved HiG; ii) forskning, ved bruk og formidling av NISlab ved HiG; iii) opprettelsen av ulike samarbeidsarenaer mellom brukergrupper; iv) samfunnsinformasjonsvirksomhet ved etableringen av NorSIS på Gjøvik; v) næringsutvikling ved etableringen av Security Incubator innenfor Gjøvik Kunnskapspark⁸. Svein Bergum presenterer i evalueringsrapporten for Bluelight status for oppnåelsen av de ulike målsetninger pr. 2006. Følgende tabell er basert på Bergums (2006: 32) fremstilling, og er oppdatert med mine kommentarer i høyre kolonne:

⁸ Innovasjon Norge, http://ekstranett.innovasjon Norge.no/templates/Page Meta_57577.aspx (udatert, hentet 24.2.2011)

Mål	Måloppnåelse	Kommentar 2011
Opprettelse av bachelor- og masterstudium i informasjonssikkerhet ved HiG.	Oppfylt.	HiG har program for bachelor, master og PhD i informasjonssikkerhet.
Visjon om å bli anerkjent som ett av de ledende kompetansenettverk innenfor informasjonssikkerhet i Europa.	Kommet et stykke på vei. Ledende i Norge, noe internasjonalt.	En av mine informanter hevder at kompetansen på Gjøvik pr. 2011 kun overgås av et par miljøer i Tyskland og England.
Bistå videre i utviklingen av NISlab og befeste dette som det faglige tyngdepunktet i nettverket.	Oppfylt.	Studier og FoU har vokst kraftig. Oppdragsforskning noe mindre pr. 2006. Parallelt med NISlab, åpnet HiG 15.02.2011 Biometrilab som skal fokusere på sikre biometriløsninger.
Delaktige i minst tre produkt/tjenestelanseringer.	Delvis oppfylt. To produktlanseringer: NonStop og Sikkerhetskortet.	Disse produktene finnes ikke lenger i 2011.
Bidra til opprettelse av tre virksomheter.	Oppfylt gjennom etableringen av Security Partner og NorSIS på Gjøvik, Sparebank 1 og Thales på Lillehammer, og Forsvarets Sikkerhetsavdeling på Jørstadmoen.	Security Partner og Thales avdeling på Lillehammer er lagt ned.
Synliggjøre nettverk og kompetanse.	Oppfylt.	Godt kjent i fagmiljøet. NorSIS opplever stor arbeidsmengde. Fra internundersøkelsen i 2006 mente mange at nettverket er for lite kjent hos forretningsforbindelser.
Bidra til to bransjearenaer og en regional arena.	Delvis oppfylt. KinS i kommunal sektor, regionalt Sikkerhetsforum.	NorSIS arrangerer blant annet konferansen Sikker.info årlig.
Legge grunnlag for videreføring gjennom NCE.	Ikke oppfylt. Søknad om NCE avslått.	Bluelight ble videreført som et medlemsbasert nettverk til det våren 2008 gikk over i Security Valley. Heller ikke Security Valley fikk tilslag på sin NCE-søknad.

Tabell 1: Måloppnåelse for Bluelight. Basert på Bergum (2006: 32).

Fra en internundersøkelse fra 2006 fremgår særlig tre punkter med forbedringspotensial i Bluelight. Dette gjelder samarbeid i nye prosjekter, internasjonale kontrakter/prosjekter og sikre arbeidsplasser (Meyer 2006, i Bergum 2006: 34). Dette viste at det pr. september 2006 var behov for et økt fokus på de kommersielle sidene ved nettverket.

Andersen (2006) studerer samarbeidsfaktorer og informasjonsflyten i Bluelight, og knytter dette til Bathelt et al. (2004) og Boschmas (2005) teori rundt buzz og nærhetsdimensjoner. Hun peker på at Bluelight var en vesentlig faktor for å etablere lokal buzz rundt informasjonssikkerhet i Innlandet, og fremhever særlig prosjektleder Svein Pettersens rolle som navet i nettverket Bluelight. Videre viser hun til at Bluelight er et eksempel på at buzz kan skapes uten samlokalisering. Dette beror på å bygge en tillit som ligger til grunn for informasjonsdeling og samhandling via IKT. Hun peker på at en vesentlig årsak til at Bluelight fungerte godt som samarbeidsforum var den kognitive nærheten mellom deltakerne; velutdannede, middelaldrende menn med grovt sett samme fagfelt. I tillegg fremhever hun at Arenaprogrammet har vært vesentlig i forhold til å skape en institusjonell ramme rundt prosjektet, og at prosjektlederen innenfor denne rammen fungerte som en tilrettelegger for samhandling og informasjonsdeling. Dette har bidratt til en større organisatorisk nærhet. Tilliten som ble etablert mellom medlemmene i styringsgruppen bidro til å styrke den sosiale nærhetsdimensjonen innenfor prosjektet, men Andersen påpeker at dette ikke gjelder for alle aktørene (Andersen 2006).

4.4 Exit Bluelight – enter Security Valley

Da arenapengene forsvant var Bluelight nødt til å tenke nytt. Den første søknaden om status som NCE ble sendt i 2006, men ble avslått. Fra høsten ble Bluelight gjort om til et medlemsbasert nettverk hvor deltakerne måtte betale en medlemsavgift. Samtidig ønsket man å bygge Bluelight ut i en mer kommersiell retning. Innovasjon og bedriftssamarbeid ble i sterkere grad enn kompetanseheving viktige stikkord. Bergum (2006) oppsummerer kick-off seminaret for nye Bluelight på Gjøvik 26-27 september 2006:

En endring av undertittelen fra ”enabling security” til ”security business”, samt endret organisering med andre styremedlemmer, signaliserer en dreining av nettverkets fokus fra kompetanseutvikling og samfunnsoppgaver til mer bedriftsrelaterte samarbeidsaktiviteter som skal resultere i mer innovasjon og kommersialisering. (...) Bluelight skal gi grunnlag for kvalifisering til og synliggjøring av egne og sammensatte leveranser for konstellasjoner av Bluelightaktører (Bergum 2006: 24).

Arbeidet skulle fra nå av organiseres i fagnoder, og ikke som delprosjekter som tidligere. Det ble opprettet fagnoder for energi, helse og offentlig sektor. Arbeidet skulle videreføres

ved ulike samarbeidsfora som seminarer, konferanser, nettsider og sekretariat for kommunal sektor (KinS) (ibid.). Blant annet begynte Bluelight å abonnere på anbudsformidlingstjenesten Doffin, og hadde noen mer eller mindre vellykkede samarbeidsprosjekter på grunnlag av dette. En av mine informanter som kjente Bluelight godt i denne perioden forteller at tilliten og informasjonsdelingen mellom medlemmene i den nye styringsgruppen fra 2006 fungerte godt, men at det likevel var en stor utfordring å opprettholde et nettverk tuftet på bedriftssamarbeid og mulighet for inntjening på kommersielt grunnlag. Jens oppsummerte det slik:

Da er det selvfølgelig litt vanskeligere å være med når det koster penger. Så prøvde man å se om man kunne gjøre noe butikk ut av dette her, altså man begynte å abonnere på Doffin, og se på andre som kom inn, og om man i fellesskap kunne få til noe. For spesielt mange av småbedriftene var for små til å kunne ta på seg sånne ting alene, men i samarbeid kunne man. (...) Så prøvde man å dra dette videre i sånn mer butikkssamarbeid, og da snakket de ikke like godt sammen som de gjorde i kompetanseverdenen.

I 2008 gikk Bluelight sammen med blant andre NorSIS og NISlab inn i det nye kompetanse- og utviklingsprogrammet Security Valley⁹.

4.5 Security Valley – internasjonalt klyngeprosjekt for informasjonssikkerhet

Security Valley ble neste bølge i nettverksaktiviteten rundt informasjonsteknologi i Innlandet. Prosjektet var ambisiøst og skulle legge til rette for samarbeid mellom næringsliv, FoU og offentlige etater innenfor kompetanseheving, innovasjon og kommersielt samarbeid. Sentrale personer i informasjonssikkerhetsmiljøet på Gjøvik hadde i 2007 arbeidet med en ny videreføring av nettverket for informasjonssikkerhet, siden det hadde vist seg vanskelig for Bluelight å finne en god forretningsmodell som sikret både prosjektfinansiering og som dekket behov og ønsker hos medlemsorganisasjonene. Da nyheten om Security Valley-satsningen kom ut i januar 2008, hadde kompetansemiljøet på Gjøvik rundt 50 ansatte, 100 studenter og 40 bedrifter knyttet til informasjonssikkerhet¹⁰. Selve navnet Security Valley hadde oppstått etter en studietur til Silicon Valley, og skulle vise til et fiktivt dalføre som inkluderte hele Innlandet fra Eidsvoll i sør til Gudbrandsdalen i nord (ibid.). Selv valgte de å beskrive seg som en næringsklynge, noe som nok var et strategisk valg i forhold til arbeidet med en søknad om status som NCE. Security Valley uttrykte satsningen slik:

⁹ Regjeringen.no, <http://www.regjeringen.no/nb/dep/fad/pressemeldinger/2008/en-halv-million-i-stotte-til-security-va.html?id=506882> (08.04.2008, hentet 27.02.2011).

¹⁰ Oppland Arbeiderblad, <http://www.oa.no/arkiv/article5400111.ece> (23.11.2010, hentet 07.02.2011).

Etter flere år med målrettet arbeid innenfor sikkerhet lanserer vi nå en ny samlet satsing for å bli enda bedre: **Security Valley**.

I et tett samarbeid mellom bedrifter, offentlige organer og utdanning/forskningsaktører fortsetter vi å utvikle Norges mest komplette sikkerhetsmiljø. I Security Valley skal vi støtte og utfordre hverandre til å levere kunnskap og produkter i verdensklasse.

Benytt sjansen. Bli med i prosjekter, utvid din kompetanse, få hjelp til å starte nye firmaer, ta eksisterende produkter internasjonalt eller kom i kontakt med de beste fagfolkene i bransjen.¹¹

Security Valley ble åpnet 08.04.2008 i forbindelse med konferansen Sikker.info 2008 på Gjøvik som et kompetanse- og utviklingsprogram for informasjonssikkerhet med drivernode lokalisert i Gjøvik Kunnskapspark (ibid.). Informasjonssikkerhetsmiljøet på Gjøvik hadde klart å bygge seg opp som et sterkt kompetansemiljø, noe Fornyings-, administrasjons- og kirkedepartementet anerkjente dette ved å bevilge 500 000 kroner til prosjektet. Særlig den klare visjonen om internasjonalt potensial ble vurdert positivt (Lyngholm 2008)¹².

Hvor Bluelight var et nettverk for samarbeid mellom ulike innlandsbedrifter og HiG organisert av Gjøvik Kunnskapspark, og derigjennom også knyttet til inkubatorvirksomheten, gikk Security Valley bredere. Security Valley kan betraktes som forsøket på å samle informasjonssikkerhetsmiljøet i Innlandet under en paraply, noe som ligger opp til forståelsen av Security Valley som et klyngeprosjekt. Informanten Tore forteller om hvordan han i utgangspunktet fikk forståelsen for hva Security Valley ville gjøre:

Så kom den her visjonen da fra kunnskapsparken om å liksom sy sammen alle aktivitetene i Gjøvik-miljøet under en paraply. At vi hadde Security Valley som paraplyen, og under der så skulle man fra høgskolen sin side starte en etter- og videreutdanningsaktivitet som *Security Valley Academy*. (...) Også skulle de konferansene, altså Sikker.info-konferansen som var etablert, den ble til *Security Valley Conference*, og så videre. Jeg husker ikke hele greia jeg. Og da ble Bluelight avviklet. Ikke på noen sånn veldig formell måte, men det ble roet ned aktivitetene i Bluelight, og heller få bedriftene over til å bli med på å betale for å være med i Security Valley, som liksom skulle ha et større overbyggende nettverk med enda mer aktiviteter.

Noe av det som var nytt med Security Valley som innovasjonsnettverk var at man inkluderte sikkerhetsinkubatoren i GKP som en formell del av nettverket. For å synliggjøre dette skiftet man også navn på sikkerhetsinkubatoren i GKP fra SECTOR (Security Incubator) til *Security Valley Incubator*. Security Valley var i utgangspunktet bygget rundt fire organisasjoner: NISlab, som er forskningsavdelingen for informasjonssikkerhet ved HiG; SECTOR, som er sikkerhetsinkubatoren i Gjøvik Kunnskapspark; NorSIS, Norsk

¹¹ Security Valley, <http://www.securityvalley.no/index.php?limitstart=44> (udatert, hentet 27.02.2011)

¹² http://www.regjeringen.no/mobil/nn/dep/fad/aktuelt/taler_og_artikler/av_ovrig_politisk_ledelse/statssekretar_lyngholm/2008/apning-av-security-valley.html?id=507038 (08.04.2008, hentet 17.02.2011).

Senter for Informasjonssikring; og Bluelight, nettverk for informasjonssikkerhet. Betegnelsen Bluelight ble i årsskiftet 2008/2009 erstattet med *Security Valley Network*, og viste til et bedriftsnettverk for erfaringsutveksling og utvikling av felles innovasjonsprosjekter (Bergum 2009). Prosjektet hadde en kjernegruppe som bestod av følgende organisasjoner: Campus Kjeller, Det Norske Veritas, Genkey, Mnemonic, NISlab, NorSIS og Secure Allied. Hver av kjernebedriftene var representert med én person i styringsgruppen. Arbeidet var organisert i prosjekter styrt av en prosjektgruppe under ledelse av prosjektlederen. I tillegg hadde Security Valley pr. februar 2009 34 medlemsbedrifter, 21 støttespillere og 15 inkubatorbedrifter knyttet til prosjektet via SECTOR (Security Valley 2009)¹³.

Som nevnt blir Security Valley oftest referert til som en næringsklynge. Organisasjonene som klyngen består av er imidlertid ikke geografisk samlokalisert, slik at klyngebegrepet i denne sammenhengen er noe mer abstrakt. Bergum (2009) skriver at Security Valley hadde to spesielle organisasjonsmessige karakteristika. For det første var det en *funksjonell* klynge, siden det først og fremst er næringsmessige fordeler knyttet til kompetanseområdet informasjonssikkerhet, snarere enn geografisk lokasjon som var sentralt for Security Valley. For det andre var det en *distribuert* klynge nettopp siden aktørene var geografisk spredt. Bruker vi Boschmas (2005) nærhetsdimensjoner i betraktningen av Security Valleys organisasjonsform finner vi at geografisk nærhet ble antatt å være av mindre viktighet enn de fire andre nærhetsdimensjonene, som vi skal gå videre inn på senere i analysen.

Den mest aktive perioden i Security Valley var mellom åpningen i april 2008 og årsskiftet 2009/2010. I 2008 og 2009 var nettsiden securityvalley.no jevnlig oppdatert med nyheter og prosjekter. Det er i stor grad dette materialet som forteller noe om Security Valleys utvikling. Arbeidet med å bygge en næringsklynge som kunne oppfylle kravene til NCE-status ble første gang omtalt på securityvalley.no sommeren 2008¹⁴. Nyhetsoppdateringene på nettsidene vitner om et omfattende arbeid knyttet til *pipelines* og nettverksetablering i inn- og utland – særlig med store brukergrupper og kompetansemiljøer. I NCE-søknaden datert 27. februar 2009 beskrives de ulike målsetningene for Security Valley. Visjonen om å skape ”Europas mest anerkjente informasjonssikkerhetsklynge” skulle oppnås ved å oppfylle følgende hovedmål: a) å øke

¹³ Organisasjonskart, samt fullstendig liste over medlemmer, støttespillere og inkubatorbedrifter finnes i vedlegg 4.

¹⁴ Security Valley, http://www.securityvalley.no/index.php?option=com_content&view=article&id=75:saab-avtale&catid=35:forside&Itemid=104 (udatert, hentet 18.02.2011).

lønnsomhet og forsere internasjonal satsning for klyngens bedrifter; b) øke klyngens innovasjonsevne ved å styrke koblingen til forskning; c) utvikle utdanningsmiljøet til å bli Europas ledende (Security Valley 2009: 4). Arbeidet skulle fokuseres rundt tre fokusområder: identifiserings- og autentiseringsløsninger, dataetterforskning og overvåkning, og simulering og modellering av kritisk IKT-infrastruktur. Det er vanskelig å identifisere hvilke konkrete prosjekter som ble initiert av prosjektgruppen i Security Valley, hvilke prosjekter som har oppstått mellom aktørene, og hvilke eksterne prosjekter aktører med tilhørighet til Security Valley har deltatt i. I NCE-søknaden nevnes spesielt fire prosjekter som har vært innovasjonssamarbeid mellom bedrifter og FoU (Security Valley 2009: 12):

- **CompFor:** Intelligent verktøykasse for dataetterforskning og bekjempelse av cyberkriminalitet.
- **PASS:** Sikre biometriløsninger.
- **GIFT:** General-Purpose Integrated Forensic Toolbox.
- **FP7 – Managing Crisis Lifecycle:** Utvikle verktøy for å modellere, simulere og utføre øvelser mht kriser i kritisk infrastruktur.

I tillegg må **ID-tyveriprojektet** nevnes spesielt. Prosjektet begynte som et samarbeidsprosjekt mellom NorSIS og Security Valley i 2007, men eies nå av NorSIS alene, og avsluttes i 2011. Gjennom å forebygge, oppdage og bekjempe id-tyveri ønsker prosjektet å bidra til ”å redusere og bremse omfanget av identitetstyverier og misbruk av personopplysninger. Prosjektet skal definere tiltak og virkemidler som forebygger og reagerer på ID-tyverier og ID-svindel”¹⁵. Prosjektet har fått mye medieomtale, og er stadig et aktuelt tema for ulike konferanser om informasjonssikkerhet.

NCE-søknaden fra februar 2009 ble avslått, og Security Valley som prosjekt fra Gjøvik Kunnskapspark sin side ble mer eller mindre formelt avvirket. Kunnskapsparken hadde satset hardt på etableringen av Security Valley som et nasjonalt ekspertcenter, men hadde i samme prosess lagt seg opp et aktivitetsnivå som ikke hadde tilstrekkelig finansieringsgrunnlag. Dette gikk hardt ut over bedriftens egenkapital, og Gjøvik Kunnskapspark var i 2009 tvunget til å si opp tre ansatte, mens ytterligere to ansatte ble overført til NorSIS (Gjøvik Kunnskapspark 2009). I 2010 ble NorSIS skilt ut fra Gjøvik

¹⁵ ID-tyveriprojektet, http://www.idtyveri.info/index.php?option=com_content&view=article&id=1:prosjektbeskrivelse&catid=1:om-oss&Itemid=2 (udatert, hentet 18.02.2011).

Kunnskapspark som siden 2006 hadde hatt operatøransvaret. Med denne utviklingen mistet informasjonssikkerhetsmiljøet i Innlandet en vesentlig faktor for nettverksbygging og synliggjøring utad. Samtidig satte dette en stopp for Gjøvik Kunnskapspark sin parallelle satsning på innovasjonsnettverk og innovasjonsinfrastruktur. GKP fokuserer i dag først og fremst på driften av SECTOR inkubator på Gjøvik og RISC inkubator, som er delvis integrert i NCE Raufoss. På nettverkssiden har relaterte aktører lansert IKT-Innlandet som har et bredere fokus enn kun informasjonssikkerhet, men som blant annet vil gå nærmere inn på biometri som løsning på sikker informasjonshåndtering.

Fra Security Valleys søknad om status som NCE går det frem et omfattende arbeid knyttet til innrullering av aktører i nettverket, etableringen av internasjonale koblinger og målsetnings- og strategiarbeid. I intervjuene til denne studien ble jeg klar over at Security Valley på mange måter aldri klarte å etablere et godt innovativt klima blant medlemsaktørene og den tilknyttede virksomheten innenfor Gjøvik Kunnskapspark. Dette på tross av at alle informanter og andre aktører i Security Valley jeg har hatt kontakt med har stilt seg positivt til initiativet med å etablere et sterkere fellesskap rundt informasjonssikkerhet som del av det regionale innovasjonssystemet i Innlandet. Hvorfor klarte ikke Security Valley å skape et sterkere og mer stabilt innovativt klima i miljøet det var en del av? I hvilken grad var aktørrelasjonene tilstrekkelig utviklet for å stabilisere et nettverk for samarbeid og innovasjon? Eksisterte i det hele tatt en felles forståelse rundt hva Security Valley var? Dette er noen av spørsmålene som vil belyses i de neste kapitler hvor jeg først vil sammenligne de to svært ulike innfallsvinklene til samarbeid i innovasjonsnettverk som Bluelight og Security Valley representerte.

5. Fra Bluelight til Security Valley – hva skjedde?

I dette kapittelet vil jeg gå inn på hvordan Bluelight og Security Valley som innovasjonsnettverk har ulike, og til dels motsatte karakteristikk. Den overbyggende forskjellen består i at mens Bluelight oppstod som et prosjekt for å løse konkrete behov og målsetninger, oppstod Security Valley som et *rammeverk* for å sikre *mulighetene* for fortsatt samarbeid innenfor informasjonssikkerhet. Måten å gjøre dette på var å finne finansiering til å bygge en klyngeinfrastruktur med navet i Gjøvik Kunnskapspark. I de neste avsnittene vil jeg drøfte ulike motstridende forhold ved de to prosjektene for å utdype egenskaper som er viktige for å stabilisere et nettverk for samarbeid og innovasjon, og skape et innovativt klima.

5.1 Aktørers behov vs. samarbeidsrammeverk: ufarlig kompetanse, farlige penger

Bluelight ble som vi har sett dannet på basis av et ønske blant store og etablerte bedrifter om kompetanseutvikling og et utdanningsprogram innenfor informasjonssikkerhet. Tilgangen på høyt kvalifisert arbeidskraft og forskningsresultater gjennom informasjonssikkerhetssatsningen på Høgskolen i Gjøvik var attraktiv blant flere store bedrifter i mjøsområdet, og det konkrete behovet for kompetanseutvikling innenfor fagområdet informasjonssikkerhet ble på mange måter limet som holdt nettverket sammen. Dette må sees i sammenheng med arbeidet som ble lagt ned fra Gjøvik Kunnskapspark sin side for å bygge tillit og dynamikk mellom aktørene i nettverket. Med Castells' (1996) ord kan man dermed si at det forelå *consistency*, altså en felles forståelse av delte interesser og målsetninger både hos aktørene og nettverket i seg selv. Dette lå til grunn for at Bluelight gjennom arenaperioden begynte å fokusere bredere på kompetanseutvikling enn kun studiene på HiG. Informanten Jens oppsummerte perioden som arenaprosjekt slik: *”Det fungerte godt å ha et kompetansebasert nettverk med bedrifter som var opptatt av den biten, for kompetanse er ufarlig!”* Han fortalte videre at man oppfattet at kimen til et større samarbeid var skapt med Bluelight, men at det var utfordringer knyttet til videre finansiering etter arenaperioden siden kontantsummen inn forsvant. Løsningen ble å etablere et nettverk med medlemsavgift og reelle inntjeningsmuligheter for medlemmene.

Fra høgskolen sin side, delte man oppfattelsen av at kompetanse var ufarlig mens det er langt mer utfordrende å skape et samarbeid som skal gi reelle inntjeningsmuligheter for medlemsbedriftene. Tore forteller om sin oppfatning av utviklingen av Bluelight etter at man hadde fått i stand masterstudiet i informasjonssikkerhet ved HiG:

Alt gikk greit ikke sant, så lenge det bare var å spytte i penger i et studium. Det er veldig enkelt, men så gikk det over til at bedriftene skulle samarbeide og få felles prosjekter og starte nye bedrifter og på en måte den aktiviteten knyttet til kunnskapsparken og sånn da. Og det er en aktivitet som er mer vanskelig i natur. (...) Så Bluelight, det var for så vidt greit nok det, men man fikk liksom ikke til det helt store. Man fikk ikke til noen sånne kjempestore samarbeidsprosjekter mellom bedrifter og sånne ting, men det er som sagt vanskelig.

Informanten fortsatte å fortelle om hvordan Security Valley oppstod som en løsning på utfordringene i Bluelight. Problemet var imidlertid at man beveget seg bort både fra det konkrete behovet for kompetanseutvikling som var limet i Bluelight i arenaperioden, men også bort fra fokuset på bedriftssamarbeid inn mot konkrete tilbud og konkrete produkter. Man startet dermed å utvikle et rammeverk for videre samarbeid mellom en rekke ulike aktører, samtidig som man fokuserte mindre på innholdet som rammeverket bør bygges rundt. I følge Tore fremstod prosjektet etter hvert som innholdsløst:

(...) Det funket bra så lenge man drev med utdanning, og bedriftsnettverket Bluelight fungerte også, men det var liksom ikke noen sånn stor aktivitet da. Men i stedet for å jobbe hardere med det da, så drar man det her enda mer luftslåttaktig opp og legger masse penger i det som ikke finnes, da tryner hele greia.

Graden av felles forståelse rundt aktørinteresser og målsetninger – consistency – som lå til grunn for det gode samarbeidet i starten av Bluelight-samarbeidet, nemlig behovet for kompetanseøkning, ble gradvis borte ettersom man prøvde å bygge opp et samarbeidsrammeverk og dermed utvikle hva Castells (1996) kaller *connectedness*. Connectedness omhandler de strukturelle rammene for kommunikasjon og derav samhandling og kunnskapsdeling. Dette viser til viktigheten av å ha en balanse mellom disse forutsetningene for å legge til rette for stabile samarbeid.

Idar knytter også den feilslåtte satsningen på Security Valley til de større behovene som finnes blant medlemsaktørene. Han har en oppfattelse av at det har oppstått en metning innenfor samarbeidsfora i IKT-bransjen, og at det dermed er av enda større betydning at samarbeidsprosjekter og nettverksinitiativ må funderes i konkrete behov innenfor de faglige fokusområdene.

Man prøvde seg jo med å konvertere Bluelight i en slags videreføring over i noe annet. Det viste seg vanskelig. For da begynte man liksom å skulle innføre et sånt generelt nettverk med liksom medlemskapsavgift, og det finnes jo så mange sånne. Da mistet man liksom nerven. Det var liksom ikke noe skarpt oppdrag lenger, det ble mer et sånt generelt forum, og det er markedet mettet for. Derfor så døde Bluelight og det vil si Security Valley egentlig óg da. Security Valley ville på en måte ta neste bølge, men man klarte ikke å få bedriftene sammen om noe da. Det ble liksom litt sånn løsrevet.

Den avtakende *buzzen* i Security Valley kan i så henseende skyldes at man i for liten grad klarte å knytte målsetninger til behov og interesser hos aktørene som bidro til

klyngeprosjektet. I NCE-søknaden for Security Valley fremgår flere konkrete fokusområder og delmål. Hovedmålsetningene om å øke lønnsomhet og innovasjonsevne, samt styrking av forsknings- og utdanningsmiljøet skulle oppnås gjennom fokusert arbeid innenfor fagområdene identifisering og autentisering, dataetterforskning og overvåking, og simulering og modellering av kritisk IKT-infrastruktur (Security Valley 2009: 4). Til sammen skulle dette bygge opp om visjonen ”Europas mest anerkjente informasjonssikkerhetsklynge” (ibid.). Fra søknaden går det også frem en rekke kvantifiserbare målsetninger for antall aktører i klyngen, antall nye prosjekter, antall nye bedriftsetableringer etc. Likevel er det vanskelig å identifisere hvilke aktører som har konkrete behov og interesser i å realisere de ulike målsetninger. Informanten Idar forklarte at fokuset på konkrete og overordnede målsetninger var en forutsetning for å samle og innrullere aktører: *“Det må liksom være i henhold til noe som noen sliter med og ser seg tjent med at blir løst. Som et grunnlag for å jobbe med å skape tillit og samhandle på andre områder”*. For stabilisering av samarbeidsnettverk ser det ut til at det trengs en *kombinasjon* av consistency, i betydningen delte interesser, og tillit mellom aktørene. Nettopp arbeidet med å skape tillit mellom aktørene i innovasjonsnettverk var et sentralt arbeid i Bluelight. Dette vil jeg gå mer inn på i neste avsnitt.

5.2 Tillitsbygging og IKT i distribuerte nettverk

Informantene som tidligere har jobbet innenfor prosjektene Bluelight og Security Valley forteller at tillitsskaping mellom aktørene var noe som ble lagt stor vekt på, og noe som var spesielt viktig på grunn av den distribuerte arbeidsformen. Arbeidet med tillitsbygging og utviklingen av et fruktbart samarbeidsmiljø var et vesentlig element å få på plass siden de forskjellige aktørene i nettverket også stod i konkurranseforhold til hverandre. Dette var av særlig stor betydning fra tidspunktet da Bluelight gikk ut av arenaperioden, og ble transformert til et medlemsbasert nettverk. Jens påpekte at det særlig overfor de mindre og spesialiserte aktørene var viktig å tillitsgjøre seg, siden disse fryktet å bli overkjørt av de større bedriftene som ikke hadde informasjonssikkerhet som sitt kjerneområde. Informanten hevder imidlertid at det var nyttig for de små spesialiserte bedriftene å delta i nettverkene for informasjonssikkerhet, siden de på den ene siden kunne utvikle samarbeid seg i mellom, og samtidig opprettholde kontakten med de store aktørene, og dermed oppnå en sterkere standing i bransjen.

Tillitsskapingen mellom store bedrifter og små spesialiserte bedrifter er hva vi med Halperns ord kan kalle *linking* (Halpern 2005, i Johnstad 2009). Suksessfull linking vil

tilrettelegge for sosial kapital mellom aktører med asymmetrisk maktforhold når det utvikles åpenhet og normer mellom aktørene (Johnstad 2009). Bergum (2004) skriver om hvordan tillitsbygging har vært et vesentlig kriterium for målrealisering i Bluelight, og fokuserer spesielt på viktigheten av *personeffekter*. Mine data gir inntrykk av at personeffekter og mellommenneskelig tillit er vesentlig for samarbeid innenfor både Bluelight og Security Valley. Dette gjelder for linking så vel som *bridging* og *bonding*, altså både koblingen mellom aktører innenfor samme organisasjon, og mellom aktører i både horisontale og vertikale relasjoner til hverandre (Bø og Schiefloe 2007; Halpern 2005, i Johnstad 2009). Personeffekt er imidlertid ikke alltid nok, siden den ofte går mellom en eller få personer som jobber med det enkelte prosjekt i de ulike organisasjonene. Jens beskrev hvordan han opplevde dette problemet i Bluelight:

Det var en kjernegruppe på åtte – ti bedrifter som ringte hverandre på privat basis omtrent. Det fungerte veldig godt. Også var det noen utenfor der som var med på arrangementer dann og vann. Også var det en litt mer perifer gruppe som nesten bare stod der som sånne “eves droppere”. (...) Men det som var det største problemet for Bluelight var at det var kontakter i hver bedrift som stort sett var *den ene ivrige* personen. Det å sørge for god forankring i de bedriftene.

Dette viser at personeffektene kan betraktes som limet i samarbeidet, men at arbeidet med relasjonsbygging også lenger ned i medlemsorganisasjonene er sentralt for å etablere et velfungerende nettverk over tid, som er mindre avhengig av “den ene ivrige” i hver bedrift. I tillegg til personeffekter er det også viktig for utviklingen av tillit med gjensidig forståelse rundt det Idar kalte ”dualiteten i samarbeidet”:

Nå skal ikke jeg overvurdere noe, men det er klart at det er en faktor at man hadde en tillitskapital i dette her. Men så så man på en måte at det ofte er enklere å samhandle om noe som ligger litt frem i tid og som er på en måte generisk og overordnet. Også gikk man ut etterpå og konkurrerte om leveranser og andre ting selvfølgelig. Man må holde dualiteten i det her da, mellom det langsiktige og overordnede, og den mer dag til dag markeds konkurransen.

Nettopp forståelsen av balansen mellom langsiktig, overordnet fokus og daglig markeds konkurransen må sees som vesentlig for å oppnå felles forståelse rundt aktørinteresser. Dette vil også kunne bidra til den sosiale kapitalen i et samarbeid ved å tilrettelegge for tillit mellom aktører i horisontalt og vertikalt maktforhold. Sagt med teoretiske begreper kan man se hvordan consistency er en forutsetning for bridging og linking. I forlengelsen av dette fortalte Idar om hvordan slike nettverk var avhengig av en legitim og tillitsvekkende fasilitatorfunksjon for å tilrettelegge for sosial kapital mellom aktørene. Johnstad (2009) ser sosialt entreprenørskap, *ildsjelene*, og hvordan miljøet fasiliterer samarbeid, visjon og lederskap som en viktig variabel på mikronivå for å forklare fremveksten av sosial kapital. I Bluelight og Security Valley ble det oppfattet at

Gjøvik Kunnskapspark som en velrenommert innovasjonsbedrift kunne etablere denne type miljø og bistå med prosjektledelse. Spesielt må prosjektlederne Svein Pettersen for Bluelight i arenaperioden, og Morten Schjelderup i Security Valley nevnes som viktige i utviklingen av *buzzen* rundt informasjonssikkerhetsmiljøet i Innlandet.

Målet om å bygge et tillitsforhold mellom de ulike aktørene i et distribuert nettverk har også implikasjoner for kommunikasjonsformen. Blant de informantene jeg har snakket med så er det en gjennomgående enighet om at ansikt-til-ansikt-kommunikasjon er en forutsetning for å skape tillit, og for å få i stand godt samarbeid. Jens understreket viktigheten av de personlige relasjonene:

(...) det handler om mennesker og hvis du ikke får mennesker til å stole på hverandre så hjelper det ikke hvor fine verktøy du har, altså. (...) Starten av all sånn type nettverkssamarbeid det handler om å ta folk i handa og sette seg ned og drikke øl med dem, og bli gode venner. Har du ikke det i bunnen, så da er det ingenting som fungerer ellers. Så er verktøyet og teknikk ting du kan hekte på etter hvert for å gjøre kommunikasjonen enklere når tilliten allerede er skapt. (...) Altså, digitalkommunikasjonen mener jeg aldri kan erstatte den fysiske møteplassen. Men den kan fungere mellom de fysiske møteplassene.

Fokuset på ansikt-til-ansikt-kommunikasjon i samarbeid betyr ikke at IKT ikke har sin plass. Informanter som var involvert i Bluelight forteller at man var svært bevisst på balansen mellom ansikt-til-ansikt-kommunikasjon og mediert kommunikasjon gjennom hele samarbeidet. Særlig i starten var det fokus på at aktørene møtte hverandre, og ble kjent med de ulike kontaktpersonene og organisasjonene de representerte. Flere informanter forteller at bruken av kommunikasjonsmedia kan sees som et modningstegn for et nettverkssamarbeid; når deltakerne begynte å ringe og sende e-post til hverandre uten at dette var initiert av prosjektlederen, så var det et tegn på at nettverket begynte ”å virke”. Jens beskrev det som at *“da er det heller ikke vanskelig for mellomlederen på Hamar å ringe administrerende i Oslo, for vi har brutt ned en del sånne barrierer på roller. Det øker jo sannsynligheten for et tett samarbeid”*. Jens peker her på to interessante teoretiske implikasjoner: For det første må *connectedness*, altså de strukturelle kommunikasjonsegenskapene, sees som betinget av det Johnstad (2004: 123) kaller “den generaliserte tilliten” som er basisen for den sosiale kapitalen. For det andre støttes informantenes erfaringer også Draft et al. (1987) som peker på kommunikasjonsmediers ulike kapasitet til å fasilitere felles forståelse. En komplisert aktivitet som tillitsbygging forutsetter en så rik kommunikasjonsform som mulig, nemlig ansikt-til-ansikt-kontakt. Når dette grunnlaget er lagt kan kommunikasjonsteknologi forsterke den sosiale kapitalen, slik som også Steinfield et al. (2010) påpeker.

5.3 IKT i Bluelight og Security Valley – to strategier

Prosjektene Bluelight og Security Valley ser ut til å ha hatt ulik innfallsvinkel til IKT-støttet kommunikasjon i samarbeidet og det kontinuerlige vedlikeholdet av kjennskap og tillit. Bluelight var i relativt liten grad understøttet av annen online kommunikasjon og informasjonsdeling enn e-post. En informant fortalte om nettsiden bluelight.no og hvordan dette var en informasjonskilde både for aktører innenfor prosjektet og for utenforstående. Nettsidene inkluderte også en enkel delingsløsning for medlemmene av prosjektet, men ble aldri brukt i særlig stor grad. I Security Valley hadde man tidlig lagt ned et omfattende arbeid i å lage en infrastruktur for kommunikasjon og informasjonsdeling. Securityvalley.no består av en forside med nyhetsarkiv, det er lagt ut informasjon om bakgrunnen for prosjektet, en presentasjon av et utvalg nasjonale og internasjonale prosjekter på informasjonssikkerhet, informasjon om deltakerne og arkiv over medieomtaler. I tillegg finnes det delingsløsninger med innloggingsfunksjon for dokumenter for Security Valley generelt, Inkubator, ID-tyveriprojektet og Security Valley Academy¹⁶. Security Valley har en prosjektside på LinkedIn, og det ble sendt rundt nyhetsbrev på e-post til medlemmene. Det ble også planlagt å opprette chatrooms for tilrettelegge for kommunikasjon mellom medlemmene. Arbeidet som var lagt ned i kommunikasjonsinfrastrukturen la til rette for connectedness, god informasjonsdeling og dermed en av hovedforutsetningene for et vellykket nettverkssamarbeid (Castells 1996). Likevel påpeker informanter at en velutbygget kommunikasjonsinfrastruktur ikke er tilstrekkelig for å innrullere aktører og stabilisere et bedriftssamarbeid. Tore forklarte:

Jeg hadde vel inntrykk av... Security Valley gjorde jo... de fikk på plass mye av alle de formelle bitene som ikke er for vanskelig å få på plass, det fikk de på plass. Security Valley ble synlig i media, de hadde et nettverk av bedrifter som de sendte ut jevnlig informasjonsmail og statuser til. Og de etablerte månedlige frokostmøter som var godt besøkt av bedriftene. Men det var på en måte ikke noe av det her som da – det var ingen av de kommunikasjonsaktivitetene som gav noen penger i kassa. Men for all del. De tingene som skulle på plass skulle jo være på plass da. Og Security Valley kunne ha blitt noe det, hvis man bare hadde hatt en to-tre sikkelige punchlines hver gang bedriftene spurte helt konkret ”what’s in it for me?”

Kommunikasjonsaktiviteter gir, som Tore påpeker, ingen direkte inntjening dersom de ikke bidrar til innrulling av nye aktører. Kommunikasjonsarbeid må likevel sees i sammenheng med inntjening siden stabilisering av nettverk knyttes til tillit, og videre til identitet og en følelse av fellesskap. Kommunikasjon via IKT er vesentlig i så henseende, siden kommunikasjon og identitet må kontinuerlig vedlikeholdes, spesielt i distribuerte

¹⁶ Security Valley, http://www.securityvalley.no/index.php?option=com_docman&Itemid=125 (datert, hentet 12.05.2011).

nettverk. I neste avsnitt vil begrepet *autokommunikasjon* benyttes for å drøfte i hvilken grad Security Valley klarte å fokusere samarbeidet rundt felles identitet og en følelse av ”hva vi er gode på”.

5.4 Identitet og autokommunikasjon

I intervjuene har jeg snakket med informantene om hvorvidt identitet og fellesskapsfølelse finnes innenfor de aktuelle innovasjonsnettverkene. Flere informanter har knyttet identitet og fellesskapsfølelse til tilliten mellom deltakerne i prosjektene. En informant som var involvert i Bluelight forteller at en fellesskapsfølelse utviklet seg på grunnlag av resultatene av delmålene man hadde satt seg:

Intervjuer: Opplevde du at det ble etablert noen sånn fellesskapsfølelse mellom de som var med på Bluelight, eller en slags utvidet organisasjonskultur da?

Idar: Ja, det merket vi absolutt! Det gjorde vi altså. Man var rett og slett litt stolt av hva man fikk til. Vi etablerte masterstudiet på åtte måneder, ikke sant, og fikk avslag på samarbeid med NTNU og UiO, ikke sant. Vi bare gjorde det som en sånn underdog. Og det gjorde at de gamle gutta som var med her, de syntes at det var litt artig, vet du, å virkelig kunne få til noe litt ”på tross av”. De var liksom litt stolt av hva de fikk til der, altså, det merket vi tydelig.

Informanter forteller at det i *visjonen* om Security Valley lå en tanke om å bygge en fellesskapsfølelse ved å samle aktørene innen informasjonssikkerhet i Innlandet og samlet fokusere på ”det vi er gode på”, nemlig informasjonssikkerhet. Denne tolkningen støttes av NCE-søknaden, som definerer Gjøvik som kompetansesenteret i klyngen (Security Valley 2009). Dessverre påpeker flere at det ikke lykkes å etablere en identitet eller fellesskapsfølelse innenfor Security Valley. Informantene peker på flere årsaker til dette. For det første oppleves det blant flere at Security Valley var et innovasjonsnettverk som ikke inkluderte gründerne i tilstrekkelig grad. Med Boschmas (2005) begrepsapparat kan man dermed si at det i praksis oppstod en eksklusjon av noen deltakere, og det kan argumenteres for at det oppstod en økt sosial og organisatorisk avstand innenfor kjernemiljøet på Gjøvik. For det andre kom Security Valley i et økonomisk uføre med manglende finansiering til et høyt aktivitetsnivå før man i det hele tatt klarte å oppfylle noen av delmålene man hadde fremsatt i NCE-søknaden. Dette kom i tillegg i kombinasjon med en lavkonjunkturperiode hvor flere bedrifter valgte å fokusere på sine egne kjerneaktiviteter fremfor nettverkssamarbeid. Som nevnt kan ikke økonomiske utfordringer løses med kommunikasjonsarbeid. Det er likevel grunn til å understreke at det later til at opprettholdelsen av en samlet identitet innenfor og mellom klyngeaktørene må sees som

spesielt viktig også i turbulente perioder for å sikre at det fortsatt finnes et “lim” i samarbeidet.

I utgangspunktet burde securityvalley.no med sin nyhetsformidling være et viktig verktøy for autokommunikasjonsarbeid i Security Valley. Mine data tyder likevel på at dette ikke har fungert etter hensikten fordi nyhetene bare ble oppfattet som relevant av noen av klyngens medlemmer. Det er grunn til å reise spørsmål om hvorvidt den ansikt-til-ansikt-baserte tillitsskapingen var tilstrekkelig fasilitert, eller om man kun forutsatte at denne forelå mellom de sentrale aktørene gjennom arbeidet i Bluelight. I NCE-søknaden beskrives kognitiv og sosial avstand mellom aktørene som liten, slik at relasjonene mellom aktørene sees som uproblematisk og i liten grad påvirket av den geografiske avstanden, jamfør Boschma (2005). Jens fortalte at i Bluelight var det en bevisst strategi å bygge identitet og fellesskap gjennom de delresultater man klarte å oppnå. For Security Valley kan man gjennom innholdet på nettsiden og tankegangen omkring nærhetsdimensjoner slik de presenteres i NCE-søknaden forutsette at tanken om autokommunikasjon i klyngens natur. Fra en teoretisk vinkling kan man dermed se hvordan Cheney og Christensens (2001) autokommunikasjonsbegrep også kan knyttes til Castells (1996) begreper *connectedness* og *consistency*: Autokommunikasjon forutsetter en god kommunikasjonsstruktur, og kan igjen bidra til å skape felles forståelse rundt hvordan prosjektet eksponeres utad, dvs. nettverkets målsetning, og i hvilken grad dette samsvarer med aktørinteressene innenfor nettverket. Her er det på sin plass å sette spørsmålstegn ved hvorvidt synliggjøringen av Security Valley gikk på å kommunisere visjonen ”Europas mest anerkjente informasjonssikkerhetsklynge”, eller om man kunne fronte prosjektet gjennom aktørenes realisering av målsetningene man hadde satt seg fore.

5.5 Synliggjøring: Proof of the pudding eller å kommunisere visjon?

Gjøvik Kunnskapspark har tradisjonelt ikke hatt noe ønske eller målsetning om ekstern eksponering av seg selv som innovasjonsselskap og merkevare. Man har i stedet ønsket å være synlig gjennom suksessfulle prosjekter og bedriftsetableringer. I intervjuet med Kalle snakket vi om ulike tiltak for å utvikle en bedre kobling mellom kunnskapspark og lokalt næringsliv. Kalle forklarte meg om strategien som Gjøvik Kunnskapspark har valgt i forhold til inkubatordelen for å skape tillit til at det kommer noe konstruktivt ut av samarbeidet mellom høyskole, innovasjonsbedrift og næringsliv:

Det er egentlig litt sånn ”proof of the pudding”, som de sier det da. Altså, GKP blir ikke bedre enn de bedriftene man klarer å levere ut av inkubatorsystemene. Og som jeg nevnte så er ikke GKP så opptatt av å eksponere seg i media. Det er viktigere for GKP at bedriftene eksponerer seg i media når de lykkes. Og henviser til kunnskapsparken som et viktig instrument da for at de kunne lykkes. Og på den måten så oppnår man tillit og troverdighet i markedet, og vet man kan bli tatt seriøst ved at man bidrar til å produsere da innovasjonsbedrifter og flere kompetanseintensive arbeidsplasser i regionen vår. Dette tar lang tid, selvfølgelig. Og klart, GKP skal kjenne litt besøkestiden sin óg. En skal ikke mase på om det er bedrifter, altså næringslivet, eller noen i tide og utide. For da mister man fort den tilliten man er helt avhengig av for å få dette til.

I Bluelight-perioden hadde man en liknende tilnærming til synliggjøring av nettverket. Man ønsket å gjøre seg gjeldende gjennom deltakernes egne nettverk, og fronte aktørene i nettverket heller enn nettverket som en merkevare i seg selv.

Som vi tidligere har vært inne på var Security Valley et langt mer omfattende og ambisiøst prosjekt enn Bluelight. Fra NCE-søknaden til Security Valley fremgår visjonen om å etablere seg som den mest anerkjente informasjonssikkerhetsklyngen i Europa, og kvantifiserbare målsetninger om ”klynge- og nettverksutvikling, FoU og kompetansespredning, utdanning og holdningsskapning, kommersialisering og innovasjon, [og] nasjonale prosjekter” (Security Valley 2009: 5). Visjon og målsetning ble presentert gjennom en rekke medieoppslag og konferanser. Informanten Idar kjenner til både Bluelight og Security Valley, og synes at synliggjøringen – eller *eksternkommunikasjonen* – til Gjøvik Kunnskapspark var vesensforskjellig i de to prosjektene. Mens informanten synes synliggjøringen til GKP i forbindelse med Security Valley-prosjektet hadde dårlig feste i virkeligheten, fremstiller han eksternkommunikasjonen i forbindelse med Bluelight-prosjektet som klart i tråd med den policyen GKP har på synlighet av sitt arbeid: Her var det bedriftene som var involvert som skulle fronte prosjektet både i media og i sine kontaktnett, mens kunnskapsparken skulle vise at de kunne produsere gode prosjekter og gode bedrifter.

Intervjuer: Hvordan oppfattet du den eksternt rettede kommunikasjonen i Security Valley?

Idar: Den opplevde jeg som overambisiøs. Rett og slett at man gikk ut med store visjoner og vyer og sånn, men veldig liten gjennomføringskraft i bunnen og veldig liten idé om hvordan man skulle kunne nå noen mål. (...) Jeg følte man kommuniserte noe man hadde en visjon om å gjennomføre en gang, men man klarte ikke å skaffe noen delresultater da.

Intervjuer: Hvordan oppfattet du den eksternt rettede kommunikasjonen i Bluelight mot eksterne kompetansemiljøer, brukergrupper osv.?

Idar: Det var ganske aktivt gjennom aktørenes nettverk og sånn og Bluelight ble oppfattet som relevante, så det ble dratt med inn i andre prosjekter. For eksempel noe som het ”Trådløs fremtid” som var et annet arenaprosjekt... som så at mye av det man holdt på med var tuftet på sikkerhet. Da må de dra dit man har en klynge og en kompetanse på det, og da drar man til Gjøvik. (...) Det var ikke Bluelight som sådan som skulle frontes som merkevaren her, det var heller aktørene selv her som måtte stå frem og så videre, men at de hadde en assosiasjon til Bluelight da.

Eksponeringen av nettverket gjennom aktørene og delmål som aktørene i samarbeid har oppnådd må sees i forhold til Cheney og Christensens (2001) benyttelse av begrepet

autokommunikasjon. Denne eksponeringen vil kunne tjene til både positiv synliggjøring utad, men også som identitetsforsterkende mekanisme mellom aktørene som inngår i samarbeidet ved å styrke følelsen av “det vi er gode på”, nemlig felles og komplementerende kompetanse på informasjonssikkerhet.

5.6 Fasilitering vs. prosjektledelse

Begrepet kompetansemegling innebærer å identifisere konkrete utfordringer i bedrifter, og løse disse ved å koble på relevant forsknings- og FoU-kompetanse, og ikke minst oversette mellom det ”akademiske språket” og ”næringslivsspråket”¹⁷. Flere av informantene jeg har snakket med forteller at de hadde inntrykk av at fasiliteringen og kompetansemeglerfunksjonen fungerte ulikt i Bluelight og Security Valley. I Bluelight var arbeidet med å koble næringsliv til academia selve forutsetningen og grunnbehovet i nettverket, siden det i første rekke handlet om å benytte høgskolen som arena for å utvikle kompetanse som næringslivet hadde behov for. Security Valley var i sterkere grad et bedriftsnettverk enn et kompetansenettverk, noe som også ligger i klyngetankegangen bak prosjektet. Det var dermed ikke et konkret behov i forhold til kompetanseutvikling som var nettverkets eksistensgrunnlag, men snarere å skape et miljø for samarbeid og innovasjon innenfor informasjonssikkerhet. Selve NCE-prosessen fungerte også som en gulrot for å innrullere aktører i nettverket. Kompetansemeglerrollen måtte innenfor et slikt nettverk/klynge formaliseres, noe som Gjøvik Kunnskapspark for så vidt arbeidet med i 2008 da de på oppdrag fra SIVA arbeidet sammen med HiG for å etablere et TTO¹⁸ (Gjøvik Kunnskapspark 2008). I tillegg oppfatter jeg at prosjektledelsen i Security Valley skulle megle mellom samfunnsmessige behov og brukere brukerbehov relatert til informasjonssikkerhet på den ene siden, og verktøy for problemløsning på den andre siden. Dette er i tråd med hva man kan kalle en *mediator*-funksjon (Schot og de la Bruheze 2005). Flere av informantene oppfattet også at Gjøvik Kunnskapspark skulle fungere som både kompetansemegler og mediator.

Da arenafinansieringen for Bluelight opphørte i 2006 begynte man å bygge nettverket mer i tråd med en trippel helix-modell¹⁹ enn man hadde gjort tidligere. Jens

¹⁷ Begrepet er lånt fra prosjektet Virkemidler for Regional Innovasjon, og er i denne sammenheng brukt noe mer abstrakt enn i VRI-sammenheng. Se VRI-Innlandet, http://vri-innlandet.no/images/Kompetansemegling/090610%20vri-km_flyer.pdf (udatert, hentet 06.05.2011).

¹⁸ *Technology Transfer Office* er avdelinger i ved høgskoler og universitet som spesialiserer seg på kommersialisering av innovasjon som oppstår innenfor academia (Macho-Stadler et al. (2007)

¹⁹ Trippel helix viser hvordan samspillet mellom universitet/høgskole, næringsliv og offentlig forvaltning tilrettelegger for innovasjon og næringsutvikling. Ofte ligger ønsket om kompetanseutvikling innenfor et

forteller at man ville samle akademia og næringslivet under veiledning av noen som klarte ”å tenke i begge baner samtidig”. Jens forklarte at *“Alle hadde ønsker og behov innenfor å utvikle sin butikk videre, og tenkte altså næringsliv. Så jobben var jo å koble det mot akademia, fordi de snakket to vidt forskjellige språk”*. Informanten forteller videre at det ble gjort ulike tiltak for å ”megle” mellom høgskole og næringsliv. Man hadde konferanser og arrangementer hvor man presenterte bedriftene for arbeidet på høgskolen og vice versa for å øke forståelsen og kunnskapen mellom de ulike aktørene. Da Bluelight gikk over i Security Valley ble som nevnt koblingen mellom forskningmiljø og bedrifter mer en målsetning i seg selv enn et verktøy for å løse konkrete utfordringer hos aktørene i nettverket. Idar forteller at han opplever det som essensielt at kompetansemeglingsfunksjonen dreier seg om å løse konkrete utfordringer, i stedet for å bruke funksjonen til å utvikle problemstillinger som nettverket kan arbeide rundt. Han mener dette fungerte på ulike måter i Bluelight og Security Valley:

Nei, i Bluelight så fungerte det på en måte litt etter hensikten og etter boka der, men Security Valley ble på en måte... Jeg vet ikke hva jeg skal si... Da beveger vi oss litt over i en annen verden. Man begynte med målsetninger om å skape så og så mange arbeidsplasser og... Så man ville finne ut om det var noen som hadde lyst til å jobbe sammen her, mens i Bluelight-perioden så jobbet man ut fra konkrete behov og konkrete applikasjoner da. I Security Valley så ble det mer å ha en overordnet ambisjon og løpe rundt å prøve å få til noe på det.

Slik jeg tolker dette er det er spørsmål om forskjeller i den grunnleggende modellen man ønsket å bygge innovasjonsnettverket/klyngen på. Bluelight hadde en logikk som gikk på å benytte fasilitering og kompetansemegling som et verktøy for å løse et problem:

Problem → fasilitering/kompetansemegling → løsning

Så lenge man hadde finansiering via Arenaprogrammet fungerte denne modellen godt, men den genererte ingen finansiering i seg selv. Det var dette Security Valley forsøkte å løse med en annen modell:

Prosjektkoordinering/kompetansemegling → finne problem → eksistensgrunnlag

Flere av informantene jeg har snakket med hadde ingen klar oppfattelse av Gjøvik Kunnskapspark sin rolle som drivernode i Security Valley. En av informantene fortalte at det var først i etterkant av Security Valley at han oppfattet at kunnskapsparken skulle ha

regionalt satsningsfelt som grunnlag for økt satsning på regionale høgskoler/universiteter og FoU. Kunnskapsveksten vil gjenspeile seg i klyngeetablering, og opprettholdelsen av trippel helix som et gjensidig støttende system (Etzkowitz 2008).

rollen som kompetansemegler. Flere av informantene har derimot oppfattet at kunnskapsparkens egeninteresse i Security Valley gikk ut over kompetansemeglerrollen. Dette vil jeg komme tilbake til i kapittel 6.

5.7 Koblingen til HiG

Forholdet mellom Gjøvik Kunnskapspark og Høgskolen i Gjøvik har alltid vært tett. Høgskolen har vært inkludert i GKP gjennom representanter i styret, og i inkubatorsammenheng har kunnskapsparken ved en rekke tilfeller vist seg som et godt kommersialiseringsverktøy. I årene da Bluelight hadde finansiering gjennom Arenaprogrammet og målsettingene først og fremst handlet om kompetanseutvikling, var samspillet med HiG tett også på nettverkssiden. Når det gjelder andre områder enn kompetanseutvikling – det vil si etableringen av informasjonssikkerhet som studium på HiG – er det imidlertid mer uklart hva som har kommet ut av samarbeidet med høgskolen innenfor innovasjonsnettverkene. En informant fortalte at på tross av at det finnes et tungt kompetansemiljø på informasjonssikkerhet ved HiG, er det begrenset hvor mye konkret som har kommet ut av samarbeidet. Informanten viser til at koblingen til høgskolen har vært viktig for å bygge trygghet rundt eksistensgrunnlaget til informasjonssikkerhetsnettverkene, men at det forskningsmessige fokuset for høgskolen ikke alltid har ligget til rette for næringslivsaktørene:

Jens: Kan vel si at vi skrøt jo av vårt tette samarbeid med HiG hele veien, altså det var viktig å ha i bunnen for å vise at vi har et tungt kompetansemiljø her, men hvor mye vi har direkte fått ut i den sammenhengen når du begynte å tenke prosjekter... Jeg synes kanskje ikke det fungerte like bra. Det har nok vært litt for stor fokus på grunnforskning der, og det er først de siste par årene at de har fått inn en del professorer som har vært litt mer orientert mot anvendt forskning, og tenker tett samarbeid. (...) Det ble jobbet med å etablere det man kalte en TTO, altså (...) å kunne overføre kompetanse fra høgskole, kompetansemiljø over i næringslivet. Så det ble jobbet noe mer med det, men helt klart; der kunne det blitt gjort betraktelig mer.

Intervjuer: Opplevde du at den koblinga mot kunnskapsmiljøet på HiG og andre forskningsinstitusjoner som var innenfor nettverket da var noe som reduserte usikkerheten?

Jens: Jeg vet ikke om det reduserte noen usikkerhet, men det gav en ekstra trygghet. Så to sider av samme sak. Helt klart en viktig betydning for nettverkets eksistens at høgskolen var med.

I sitatet forteller Jens at samarbeidet med høgskolen har fungert som sikkerhet rundt prosjektet, og at koblingen til HiG som en sterk kompetanseaktør er essensielt for nettverksarbeidet rundt informasjonssikkerhet som er gjort i Innlandet de siste ti årene. I sitatet pekes det likevel på at den konkrete nytten av koblingen til HiG innenfor innovasjonsnettverkene er vanskelig å identifisere, og at denne linken nok hadde vært mer fruktbar hvis man hadde fått på plass en bedre kompetansemeglingsfunksjon eller et TTO.

Fra NCE-søknaden til Security Valley går det frem at GKP som navet i nettverket skulle ha en rekke koordineringsfunksjoner for prosjektene innenfor klyngen. Koblingen mellom kompetanseaktørene HiG, NISlab og Campus Kjeller og næringslivsaktørene stod i sentrum for satsningen, men fasiliteringsfunksjonen, eller kompetansemeglerrollen nevnes ikke. Det gjør heller ikke arbeidet med et TTO. På spørsmål om hvordan GKP er aktive med å koble sikkerhetsbedriftene innenfor SECTOR til relevante kompetansepersoner og prosjekter på HiG fortalte en informant meg at han først etter at Security Valley hadde strandet oppfattet at dette var en av egenskapene nettverket skulle ha. Han opplevde videre at kimen til å få til en effektiv kompetansemegling eksisterte i visjonen Security Valley, men at dynamikken innenfor nettverket gjorde at hans bedrift ble plassert på sidelinjen. Fra høgskolens side har samarbeidet fra Security Valley heller ikke stått i høgsetet. Tore fortalte at usikkerhet rundt forretningsplanen til Security Valley gjorde at høgskolen ikke ønsket å legge verken penger eller mye energi inn i samarbeidet:

Når Security Valley da skulle starte så... Det var jo positivt fordi det høres ut som et godt initiativ, og det så jo veldig flott ut med de målene. Men så stilte man spørsmål til kunnskapsparken da, for høgskolen skulle jo bli med å finansiere dette her. Og da ville høgskolen se forretningsplanen, altså hvordan Security Valley går rundt. Og den spurte høgskolen etter to ganger på et halvt år, og fikk aldri noe svar på. Og da fikk det der seile sin egen sjø.

Bruker vi Boschmas (2005) nærhetsdimensjoner i betraktningen av forholdet mellom høgskolen og innovasjonsnettverkssiden hos Gjøvik Kunnskapspark, synes det rimelig å anta at den geografiske nærheten har vært vesentlig for å kunne argumentere for eksistensen av en kompetansekjerne på Gjøvik. Informasjonen fra mine informanter støtter også Andersen (2006) som skriver at den kognitive, sosiale og organisatoriske nærheten var en vesentlig forutsetning for måloppnåelsen i Bluelight. Mine data viser likevel at det i årene etter arenaperioden, og særlig i Security Valley-perioden oppstod en større organisatorisk avstand mellom Security Valley og HiG. I sitatet ovenfor går det frem hvordan HiG ikke lenger så det mulig å delta aktivt i prosjektet. Dette kan sies å bryte opp deler av den sosiale kapitalen som forelå gjennom flere års arbeid ved at HiG som klyngeaktør ikke lenger så muligheten for linking eller bridging innenfor Security Valley, jf. Halpern (2005), i Johnstad (2009).

5.8 Tidsperspektivet

Som tidligere nevnt må hovedmålet med Security Valley sies å være sikring av finansiering til informasjonssikkerhetsaktivitetene på Innlandet generelt, og Gjøvik

spesielt, ved å etablere et NCE med drivernode i Gjøvik Kunnskapspark. Målet med Security Valley var dermed mer abstrakt enn hva det var med Bluelight. Dette gjorde sannsynligvis at det for Security Valley var enda viktigere å synliggjøre realiseringen av delmål. Prosjektet Security Valley var i en intensiv periode i 2008 og 2009 for å bygge et nettverk stort nok til å fundere et NCE. Dette arbeidet var også økonomisk krevende, slik at det var viktig å oppnå målet med stabil finansiering hurtig. Jens forklarte at Security Valley strandet nettopp på grunn av en unaturlig vekstrate, siden vekst gikk på bekostning av utvikling og stabilisering av fundamentet for informasjonssikkerhetsarbeidet, nemlig det som var ”gamle” Bluelight.

Jens: Jeg vil da si at Security Valley var en flopp! Og jeg skjønner jo også hvorfor, og det så jeg vel egentlig tidligere enn det en del andre gjorde. Poenget er at et cluster er noe som må vokse naturlig og det tar jo 10 til 20 år å få bygd opp et sånt type miljø. Og Bluelight vokste stille og rolig, også ønsket man da å løfte det videre da man ikke fikk mer støtte fra myndighetene, altså Innovasjon Norge i dette tilfellet her. Derfor prøvde man å vri det over til Security Valley. Og det ble et luftslått med et fint navn og en god tanke, også ble det ansatt litt mange mennesker inn i et cluster som ikke hadde nok fundament enda. Og sånn sett så brukte Security Valley opp kontantsummen sin raskere enn man klarte å skaffe mer inn, og døde på grunn av det.

Intervjuer: Tok man et steg til bake da Security Valley ble videreføringen av Bluelight?

Jens: Man tok vel ikke et steg tilbake, men man prøvde å se det i en litt større kontekst. Begynte å bevege seg litt utenfor landets grenser (...). Men det handler om finansiering, og når det ikke var mer Arena-penger (...) så prøvde man seg på NCE, men var ikke store nok til å bli det, dessverre. Men det tror jeg nok man kanskje kunne løst, hadde man fått da den finansieringen til å kunne jobbe i tre, fire, fem år til så hadde det vært mulig å få noe ut av dette her. Men du bygger ikke opp et cluster på 3 – 4 år. Og det er... ja... det kunne kanskje Innovasjon Norge bidratt med, men de valgte å se bort fra det i neste fase selv om de hadde investert fire år i Bluelight så ville de ikke være med videre.

Ser vi igjen Bluelight og Security Valley i lys av målsetninger om regional innovasjon er det nærliggende å reise spørsmål ved Innovasjon Norges forhold til prosjektene man har investert i gjennom Arena, men som ikke går over i NCE. Informanten stilte senere i intervjuet spørsmålsteget ved Innovasjon Norges prioriteringer i forbindelse med ettervern av disse prosjektene. Ut fra mine data er dette et betimelig spørsmål ettersom det synes å være en gjennomgående holdning at Innlandet – og Gjøvik-distriktet spesielt – hadde vært tjent med å ha en informasjonssikkerhetsklynge i dag.

5.9 Bottom up vs. Top down

I dette kapittelet har jeg pekt på en rekke forhold ved nettverk for samarbeid og innovasjon som har fungert ulikt i prosjektene Bluelight og Security Valley. Ingen av prosjektene klarte å oppnå betingelsene for videre opprettholdelse, og man kan dermed si at verken Bluelight eller Security Valley oppnådde stabilisering som nettverk for samarbeid og innovasjon. Det innovative miljøet rundt informasjonssikkerhet som startet med

etableringen av masterstudiet i informasjonssikkerhet ved HiG i 2001/2002 og som ble videreført i arenaperioden til Bluelight, kan ikke sees å ha blitt stabilisert gjennom Security Valley, siden det ikke ble oppnådd fremtidig finansiering. Tabellen oppsummerer funnene som er drøftet i dette kapittelet:

Bluelight – bottom up	Security Valley – top down
Kompetanseutvikling.	Rammeverk for forretnings samarbeid.
Offentlig støtte. Høykonjunkturperiode.	Medlemskontingent, noe offentlig støtte, egenkapital. Lavkonjunkturperiode.
Konkrete behov og målsetninger.	Rammeverk for samarbeid. I liten grad konkrete produkter, tjenester og behov. Målsetninger betraktes som visjoner.
Proof of the pudding. Markedsføring av prosjektet gjennom deltakerne.	Visjon. Markedsføring av eget prosjekt.
Sakte bygging av fundament.	Hurtig vekst.
Fasilitator. Integrert kompetansemegler og prosesskompetanse.	Prosjektleder og prosjektgruppe. Kompetansemegling og prosesskompetanse som uttalt målsetting.
Reell kobling mot HiG og NISlab Liten kobling mot akademia forøvrig.	Liten reell kobling mot NISlab (og HiG forøvrig). Kobling mot akademia og forskningsmiljø i inn- og utland.
Regionalt.	Regionalt? Nasjonalt? Internasjonalt?
Identitet, fellesskapsfølelse blant de fleste (jfr. Andersen 2006).	Mangel på identitet og fellesskapsfølelse hos de fleste.
Dårlig utbygget IKT-støtte i kommunikasjon og kunnskapsdeling.	Godt utbygget IKT-støtte i kommunikasjon og kunnskapsdeling.

Tabell 2: Nøkkelkarakteristikker ved Bluelight og Security Valley.

Det ser ut til at Bluelight var lettere å stabilisere som nettverk for innovasjon og samarbeid siden det dreide seg om kompetanseutvikling snarere enn bedriftssamarbeid og aktørenes interesser knyttet til direkte inntjening. Etableringen – og stabiliseringen – av et rammeverk for samarbeid er imidlertid ikke gratis, og næringsliv kan vanskelig mobiliseres uten å kunne identifisere ”what’s in it for me”, også i et kortsiktig perspektiv. Skal en kunnskapspark stabilisere et nettverk for bedriftssamarbeid og inntjeningsmuligheter, samtidig med å opprettholde sine forpliktelser som regional innovasjonsaktør, må det dermed etableres tillit og felles forståelse rundt prosjektets omfang og målsetninger. Tillit og sosial kapital kan forsterkes eller forvitre, slik at arbeidet med å skape en

fellesskapsfølelse og gjensidig kjennskap til hverandre blant aktørene bør være et kontinuerlig fokus. Hele samarbeidet bør bygges på konkrete behov fremsatt av aktørene, og det må vektlegges felles forståelse rundt dette.

Fra det teoretiske perspektivet viser diskusjonen i dette kapittelet til hvordan et bevisst forhold til autokommunikasjon kan balansere connectedness og consistency for å legge til rette for sosial kapital. Ut fra min analyse ser dette ut til å ha vært det grunnleggende problemet med Security Valley som Gjøvik Kunnskapspark ikke klarte å løse i tide: Hvor Bluelight hadde vært et prosjekt med rotfeste i konkrete behov og felles forståelse (*bottom up*), var Security Valley et rammeverk uten dette fotfestet hos medlemmene (*top down*). Selv om det kan antas å være en kognitiv og organisatorisk nærhet, må tillitsarbeidet og felles forståelse ligge i grunn. Erfaringer fra Bluelight tyder på at ansikt-til-ansikt-kommunikasjon er nødvendig for å bygge tillitsfulle relasjoner, og videre en forutsetning for å få kommunikasjon via IKT til å lykkes. Også denne studien viser at velutbygget IKT er et godt supplement til ansikt-til-ansikt-kommunikasjon, men at det aldri kan erstatte den når det kommer til tillitsbygging. Dette støttes også av Vålands (2004) og Bergums (2004) forskning på området. Identitet, fellesskapsfølelse og et innovativt klima bygges gjennom delresultater. Dette må synliggjøres innad, f.eks. gjennom konferanser og møter og nettsiden, og det må synliggjøres utad gjennom de aktørene som har vært delaktig i realiseringen av delmålene. Det er viktig at det er samsvar mellom det som kommuniseres utad og det som kommuniseres innad for å opprettholde en samlet identitet og felles forståelse av prosjektet og dets omfang. Fasilitering bør være knyttet opp mot tilrettelegging for oppnåelse av konkrete mål med støtte hos deltakere, ikke knyttet opp mot egeninteresse hos drivernoden.

Å utvikle et kompetansenettverk til å bli en næringsklynge hvor inntjeningspotensial er sentralt, ser ut til å være avhengig av langsiktig offentlig økonomisk støtte. En bråstopp som følge av tap av stabil inntekt ser ut til å skape et vakuum i det innovative klimaet innenfor klyngen. Det er vanskelig å stabilisere et nettverk på kort tid og med usikker finansiering. I neste kapittel vil jeg gå nærmere inn på hvordan Security Valley ble oppfattet av gründeraktørene i nettverket. Hvorfor klarte ikke Security Valley å oppnå en god dynamikk i innovasjonsmiljøet det var en del av i Gjøvik Kunnskapspark?

6. Innovasjonsnettverk vs. innovasjonsinfrastruktur

Gjøvik Kunnskapspark hadde siden starten i 2000 bygget opp en parallell satsning på innovasjonsnettverk og innovasjonsinfrastruktur som gjensidig støttende funksjoner. Innovasjonsnettverk viser til samarbeidsprosjekter mellom flere etablerte organisasjoner som sammen jobber mot en felles målsetning innenfor rammen av regional innovasjon, mens innovasjonsinfrastrukturen består av inkubator og tilknyttet aktivitet rundt fremming av gründerskap og kobling til finansieringsordninger. Innovasjonsnettverkene skal kunne bidra til å koble gründerbedriftene innenfor inkubatoren til marked, og til andre relevante markeds- og kompetanseaktører. Innovasjonsinfrastrukturen støtter nettverksdelen ved å videreføre arbeidet innenfor nettverkene gjennom nye bedriftsetableringer, og er et kommersialiseringsverktøy for innovasjon. I innovasjonsnettverket/klyngeprosjektet Security Valley var inkubatoren SECTOR en inkludert del av nettverket fra starten. Dette må sees som en annen tilnærming til forholdet mellom innovasjonsnettverk og innovasjonsinfrastruktur enn man hadde sett tidligere med for eksempel Bluelight hvor inkubator ikke var en integrert del av arbeidet innenfor nettverket.

I dette kapittelet vil jeg drøfte mine informanternes utsagn omkring hvordan det oppstod en spenning mellom Security Valley som innovasjonsnettverk og SECTOR – eller *Security Valley Incubator* – som innovasjonsinfrastruktur. Jeg vil vise hvordan dette kan sies å ha bidratt til friksjon i aktørrelasjonene innenfor klyngen, og dermed peke på hvordan kontinuerlig arbeid med fundamentet i kjerneområdet kan bidra til å stabilisere nettverk for samarbeid og innovasjon. Fra flere intervjuer har jeg indikasjoner på at tilliten mellom de små bedriftene med (informasjons)sikkerhet som kjerneområde, og de store bedriftene som hadde dette som en mer perifer aktivitet, ikke var tilstrekkelig utbygget i Security Valley. Flere av de små aktørene opplevde å bli satt på sidelinjen mens prosjektledelsen prioriterte synliggjøring av eget prosjekt, store selskaper og internasjonale kompetansemiljøer. Dette må sees i sammenheng med Innovasjon Norges krav til klynger for tildeling av NCE-status, og har implikasjoner for hvordan den sosiale kapitalen i klyngen har kunnet utvikle seg på basis av bonding, bridging og linking. I den videre analysen vil jeg ta utgangspunkt i begrepene innovasjonsnettverk og innovasjonsinfrastruktur for å gå inn på forholdet mellom prosjektet Security Valley og gründerbedriftene som var en del av miljøet i Gjøvik Kunnskapspark. På hvilken måte fungerte Security Valley som støtte for inkubatorbedriftene? Gikk satsningen på stabilisering av nettverket gjennom NCE på bekostning av å bygge et solid fundament?

6.1 Bredt samarbeidsprosjekt vs. produktfokus

Som drøftet i kapittel 5.1 peker flere informanter på at Security Valley i liten grad klarte å fokusere arbeidet rundt konkrete behov hos medlemmene, og at prosjektet dermed ble oppfattet diffust og lite relevant. Flere av gründerne jeg har snakket med understreker nødvendigheten i å fundere et bedriftsnettverk eller en klynge-satsning i de konkrete produktene som aktørene innehar, eller som kan utvikles i fellesskap. Informanten Jan Petter fortalte at han i utgangspunktet syntes tanken om å bygge opp et nettverk eller en klynge for informasjonssikkerhet i Innlandet var positiv, men kritiserte prosjektet Security Valley på flere punkter. For det første mente han at det konkrete produktfokus manglet, og at man dermed dreide fokus bort fra inntjeningsmuligheter som lå i produktsalg, og at prosjektet dermed ikke ble oppfattet som en investering i gründerstøtte og bedriftsutvikling. For det andre oppfattet han arbeidet med nettverksbygging på nasjonalt og internasjonalt nivå som for lite praktisk innstilt, og at dette gikk på bekostning av det lokale/regionale fokuset.

Altså, for det første så var det totalt feilsatsning. Det eneste det gjorde var å generere masse arbeid for seg selv. Altså, de hadde jo ikke noe produkt! Og når det ikke er noe produkt så er det uinteressant. (...) Og jeg har alltid ment – og mener fremdeles – at skal Security Valley bli noe av som det egentlig har muligheten til å bli, så må det punkt 1 ha produkt. Jeg som bedrift, hva kan jeg oppnå ved å være med i Security Valley? Også kundene, de som vil kjøpe tjenestene våre, fra kollegaer og andre firma, hvordan får de tak i produktene? Altså, det var jo *ingen* satsning på det. Det var veldig sånn å etablere seg mot tyske og engelske og canadiske nettverk, som er så *far beyond scope*, altså. Når du er gründer og sitter der og lurere mer på hvordan du skal få lønning neste måned, da er du avhengig av produkter, og du er avhengig av å få folk til å kjøpe produktene dine. Det hadde de glemt.

Det brede arbeidet med nettverksetablering både på nasjonalt og internasjonalt nivå må sees i forbindelse med arbeidet rundt å skape et stort nok miljø med globale *pipelines* for bli anerkjent som NCE, og dermed sikre fremtidig finansiering. Å støtte gründerne som en inkludert del av nettverket/klyngen ser dermed ut til å ha vært vanskelig forenlig med arbeidet rundt å skape et miljø som kvalifiserer til NCE. Jan Petter mente at Security Valley i større grad burde frontet klyngeaktørens produkter i stedet for å fokusere på videre nettverksbygging. Selv om gründerbedriftene i inkubatoren var av liten økonomisk betydning for Security Valley, var de likevel viktige av flere årsaker. For det første har det med tillitsforhold, fellesskapsfølelse og buzz i et relativt lite arbeidsmiljø å gjøre. For det andre ville det bidratt til consistency ved å vise et samsvar mellom klyngeprosjektets interesser og aktørens interesser. For det tredje må inkludering av inkubatoren sees som

viktig for legitimiteten til prosjektet hos GKPs styre og eiere, og hos Innovasjon Norge, Forskningsrådet og SIVA i forhold til NCE-status.

I NCE-søknaden til Security Valley nevnes seks konkrete produktrelaterte prosjekter som har oppstått mellom bedrifter innenfor nettverket (Security Valley 2009: 12):

- Utvikling av UAV-løsninger (Unmanned Aerial Vehicles) for sikring av områder
- Utvikling av løsninger for merking av overgripere, hjemmesoning og omvendt voldsalarm mellom Stealth Scientific, Telenor og SFAS Security.
- E-læringskonsept innenfor informasjonssikkerhet mellom Apropos Internett, Virosafe og kommunene i IKOMM.
- Utvikling av identitetskortløsning mellom 3 klyngeaktører
- Utvikling av ”Biometric Bag Drop” mellom Genkey, IDEX og Norwegian på Rygge Flyplass.
- Utvikling av fremtidens intelligente våpenskap mellom Stealth Scientific og Raufoss Ammunisjonsfabrikker

Fra securityvalley.no og relaterte medieoppslag fremgår ingen spesiell synliggjøring av disse produktene fra Security Valley sin side, men snarere en synliggjøring av Security Valley som en merkevare i seg selv. På spørsmål om hvordan Gjøvik Kunnskapspark synliggjorde seg gjennom Security Valley fortalte Jan Petter at *”De var hele tiden opptatt av å finne ett eller annet forskningsmiljø ett eller annet sted og knytte noen kontakter og rammeavtaler og høye smørbrød og sånn i stedet for å si at ”disse produktene har vi”*. Jan Petter fortalte videre at han synes kunnskapsparken burde fokusere sterkere på å bidra i markedsføringen av produktene til inkubatorbedriftene ved å lage ”happeninger”, og så at dette potensialet lå i Security Valley når det gjaldt inkubatorbedrifter innenfor informasjonssikkerhetsmarkedet. Han opplevde likevel ikke at Gjøvik Kunnskapspark gjennom Security Valley bidro til dette selv om det hadde vært god markedsføring av både gründerbedriftene og klyngeprosjektet i seg selv, noe som i neste rekke ville kunne bidra til å stabilisere og tillitsgjøre Security Valley som innovasjonsnettverk. Dette er i stor grad et ekko av hva vi tidligere har drøftet med tanke på viktigheten av et konkret fokus i innovasjonsnettverk. Tore oppsummerte det slik: *”Og Security Valley kunne ha blitt noe det, hvis man bare hadde hatt en to-tre skikkelige punchlines hver gang bedriftene spurte helt konkret what’s in it for me?”*

Informanten Karl representerte også en av inkubatorbedriftene i nettverket, men har en annen oppfattelse av hva som fungerte og ikke fungerte i prosjektet. Han vurderte arbeidet som ble lagt ned i å knytte til seg internasjonale kompetanseaktører som positivt, og forteller at hans bedrift fikk til konkrete samarbeid på produkter og tjenester med utenlandske firma via Security Valley. Han understreker likevel at det må arbeides med konkret produktutvikling dersom man skal få noe ut av nettverksarbeid, det holder ikke *”å bare være med”*.

6.2 Gjøvik Kunnskapspark sin egeninteresse vs. gründeres interesser

Fra NCE-søknaden går det frem klare målsetninger om å utvikle arbeidsplasser innenfor klyngen, og å utvikle Gjøvik Kunnskapspark som en administrasjonsenhet innenfor nettverket/klyngen. Det kan synes som om visjonen om å etablere en bærekraftig klynge for informasjonssikkerhet ved å formalisere samarbeid mellom både regionalt, nasjonal og internasjonalt distribuerte aktører gjennom Security Valley-prosjektet ble en egeninteresse for Gjøvik Kunnskapspark. Informanten Stein Ove var tilknyttet Security Valley gjennom sin gründerbedrift innenfor SECTOR. Han fortalte at han oppfattet at fokuset på å etablere Security Valley som en næringsklynge for det første gjorde at gründerbedrifter i Gjøvik havnet i konkurranse med store etablerte bedrifter i Oslo, og at han for det andre opplevde i praksis å bli stengt ute fra prosjektet siden han fikk lite informasjon om hva som foregikk: *”Jeg følte at folk trodde ikke på det jeg gjorde, dermed så måtte jeg oppsøke og søke etter informasjon selv. Jeg fikk ingen informasjon automatisk”*. Informanten fortalte likevel at han oppfattet den uformelle kontakten innad i kjernemiljøet som god. Jeg tolker dette som et klart eksempel på ubalanse mellom Boschmas (2005) nærhetsdimensjoner. Sitatet ovenfor peker på at selv om det fantes sosial nærhet som følge av den uformelle kontakten aktørene mellom, opplevde informanten i mindre grad en organisatorisk nærhet på grunn av oppfatningen om manglende informasjon. I tillegg fortalte Stein Ove at profileringen av Gjøvik Kunnskapspark gjennom Security Valley-prosjektet gikk på bekostning av å synliggjøre bedriftene innenfor GKP slik man tidligere hadde gjort. I følgende sitat spurte jeg informanten om i hvilken grad det er ønskelig at Gjøvik Kunnskapspark som innovasjonsbedrift synliggjør seg på bred basis overfor næringslivet:

Tveegga sverd, fordi den satsinga på Security Valley som var her, det var jo delvis i konkurranse med bedrifter som var i inkubatoren. Det ble for store interessemotsetninger i det å satse på egen bedrift og egen synliggjøring og det at andre bedrifter som var med i inkubatoren også skulle jobbe innenfor samme område. Så det tror jeg er en farlig vei å gå faktisk, jeg tror inkubatoren og kunnskapsparken – derav – bør satse på å hjelpe de bedriftene som er her enn å drive egen business

(...) Security Valley-satsinga, den har blitt lagt merke til. Og det hjalp en stund å kunne skilte med at du var en del av Security Valley. Nå har Security Valley fått et negativt fortegn fordi det ikke gikk slik som man hadde planlagt. Så sånn sett så vet jeg ikke om det er verdifullt lenger å ha det på visittkortet eller ikke. Men det er klart at den type satsinger for miljøet totalt sett kan være positiv hvis det gjøres riktig.

Informanten snakker i forlengelsen av dette om at han har stor tro på klynge-satsninger og fokuserte prosjekter for å skape et samarbeidsmiljø, men at dette forutsetter at det finnes et sekretariat som kan holde seg til den røde tråden. Han vektlegger også at slike satsninger må forankres lokalt, og at det dermed også finnes potensial for å utvikle en fellesskapsfølelse rundt delt og komplementær kompetanse. Dette er klart i tråd med hvordan Cheney og Christensen (2001) beskriver at autokommunikasjon kan være vesentlig for å skape identitet, og i neste rekke stabilisere nettverk. I forlengelsen av dette kan man si at sosial kapital kan bygges på grunnlag av denne fellesskapsfølelsen. Stein Olav fortalte videre om en for stor satsning på et stort prosjekt, noe som resulterte i at omfang og veksthurtighet ikke hang på greip med det man skapte blest om. Denne tolkningen tilsvarer inntrykket Jens hadde om at næringsklynger vanskelig kan etableres over kort tid, siden det krever både et svært solid fundament i medlemsmassen og konkrete oppgaver å bygge på.

Intervjuer: Hvordan opplever du den eksternt rettede kommunikasjonen i Security Valley? Altså mot eksterne kompetansemiljøer, brukergrupper, kunder osv.?

Stein Ove: Den opplever jeg... Tja, hva skal jeg si... Til dels litt hodeløst og lite målretta. Det ble liksom veldig mye PR og lite saft bak. (...) sånn som jeg opplever det, så synes jeg at det gikk litt for fort. Fordi at det ble ansatt folk her, i et lite miljø. Tre stykker samtidig, og det ble en litt for heavy satsing. Så man fikk ikke oppdrag til alle, også gikk det på trynet økonomisk. Det er vel det som er en kort oppsummering. Også at man måtte rydde opp i det, og da ble oppryddinga så kraftig at det ble ikke så mye igjen.

Informanten forteller videre at det kun i liten grad fantes noen formalisert internkommunikasjon i klyngens drivernode, altså Gjøvik Kunnskapspark. På tross av at kommunikasjonsinfrastrukturen i form av e-postlister, hjemmeside og kontorfellesskap forelå, peker flere av informantene på at internkommunikasjonen som sådan hadde vesentlige mangler. Flere av gründer-aktørene fortalte at det opplevdes som vanskelig å "slippe inn" i det som foregikk i Security Valley. Dette artet seg på den måten at man ikke opplevde å motta noen informasjon om hva som foregikk, men måtte oppsøke denne informasjonen selv. Igjen ser vi relevansen Castells (1996) nettverksteori som påpeker at consistency og connectedness som gjensidig støttende funksjoner for suksessfulle nettverkssamarbeid. Det er likevel ulike oppfattelser rundt kommunikasjonen i Security Valley, siden flere informanter vurderte informasjonsflyten som god. Dette viser imidlertid til at mer arbeid burde vært lagt ned i å sikre at informasjon kom ut til *alle* aktører. Blant

gründerbedriftene som var lokalisert innenfor Gjøvik Kunnskapspark sine lokaler opplevdes informasjonsflyten mer som ”korridorssnakk” mellom kolleger enn som strukturert informasjon. Dette viser til at det også er behov for strukturert informasjon i små bedriftsmiljøer, selv om de fleste av mine informanter som arbeider eller har arbeidet innenfor inkubatoren understreker viktigheten av den uformelle kommunikasjonen mellom gründere. I tillegg påpekte Jan Petter at alle nyheter ikke nødvendigvis bidrar til å skape en fellesskapsfølelse: når det ”store” aktørene innenfor prosjektet drar på tur til Silicon Valley sammen, kan det for gründerbedriftene føles som at de blir tilsidesatt, siden de ikke har ressurser til å delta på den type opplegg:

I Security Valley vet jeg ikke, for man slapp jo aldri inn i det miljøet der. (...) Man fikk høre at man inviterte til bransjesamling i Silicon Valley. Og det er veldig relevant når man sitter som gründer og lurer på om man får etableringsstipendet sitt. Men i parken så var det litt mer sånn over kaffen, som du sier, og man slang seg ned på pulten, og jeg snakket masse med [firmanavn] blant annet. Jeg hadde en del kontakt med dem. Og det ble jo noe ut av det da.

Det som imidlertid ble oppfattet positivt er ansikt-til-ansikt-kontakten det ble lagt opp til mellom aktørene. Dette støtter også nødvendigheten av umediert kontakt for tillitsskaping mellom samarbeidende aktører som Jens og Idar fortalte om i kapittel 5.2. Stein Ove forklarte:

Det ble holdt noen sånne månedlige møter oppi kantina som jeg opplevde ganske positivt. Og det var jo bedrifter rundt omkring innkalt til de møtene der. Det varte vel et halvt år eller vel så 9 mnd, også kokte det bort i kålen. Det kunne blitt en type nettverksbygging, og det ble tatt opp interessante tema som korte foredrag og sånt noe. Og der kunne man også lære å kjenne nye fjes. Det kunne blitt en bra seanse.

Informantens uttalelse er i tråd med teorien og tidligere forskning som sier at umediert kontakt og personlige knutepunkter er viktig for klyngeutviklingen, spesielt i startfasen av prosjektet (Dahl og Pedersen 2004; Våland 2004; Bergum 2004).

6.3 Geografisk omfang

Security Valley kan altså beskrives som et prosjekt for å samle informasjonssikkerhetsaktivitetene på Gjøvik og Innlandet generelt under én paraply, og slik sett bygge ut informasjonssikkerhet som en del av det regionale innovasjonssystemet. Som nevnt i forrige kapittel hadde Security Valley også klart internasjonale ambisjoner, noe som ble betraktet som positivt fra politisk hold. Internasjonaliseringspotensialet er også at uttalt krav som stilles til NCE-kandidater, slik at fokuset på å etablere pipelines kan knyttes til fremtidige finansieringsstøtte gjennom NCE-programmet. Med regionale og

lokale målsetninger på den ene siden, og internasjonale målsetninger på den annen side, ser det ut til at det har vært vanskelig for mange av aktørene i Security Valley å danne seg en klar oppfattelse av prosjektets geografiske omfang. Tore forklarte at også høghskolen hadde vanskelig for å forstå omfanget av prosjektet:

Intervjuer: Var det et klyngeprosjekt med regional forankring, eller var det nasjonalt, eller skulle det ha et internasjonalt nedslagsfelt? Var det en felles forståelse rundt dette her på noe tidspunkt tror du?
Tore: Det var ikke noen felles forståelse sånn som jeg var klar over det. (...) det er nettopp det du spør om nå som er nettopp det samme som vi spurte om – vi ville gjerne være med videre, men hva er den konkrete modellen? Og det fikk vi aldri tydelig svar på. Så jeg vet rett og slett ikke helt. (...) altså Høghskolen i Gjøvik er jo en viktig aktør i regionen her, så alt vi kan gjøre for å støtte opp om bedriftsetableringer og nye arbeidsplasser der må vi selvfølgelig være aktive. Så vi var interesserte i å bli med på det da. Men det ble ikke konkret nok. Og da må jo vi fokusere på kjerneaktiviteten som er å utdanne kandidater som passer inn i bedriftene som er med her.

Fra sitatet forstår vi at visjonen bak Security Valley, altså å kunne være et innovasjonsnettverk eller en klynge for utvikling innenfor og mellom bedrifter, gründere og kunnskapsaktører ble vurdert som positivt, men at uklarhet rundt omfanget til prosjektet var et vesentlig usikkerhetsmoment. Denne usikkerheten ser i seg selv ut til å ha motarbeidet målsettingene med prosjektet, siden man ikke klarte å oppnå helhjertet deltakelse fra viktige aktører. I neste sitat presenteres gründeren Cato sitt perspektiv på hvordan GKP i fortiden har ivaretatt det lokale, og hvordan man bør gjøre dette i fortsettelsen. Han knytter fokuset på lokal/regionale innovasjonsnettverk til utviklingen av et innovativt klima, og forteller at han opplevde dette som sterkere før. Cato forklarer at synliggjøring av lokale prosjekter er viktig, og at dette fungerte bedre for noen år tilbake:

(...) den Security Valley, den... Jeg er ikke så sikker på om den var veldig rettet lokalt her. Det var nok kanskje ikke det. Opplevde det ikke sånn i hvert fall. Jeg har vel mer tanker rundt dette med utløp av noen bedrifter sånn som Scandicraft, Innlandets Vitensenter, NCE på Raufoss, også de utspringa hvor stor deltakelse har jo kommet fra GKP. Og de tinga der var jo mer synlig på det tidspunktet der.

Som flere av informantene har uttalt så er det viktig å ha pågående prosjekter og nettverksaktivitet ved siden av inkubatorvirksomheten. Sitatet ovenfor understreker viktigheten av at man befester disse prosjektene på lokalt eller regionalt nivå, som en del av det regionale innovasjonssystemet. Et interessant moment er at på tross av gründerbedriftene, og til dels HiG, ikke oppfattet Security Valley som et regionalt prosjekt, så oppfattet aktører utenfor Innlandet prosjektet som lokalt/regionalt fokusert. Følgende sitat er hentet fra intervju med informanten Trond, som arbeider i en organisasjon utenfor Innlandet, og viser en oppfatning om Security Valley som en geografisk avgrenset innovasjonsnettverk som også har internasjonale aspirasjoner:

Det er klart at tyngden lå jo på Innlandet, og der har de jo mye kompetanse og mange aktive selskap og miljø. Men det bar jo preg av å gjøre noe på nasjonalt plan, og når man kjører studieturer til Tyskland blant annet så er jo det på initiativ til å prøve å få i gang internasjonale eller bilaterale forhold eller samarbeid. Så det synes jeg var positivt. (...) Jeg oppfattet det vel mest som å prøve å få i gang gründere og skape et miljø å etablere flere arbeidsplasser og gjennom det skape fokus på informasjonssikkerhet.

Likevel synes også Trond at det var vanskelig å oppfatte hvilket fokus Security Valley hadde, både hva gjelder konkrete målsetninger og geografisk omfang.

6.4 Et feilslått innovasjonsnettverk?

I dette kapittelet har det blitt drøftet flere vesentlige motsetningsforhold mellom gründerbedriftene innenfor SECTOR inkubator og Security Valley som et klyngeprosjekt under ledelse av Gjøvik Kunnskapspark. Dette ser ut til å ha vært problematisk for den grunnleggende tankegangen rundt innovasjonsnettverk og innovasjonsinfrastruktur som gjensidig støttende funksjoner. Tabellen oppsummerer funn presentert i dette kapittelet:

Security Valley som innovasjonsnettverk	Innovasjonsinfrastruktur
Security Valley som egeninteresse for GKP.	SECTOR og gründernes interesser.
Store organisasjoner, etablert næringsliv.	Gründere. Konkurransforhold med større etablerte bedrifter.
Regionalt/nasjonalt/internasjonalt.	Lokalt/regionalt.
Bredde, rammeverk for samarbeid. Finansiering som overordnet mål (NCE).	Fokus på inntjening og produkter. Finansiering som middel for markedsføring og produktutvikling.
Visjon, markedsføring av prosjektet.	Proof of the pudding, markedsføring av produkter.

Tabell 3: Nøkkeltrekarakteristikker ved Security Valley vs. SECTOR

For prosjektledelsen i Security Valley ser det ut å være vanskelig å forene arbeidet med å oppfylle kravene for NCE med å stabilisere fundamentet for klyngen. Jobben som ble gjort mot NCE ser ut til å ha gått på bekostning av det innovative klimaet i og rundt Gjøvik Kunnskapspark, spesielt blant gründerne. Arbeidet med å bygge et rammeverk for samarbeid med internasjonalt potensiale mellom ulike informasjonssikkerhetsaktører ser ut til å ha vært vanskelig forenlig med å skape og vedlikeholde buzz og sosial kapital innenfor kjerneområdet på Gjøvik. Dette må sees i sammenheng med

kommunikasjonsutfordringene og tidsperspektivet som ble drøftet i kapittel 5. Produktfokus etterlyses for å inkludere de små aktørene og dermed skape et innovativt miljø i drivernoden GKP. Produkt- og markedsfokus står i sentrum i innovasjonsinfrastrukturen. Dette burde sannsynligvis også vært et sterkere fokus i klyngeprosjektet Security Valley siden man valgte å inkludere inkubatoren som en del av klyngen. På tross av at Gjøvik Kunnskapspark som innovasjonsbedrift hadde et veletablert fokus på gründerskap ble det oppfattet at kunnskapsparken satset på Security Valley som en egen merkevare, noe som oppleves som uheldig. I henhold til teori rundt autokommunikasjon er det dekning for å påstå at dette har ført til en ”identitetskrise” for miljøet innenfor Gjøvik Kunnskapspark, og dermed at den sosiale kapitalen og buzzen ble svekket. Det vektlegges blant flere at store satsninger bør funderes lokalt, og det må være samsvar mellom hvordan man agerer ”utad” – eller snarere *oppfattelsen* av hvordan man agerer utad – og hva som skjer ”innad” i organisasjonen. Dette viser at selv i små miljøer hvor den uformelle kommunikasjonen er bra, er det behov for formalisert kommunikasjon og informasjonsdeling. For GKP/Security Valleys del ville dette kunne bidra til å sikre felles forståelse rundt hvordan internasjonale pipelines etableres som støtte til regional innovasjon, ikke omvendt. Dette ville kunne bidratt til å skape consistency.

Klyngeprosjektet Security Valley klarte ikke å stabilisere seg som nettverk, og etter min oppfattelse har også det innovative klimaet rundt informasjonssikkerhet som satsningsområde for regional innovasjon i stor grad visnet. I løpet av de siste ti år med arbeid innenfor informasjonssikkerhet som regionalt innovasjonssatsningsfelt kan man likevel notere noen suksesser. Neste kapittel vil gi oppsummere hvilken lærdom man kan hente fra å studere casen Security Valley, og gi en kort presentasjon av hva som har blitt oppnådd.

7. Svaner og kalkuner: stabilisering av innovasjonsnettverk

Som nevnt innledningsvis kan en overfladisk analyse av aktiviteten rundt innovasjonsnettverk for informasjonssikkerhet i Gjøvik tolkes som historien om svanen som igjen ble til en kalkun. Den tidligere forskningen rundt Bluelight som arenaprosjekt viser til et suksessfullt nettverk som klarte å oppnå mange av målsetningene man hadde satt seg. Bluelight var imidlertid avhengig av et felles fokus på kompetanse og finansieringen via Arena for opprettholdelse, noe som forutsatte nytenkning rundt prosjektfinansiering etter arenaperioden i 2006. Siden det viste seg vanskelig å stabilisere Bluelight som medlemsbasert nettverk, bakte man det i 2008 inn i klyngeprosjektet Security Valley, som arbeidet mot NCE-status innen 2009. På overflaten ser det ut til at Security Valley ble et kostnadskrevende luftslått som kun i liten grad klarte å innrullere og stabilisere medlemsaktørene. En kalkun. Basert på erfaring fra personer hentet fra ulike miljøer og organisasjoner som dannet grunnlaget for Security Valley, danner denne studien et mer nyansert bilde av utviklingen. I analysen ble det belyst hvordan utviklingen fra kompetansenettverk til næringsklynge vanskelig kunne stabiliseres som en top-down modell med usikker finansiering. Innenfor en slik oppbygning ser det også ut til å ha blitt ekstra utfordrende å få innovasjonsnettverk og innovasjonsinfrastruktur til å fungere som gjensidig støttende funksjoner, noe som hadde konsekvenser for det innovative klimaet i kjerneområdet. Dette konklusjonskapitlet fokuserer på tre hovedpoeng knyttet til betingelsene for stabilisering av nettverk for samarbeid og innovasjon.

7.1 Betydningen av temporale forhold og byggingen av enterprise eller bureaucracy

Castells (1996: 187) betrakter byggingen av nettverksorganisasjoner enten som *enterprise*, eller *bureaucracies*. Enterprise setter seg fore å oppnå definerte målsetninger gjennom bruk av ulike virkemidler. Byråkratiet ønsker å oppnå eksistensgrunnlag for seg selv som et rammeverk eller verktøy. I analysen ble det pekt på hvordan Security Valley beveget seg bort fra både det konkrete behovet for kompetanseutvikling som var limet i Bluelight i arenaperioden, men også bort fra bedriftssamarbeidet inn mot konkrete tilbud og produkter. Denne prosessen kan beskrives som overgangen fra en nettverksmodell som enterprise til en byråkratisk modell, hvor målet var selvoppholdelse via finansieringsstøtte fra NCE-programmet. Prosjektledelsens rolle på vegne av Gjøvik Kunnskapspark ble tilsvarende modifisert: Fra å ha en samarbeidslogikk hvor fasilitatorfunksjonen bidro til å

løse konkrete problemstillinger ved å legge opp til samarbeid mellom relevante aktører, gikk man over til en samarbeidslogikk som var avhengig av å arbeide seg frem til problemstillinger som kunne fundere klyngens eksistens.

Byggingen av Security Valley som en byråkratisk nettverksmodell forutsatte et omfattende arbeid for å knytte til seg medlemmer og partnere for å skape et solid nok grunnlag for å søke om opptak i NCE-programmet. Siden denne etableringsfasen var såpass kostnadsintensiv, var det av stor viktighet å få på plass dette grunnlaget innen kort tid. Arbeidet med å innrullere aktører *utenfor* kjerneområdet ser imidlertid ut til å ha gått på bekostning av stabiliseringen i kjerneområdet. Som nevnt mistet man både Høgskolen i Gjøvik som aktiv partner, og flere av gründerbedriftenes engasjement som følge av fokuset på bred nettverksbygging utenfor kjerneområdet. Bathelt et al. (2004) viser til dette fenomenet som *hollow clusters*. Dette oppstår når etableringen av pipelines går på bekostning av å opprettholde den lokale buzzen, og det pulserende innovative klimaet. I videreføringen av dette kan man si at Security Valley viser at stabilisering av nettverk er avhengig av å oppnå en god balanse mellom å være en ekstrovert eller introvert klynge (Bathelt et al. 2004). I Security Valleys tilfelle vedrører dette spesielt balansen mellom produktfokus og nettverksaktiviteter. En for introvert utvikling av Security Valley ville ikke skaffet tilstrekkelig inntjening til videre drift av prosjektet. En for ekstrovert utvikling knyttet til destabilisering av aktørrelasjoner i kjerneområdet. Opprettholdelsen av denne balansen ble vanskeliggjort av at stabil finansiering måtte etableres på kun få år, noe som er å regne som svært kort til for etableringen av gode nettverk eller klynger. På bakgrunn av dette er det rimelig å hevde at Security Valley utviklet seg til å bli en “hul” klynge som følge av det ekstroverte fokuset på å bygge et rammeverk for samarbeid mellom informasjonssikkerhetsbedrifter, noe Castells (1996) ville kalt et “byråkrati”.

7.2 Påvirkningen av institusjonelle forhold på geografisk nærhet

Andersen (2006) konkluderer i sin studie av Bluelight med at det er mulig å fungere som nettverk og skape buzz uten samlokalisering. I følge forfatteren ligger bruken av IKT for samhandling og kunnskapsdeling som grunnleggende forutsetning for dette. Med grunnlag i Boschmas (2005) nærhetsdimensjoner skriver hun at Bluelights suksess som distribuert nettverk i det vesentlige skyldtes den kognitive nærheten mellom nøkkelpersoner i nettverket, som igjen bidro til en sosial nærhet. Å ha Arenaprogrammet som rammeverk for samarbeid bidro til institusjonell og organisatorisk nærhet (Andersen 2006).

Security Valley skiller seg en del fra Andersens konklusjon i Bluelight-studien. Security Valley ble startet opp fordi støtten via Arenaprogrammet falt bort, samtidig som det ikke fantes et sterkt nok grunnlag for videreføring som NCE. Siden prosjektet ikke utviklet seg innenfor et definert virkemiddelprogram er det rimelig å hevde at man ikke hadde den samme graden av formalisert institusjonell nærhet eller økonomisk stabilitet som Andersen (2006) beskriver i Bluelight. Boschma (2005) skriver at geografisk nærhet i klynger sannsynligvis er mindre viktig enn tidligere antatt, siden andre nærhetsdimensjoner kan være tilstrekkelig for at kunnskapsutveksling og læring skal finne sted, og at klyngen dermed “virker”. Geografisk nærhet kan imidlertid forsterke effektene av andre nærhetsdimensjoner (ibid.). Når det gjelder geografisk nærhet synes casestudiet av Security Valley å peke på en interessant distinksjon. Som nevnt i kapittel 5, så flere av informantene IKT-bruk mellom nettverksaktørene som tegn på at samarbeidet “virket”, og at det dermed var etablert en kognitiv, sosial og organisatorisk nærhet. Stabilisering som langsiktig mål kan kanskje være uavhengig av geografisk nærhet, særlig innenfor en institusjonalisert nærhetsdimensjon som Arena og NCE representerer, noe som også Andersen (2006) påpeker i sin studie av Bluelight. For Security Valley synes det imidlertid mer komplisert, siden man manglet den institusjonelle rammen av Arenaprogrammet. Veien mot stabilisering var dermed forbundet med større usikkerhet, slik at det kan synes som om sosial og organisatorisk nærhet vanskelig kunne knyttes mellom aktørene innenfor nettverket. Som drøftet i forrige avsnitt handler stabilisering i stor grad om å balansere introversjon og ekstroversjon. I Security Valleys tilfelle kan man anta at denne balansen hadde vært lettere å oppnå dersom det hadde vært større geografisk nærhet mellom flere av aktørene. På denne bakgrunnen er det rimelig å si at hvis man ikke har et rammeverk som sikrer institusjonell nærhet, vil behovet for geografisk nærhet for å oppnå stabilitet øke.

7.3 En stabiliserende triade: autokommunikasjon, consistency og sosial kapital

Relevansen i studiet av Security Valley som case ligger først og fremst i hvordan kunnskap hos deltakerne og berørte aktører kan gi innsikt i hvorfor aktørdynamikk, kommunikasjon og sosial kapital er viktig i stabiliseringen av innovasjonsnettverk. Med Johnstads (2004; 2009) ord bidrar dette til å åpne *black boxen* som sosial kapital ofte utgjør i næringsklynger. Det har vært spesielt interessant å studere dette innenfor rammen av innovasjonsnettverk og innovasjonsinfrastruktur som gjensidig støttende funksjoner innenfor klyngesatsningen.

Når det i denne studien snakkes om sosial kapital er dette knyttet til mesonivået, altså mellom bedrifter og organisasjoner i klyngen, eller direkte til tilliten og gjensidigheten mellom mennesker som arbeider i klyngens medlemsorganisasjoner. Begrepene bonding, bridging og linking (Halpern 2005, i Johnstad 2009; Bø og Schiefloe 2007) har vært spesielt nyttige i analysen av dynamikken mellom aktører innenfor Security Valley. Tillitsbyggingen, eller linkingen, mellom små og store aktører ser ut til å være en særdeles viktig for å stabilisere nettverket, noe som i Security Valleys tilfelle ser ut til å ha blitt forsterket på grunn av drivernodens parallelle og gjensidige satsning på innovasjonsnettverk og innovasjonsinfrastruktur. Likeledes avhenger bonding og bridging av en rekke faktorer som gunstige personeffekter, solid fotfeste i medlemsbedriftene og en felles forståelse rundt hva vi kalte “dualiteten i samarbeidet”. Castells’ (1996) begreper consistency og connectedness er brukt som teoretisk forståelsesramme gjennom store deler av analysen. Som beskrevet i teorikapittelet omhandler consistency samsvaret mellom aktørens interesser og nettverkets interesser, mens connectedness vedrører de strukturelle forholdene rundt kommunikasjonen i nettverk. Bevissthet rundt autokommunikasjon som kommunikasjonslogikk i nettverk er viktig for å forstå påvirkningen som utadrettet kommunikasjonsaktivitet har på klimaet innad i samarbeidet, og således bidra til felles forståelse rundt mål og interesser. Dette leder igjen til vektleggingen av at gode visjoner må funderes i konkrete målsetninger hos innrullerte aktører, fokus på gode produkter, aktuelle prosjekter og oppnådde delresultater. Et slikt fokus vil kunne skape koherens mellom eksternt og internt budskap, og fungere identitetsbyggende og styrke den sosiale kapital.

I kapittel 5 ble sammenhengen mellom autokommunikasjon, consistency og sosial kapital utforsket. Fra denne drøftingen er det rimelig å forstå sosial kapital som avhengig av oppfattelse om felles overordnet målsetning for aktørene i nettverket og nettverket i seg selv. Denne forståelsen ser ut til å kunne tilrettelegges av et bevisst forhold til autokommunikasjon som kommunikasjonslogikk i nettverksorganisasjoner. Spesielt i Security Valleys tilfelle synes nødvendigheten av en felles forståelse rundt prosjektets målsetning og utvikling å være forsterket av drivernodens parallelle satsning på innovasjonsnettverk og innovasjonsinfrastruktur som gjensidig støttende og delvis inkluderte funksjoner. Med teoretiske begreper kan dermed si at stabilisering av nettverk for innovasjon og samarbeid i stor grad ser ut til å være avhengig av hvordan produktfokus, konkrete aktørrelaterte behov og målsetninger, og delresultater innenfor prosjektet

synliggjøres gjennom en bevisst autokommunikasjonsstrategi for å styrke consistency og dermed sosial kapital.

7.4 Stabilisering av nettverk – teoretiske og politiske implikasjoner

Siden Security Valley var et initiativ som skulle løse den grunnleggende utfordringen ved å skape finansielt grunnlag for et klyngesamarbeid, ble det fokusert på å reise et selv bærende rammeverk for bedriftssamarbeid. Castells (1996) viser til slike nettverksorganiseringer som bureaucracies. Teoretisk argumenterer jeg for at byggingen av byråkratiske nettverksorganisasjoner i sterkere grad bør sees i sammenheng med faren for å bygge innholdsløse klynger. I Security Valley ser det til at man ville skape noe som lå frem i tid – altså *visjonen* om Security Valley – sterkere enn man ville opprettholde et innovativt klima som allerede fantes, og at man dermed skapte en innholdsløs klynge. Her må Castells' teori om nettverksorganisasjoner og Bathelt et al. (2004) sin teori om innovasjon og klyngeutvikling i skjæringspunktet mellom ekstroversjon og introversjon sees i sammenheng. En balanse mellom introversjon og ekstroversjon er viktig for å skape et gunstig klima for samarbeid og kunnskapsutvikling. For mye innadrettet aktivitet vil føre til lock-in, for mye utadrettet aktivitet i forbindelse med etableringen av en byråkratisk nettverksorganisasjon vil føre til en innholdsløs klynge. Denne teoretiske tilnærmingen må videre forstås i forhold til Boschmas (2005) nærhetsdimensjoner. Casestudien av Security Valley viser at balansen mellom introversjon og ekstroversjon i byråkratiske nettverksorganisasjoner er spesielt relevant i klyngeutviklingsprosesser utenfor den institusjonelle nærheten som virkemiddelapparatets klyngeutviklingsprogrammer gir. Jeg argumenterer for at mer geografisk nærhet vil kunne være gunstig for balansen mellom ekstroversjon og introversjon i klynger når institusjonell nærhet ikke er sikret gjennom tilknytning til virkemiddelprogrammer. Dette virker særlig viktig i byggingen av byråkratiske nettverksorganisasjoner, siden disse først og fremst ikke dreier seg om produktutvikling og salg, men om reproduksjon av virkemidler for samarbeid. I Security Valley ville dette kanskje bidratt til å holde på det innovative klimaet på tross av at innovasjonsnettverket var i en usikker fase gjennom å sikre den lokale buzzen.

Det siste hovedpoenget som studien av Security Valley belyser er at kommunikasjonen fra drivernoden i klynge- og nettverkssamarbeid bør tilrettelegges for å skape koherens mellom hva man ønsker å uttrykke eksternt, og hva man ønsker å uttrykke internt. På det teoretiske nivå argumenterer jeg for at autokommunikasjon og begrepsparet consistency og connectedness (Castells 1996) er i gjensidig påvirkningsforhold:

Connectedness gir rammeverket og infrastrukturen for (auto)kommunikasjon. Autokommunikasjon vil bidra til å skape consistency ved å bygge en felles forståelse rundt nettverkets interesser og aktørenes interesser. Denne felles forståelsen vil igjen tilrettelegge for sosial kapital ved å bidra til tillit, identitet og fellesskapsfølelse mellom aktørene.

Verken Bluelight eller Security Valley klarte å få på plass langsiktig finansieringsstøtte via NCE. Som påpekt i analysen kan dette sies å ha lagt en kraftig demper på aktiviteten rundt innovasjonsnettverk for informasjonssikkerhet med drivernode i Gjøvik Kunnskapspark, og i den videre betydning også rundt informasjonssikkerhet som satsningsområde innenfor det regionale innovasjonssystemet. Likevel står en del ting tilbake som suksesser etter nettverksaktiviteten på Gjøvik. Dette knytter seg først og fremst til utviklingen av Høgskolen i Gjøvik og NISlab som kompetansesenter på informasjonssikkerhetsforskning. NorSIS oppfattes også som en velrennomert og aktuell etat. NorSIS' ID-tyveriprojekt betegnes av mange som det mest positive som kom ut av Security Valley, og er stadig et aktuelt prosjekt innenfor fagområdet informasjonssikkerhet. Flere av aktørene innenfor Bluelight og Security Valley er også aktuelle i prosjektet IKT-Innlandet som ble lansert våren 2011. IKT-Innlandet har en liknende grunntanke om klyngeutvikling, og ønsker status som Arenaprogram i 2012²⁰.

Denne aktiviteten aktualiserer et spørsmål som det innenfor denne masteroppgavens fokus ikke har vært anledning til å drøfte mer inngående. Dette dreier seg om treffsikkerheten og langsiktigheten i Arenaprogrammet. Flere av informantene i denne studien har satt spørsmålstegn ved at virkemiddelapparatet velger å investere i klyngeprosjekter over en treårsperiode gjennom Arena, men at det ikke finnes noe ettervern for klyngene som trenger et videre fokusert arbeid over flere år for å bygge seg opp tilstrekkelig potensial for NCE. Relatert til dette har det også blitt reist spørsmål til treffsikkerheten til Arenaprogrammet. Argumentet er at programmet er velegnet for å samle et miljø eller en klynge som i praksis allerede eksisterer, men at programmet ikke tilrettelegger for å skape en *ny* klynge eller et *nytt* nettverk. Dette har vært opplevd som spesielt utfordrende i Gjøvik-området hvor man – som en informant formulerte det – “*begynner på minus-siden*” med tanke på den begrensede handelen, og så nært, men likevel fjernt fra det kompetanse- og næringsmessige sentrum i og rundt hovedstaden. Denne problemstillingen virker betimelig å ta opp i et politisk klima hvor regionalpolitikk og innovasjonspolitikkk inkluderes i hverandre.

²⁰ IKT-Innlandet, <http://www.ikt-innlandet.no/> (udatert, hentet 09.05.2011).

Litteraturliste

Andersen, Mette (2006) *Understanding the collaboration and the information flow in Bluelight – a distributed network*. Masteroppgave. Institutt for teknologi, innovasjon og kultur, Universitetet i Oslo

Andersen, Svein S. (1997) *Case-studier og generalisering – Forskningsstrategi og design*. Bergen: Fagbokforlaget

Bathelt, Harald, Anders Malmberg og Peter Maskell (2004) “Clusters and knowledge: local buzz, global pipelines and the process of knowledge creation” *Progress in human geography*. Vol. 28 (1): ss. 31-56

Bathelt, Harald og Mike Taylor (2002) “Clusters, power and place: inequality and local growth in time-space” *Geografiska annaler*. Vol. 84 B (2): ss. 93-109

Bell, David (2007) *Cyberculture theorists. Manuel Castells and Donna Harraway*. Abigdon, Oxon: Routledge

Bergum, Svein (2006) *Evauering av Bluelight. Nettverk for informasjonssikkerhet*. ØF-rapport nr. 20/2006. Lillehammer: Østlandsforskning

Bergum, Svein (2009) ”Informasjonssikkerhet i Innlandet: Fra dugnad til Security Valley”, i Johnstad, Tom og Atle Haugen, red. *Samhandling og innovasjon – aktører, systemer og initiativ i Innlandet*. Vallset: Oplandske Bokforlag, ss. 361-379

Bergum, Svein og Lene Nyhus (2004) *Bluelight: nettverk for informasjonssikkerhet – historien og kritiske suksessfaktorer*. ØF-rapport nr. 04/2004. Lillehammer: Østlandsforskning

Berker, Thomas (2010) ”Dealing with uncertainty in sustainable innovation: Mainstreaming and substitution” *International Journal of Innovation and Sustainable Development*. Vol. 5 (1): ss. 65-79

Boschma, Ron A. (2005) "Proximity and innovation: a critical assessment" *Regional studies*. Vol. 39 (1): ss. 61-74

Buckhanon, Kalisha (2009) "High impact networking" *Diversity MBA magazine*. Hentet 02.06.2011 fra http://diversitymbamagazine.com/wp-content/woo_custom/21-networking.jpg (Forsidebilde)

Bø, Inge og Per Morten Schiefloe (2007) *Sosiale landskap og sosial kapital. Innføring i nettverkstenkning*. Oslo: Universitetsforlaget

Castells, Manuel (1996) *The rise of the network society*. Oxford: Blackwell Publishers

Cheney, George og Lars Thøger Christensen (2001) "Organizational Identity: Linkages between internal and external communication", i Jablin, Fredric M. og Linda L. Putnam, eds. *The new Handbook of Organizational Communication. Advances in Theory, Research, and Methods*. London: Sage Publications, pp. 231-269

Coleman, James S. (1988) "Social capital in the creation of human capital" *American Journal of Sociology*. Vol. 94: pp. 95 -120

Cooley, Charles Horton (1902) *Human nature and social order*. New York: Charles Scribner's sons

Dahl, Michael S. og Christian Ø. R. Pedersen (2004) "Knowledge flows through informal contacts in industrial cluster: myth og reality?" *Research Policy*. 33 -2004: 1673-1686

Dey, Ian (2004) "Grounded theory", i Seale, Clive, Giampietro Gobo, Jaber F. Gubrium og David Silverman, red. *Qualitative research practice*. London: Sage Publications, ss. 80-93

Draft, Richard L., Robert H. Lengel og Linda Klebe Trevino (1987) "Message equivocality, media selection, and manager performance: Implications for information systems" *MIS Quarterly*. Vol. 11 (3): 355-366

Etzkowitz, Henry (2008) *The triple helix. University-industry-government innovation in action*. New York: Routledge

Flyvberg, Bent (2004) "Five misunderstandings about case-study research", i Seale, Clive, Giampietro Gobo, Jaber F. Gubrium og David Silverman, red. *Qualitative research practice*. London: Sage Publications, ss. 390-404

Fornyings- og administrasjonsdepartementet (2007) *Nasjonale retningslinjer for å styrke informasjonsikkerheten 2008-2010*. Oslo: Fornyings- og administrasjonsdepartementet, Justis- og politidepartementet, Forsvarsdepartementet og Samferdselsdepartementet

Gjøvik Kunnskapspark (2009) *Årsberetning 2009 Gjøvik Kunnskapspark as*. Tilgjengelig via Norsk Samfunnsvitenskapelig Datatjeneste, dimp.nsd.uib.no

Gjøvik Kunnskapspark (2008) *Årsberetning 2008 Gjøvik Kunnskapspark as*. Tilgjengelig via Norsk Samfunnsvitenskapelig Datatjeneste, dimp.nsd.uib.no

Gjøvik Kunnskapspark (udatert) *Gjøvik Kunnskapspark AS*. Hentet 28.02.2011 fra http://www.gkp.no/index.php?option=com_content&view=article&id=47&Itemid=1

Griffin, Siri Loretta (2006) *The rocky road to innovation. Casestudie av kommunikasjon i innovasjonsprosessen hos Numerical Rocks AS*. Masteroppgave. Institutt for sosiologi og statsvitenskap, NTNU

Halvorsen, Knut og Michel Lacave (1998) *Innovation systems in urban areas. A study of science parks and technopoles*. NIBR working paper 1998: 110. Oslo: NIBR

Halvorsen, Thomas (2001) *Science park policy – nurturing environment or artificial life support?* ISS-Rapport 2001: 59. Trondheim: NTNU

Hauge, Atle, Tom Johnstad og Morten Ørbeck (2009) "Innlandets innovasjonssystem og forskningsstrategi", i Johnstad, Tom og Atle Haugen, red. *Samhandling og innovasjon – aktører, systemer og initiativ i Innlandet*. Vallset: Oplandske Bokforlag, ss. 125-154

Hotz-Hart, Beat (2000) "Innovation Networks, Regions, and Globalization", i Clark, Gordon L., Maryann P. Feldman og Meric S. Gertler, red. *The Oxford handbook of economic geography*. Oxford: Oxford University Press, ss. 432-450

Idtyveri.info (udatert) *Prosjektbeskrivelse*. Hentet 18.02.2011 fra http://www.idtyveri.info/index.php?option=com_content&view=article&id=1:prosjektbeskrivelse&catid=1:om-oss&Itemid=2

IKT-Innlandet (2011) *IKT-Innlandet*. Hentet 09.05.2011 fra <http://www.ikt-innlandet.no/>

Innovasjon Norge (udatert) *Bluelight (avsluttet høsten 2005)*. Hentet 17.02.2011 fra http://ekstranett.innovasjon norge.no/templates/Page_Meta_57577.aspx

Innovasjon Norge (udatert) *Hva er Arena?* Hentet 17.02.2011 fra http://ekstranett.innovasjon norge.no/templates/Page_Meta_56170.aspx

Innovasjon Norge (udatert) *Om klynger*. Hentet 28.03.2011 fra http://ekstranett.innovasjon norge.no/templates/Page_Meta_56334.aspx

Innovasjon Norge, Norges Forskningsråd og SIVA (2010) *Håndbok for Arena-programmet 5. utgave*. Hentet 26.04.2011 fra http://ekstranett.innovasjon norge.no/Arena_fs/Arena%20Håndbok%205.%20utgave,%20oppdat.%2018.10.10.pdf

Johnstad, Tom (2009) "Innovasjon og samhandling – perspektiver på teorier", i Johnstad, Tom og Atle Haugen, red. *Samhandling og innovasjon – aktører, systemer og initiativ i Innlandet*. Vallset: Oplandske Bokforlag, ss. 59-92

Johnstad, Tom (2004) "Nettverk og klynger, partner- og lederskap", i Johnstad, Tom, red. *Klynger, nettverk og verdiskaping i Innlandet*. Oslo: NIBR, ss. 106-132

Kvale, Steinar (2001) *Det kvalitative forskningsintervju*. Oslo, Gyldendal Akademisk

Lotman, Yuri M. (1990) *Universe of the mind*. London: I.B. Tauris & Co

Lundvall, Bengt-Åke og Jesper Lindgaard Christensen (2004) "Introduction: Product innovation – on why and how it matters for firms and the economy", i Christensen, Jesper Lindgaard og Bengt-Åke Lundvall, red. *Product innovation, interactive learning and economic performance*. Oxford: Elsevier, ss. 1-18

Lyngholm, Wenche (2008) *Åpning av Security Valley*. Tale holdt under konferansen Sikker.info 08.04.2008, Gjøvik. Hentet 17.02.2011 fra http://www.regjeringen.no/mobil/nn/dep/fad/aktuelt/taler_og_artikler/av_ovrig_politisk_ledelse/statssekretaer_lyngholm/2008/apning-av-security-valley.html?id=507038

Macho-Stadler, Inés, David Pérez-Castrillo og Reinhilde Veugelers (2007) "Licensing of university inventions: The role of a technology transfer office" *International Journal of Industrial Organization*, 25 -2007: 483-510

Oppland Arbeiderblad (2010) *Kunnskapsparken er pengelens*. 23.11.2010, hentet 07.02.2011 fra <http://www.oa.no/arkiv/article5400111.ece>

Regjeringen.no (2008) *En halv million i støtte til Security Valley på Gjøvik*. Pressemelding, Fornyings- og administrasjonsdepartementet, hentet 27.02.2011 fra <http://www.regjeringen.no/nb/dep/fad/presSESenter/pressemeldinger/2008/en-halv-million-i-stotte-til-security-va.html?id=506882>

Reve, Torgeir og Erik W Jakobsen (2001) *Et verdiskapende Norge*. Oslo: Universitetsforlaget

Ringdal, Kristen (2007) *Enhet og Mangfold. Samfunnsvitenskapelig forskning og kvantitativ metode*. Bergen: Fagbokforlaget

Schot, Johan og Adri Albert de la Bruheze (2005) "The mediated design of products, consumption and consumers in the twentieth century", i Oudshoorn, Nelly og Trevor Pinch, eds. *How users matter – the co-construction of users and technology*. Cambridge, Mass., MIT-Press, pp. 229-245

Security Valley (2009) *Security Valley: Søknad om Norwegian Centre of Expertise*. Gjøvik Kunnskapspark, Gjøvik 27.02.2009

Security Valley (udatert) *Security Valley – en global merkevare for informasjonssikkerhet*. Hentet 27.02.2011 fra <http://www.securityvalley.no/index.php?limitstart=44>

Security Valley (udatert) *Saab AB skal hjelpe Security Valley til å bli et nasjonalt ekspertsenter*. Hentet 18.02.2011 fra http://www.securityvalley.no/index.php?option=com_content&view=article&id=75:saab-avtale&catid=35:forside&Itemid=104

SIVA (udatert) *Mer om kunnskapsparke*. Hentet 28.03.2011 fra [http://www.siva.no/internett/cms.nsf/\\$all/1266DB357E99C8B4C1257506005C884B](http://www.siva.no/internett/cms.nsf/$all/1266DB357E99C8B4C1257506005C884B)

Steinfeld, Charles, Ada Scupola og Carolina López-Nicolás (2010) “Social capital, ICT use and company performance: Findings from the Medicon Valley Biotech Cluster” *Technological forecasting & social change*. 77 -2010: ss. 1156-1166

Stortingsmelding nr. 25 (2004-2005) *Om regionalpolitikken*. Oslo: Kommunal- og regionaldepartementet

Sørensen, Knut H. (2005) “Jakten på innovasjon: Fra nasjonsbygging til dot.com”, i Frønes, Ivar og Lise Kjølrsrød, red. *Det norske samfunn*. Oslo: Gyldendal Akademiske: ss. 511-535

Thagaard, Tove (2003) *Systematikk og innlevelse. En innføring i kvalitativ metode*. Bergen, Fagbokforlaget

VRI-Innlandet (udatert) *VRI-Innlandet Kompetansemegling*. Hentet 06.05.2011 fra http://vri-innlandet.no/images/Kompetansemegling/090610%20vri-km_flyer.pdf

Våland, Terje I. (2004) ”Industrielle nettverk – innovasjon og kommersialisering” *Magma*. Årgang 7 (4)

Vedlegg 1.

Intervjuguide Bluelight og Security Valley

Innledning

Forskningsprosjektet omhandler kommunikasjon, innovasjon og kunnskapsdeling i kunnskapsnettverk. Dette er et intervju for å samle din erfaring om å arbeide innenfor et slikt nettverk, og hvilke egenskaper, fordeler og ulemper du føler i forhold til det. Jeg ønsker spesielt å innhente kunnskap om hvilken rolle kommunikasjon og IKT spiller for å stabilisere et slikt nettverk og bidra til innovasjon og næringsskapning.

Siteringer som fremkommer i forbindelse med rapporteringen av dette forskningsoppdraget kan presenteres i anonymisert form. Det er mulig å trekke seg når som helst. Jeg vil gjerne ta opp samtalen som lydfil. Er det OK?

Problemstilling

Hvordan kan en kunnskapspark stabilisere et nettverk for kunnskapsdeling og innovasjon. Hvilke kommunikasjonsstrategiske valg bør inngå i dette? Hvilken rolle spiller IKT i stabiliseringen av et nettverk for kunnskapsdeling og innovasjon?

Bedriftene og din rolle innenfor Bluelight

- Presenter din rolle i Bluelight og Security Valley
- Din opplevelse av Bluelight og Security Valley – hva fungerte, hva fungerte ikke?
- Hvilken motivasjon opplevde du for at deltakerne hadde for å bli med i nettverket?
 - *Behov for kompetanseutvikling i bedriften? I brasjen?*
 - *Kobling mot grunnforskning, FoU og fremtidig arbeidskraft ved HiG?*
 - *Hjelp til bedriftsetablering med mer.*
 - *Erfaringsutveksling, synergier vinn/vinn situasjoner.*

Hvordan hankses med usikkerhet

- I hvilken grad opplevde du usikkerhet i bedriftene i forbindelse med videreutviklingen av bedrifter og tjenester? (*Dette varierte sikkert mht. bedriftsstørrelse, og funksjon i nettverket, eks. produsent eller bruker.*)
- Hvordan bidro GKPs kompetanse innenfor næringsetablering til å redusere denne usikkerheten?
 - o Opplevde du at det var usikkerhet i forhold til hvordan GKP som drivernode i nettverket kunne redusere usikkerhetsmomentene?
- Hvordan gikk dere frem for å videreutvikle nettverkets tjenester og produkter? Hvor og hvordan startet initiativet for utvikling av produkter og tjenester?
 - *Her ønsker jeg å finne ut om innovasjonsprosessen sees på som lineær eller dynamisk.*
 - *Probe: Er kunnskap fra grunnforskning og FoU ved HiG den eneste viktige forutsetningen for innovasjon?*
 - *Probe: Kan utvikling og innovasjon best forstås som en dynamisk og multidimensjonal prosess, hvor både egne erfaringer, forskning og kundeetterspørsel spiller inn? Kommer du frem til et ferdig produkt, eller stabiliseres produktet på basis av kontinuerlig tilpasning til brukerkraft?*
- Er koblingen mot kunnskapsmiljøet på HiG og andre forskningsinstitusjoner noe som reduserer usikkerhet, eller er denne koblingen kun av ”formell” karakter for aktørene?
 - *Her kan jeg eventuelt spinne videre for å undersøke ”kunnskapshierarkiet”. Kan kunnskap fra HiG omsettes i praksis?*
- ”Mottakerkompetanse”. Hadde dere noen spesiell strategi som gikk på å forberede medlemsbedriftene til å ta inn og omsette kunnskap og arbeidsform i nettverk til sitt eget beste?
 - *Mottakerkompetanse: Om å organisere ressurser og kunnskap på en slik måte at en bedrift kan tilpasse seg nettverksarbeid og distribuert arbeid.*

- Hvor viktig er det å definere en konkret output av en utviklings- eller innovasjonsprosess? Kan man like gjerne se for seg noen overordnede målsetninger?
 - *Med overordnede målsetninger tenker jeg på for eksempel Bluelights formulering av "hovedmålsetninger" 2006:*
 - 1) *Fremstille og realisere samarbeidsprosjekter*
 - 2) *Etablere og vedlikeholde arenaer for aktiv nettverksbygging*
 - 3) *Øke troverdigheten for de tilknyttede aktører*
 - 4) *Legge til rette for at aktørene an øke sin faglige kompetanse*

- Jeg har oppfattet at noe av utfordringen i Bluelight – og som også har vært vedvarende i Security Valley – er usikkerhet rundt nettopp hva som kommer ut av et samarbeid. Kan du si noe om hvordan man brukte kommersialiseringsprosessen via Security Partner for å hankses med denne usikkerheten?

Kommunikasjon, kunnskapsdeling og innovasjon

- Hva vil du si er de viktigste kildene til innovasjon? Og hvilke typer aktører mener du bør representeres innefor et kunnskapsmiljø?
 - *Probe: Forskningsinstitusjoner, FoU-institutter, brukere/kunder, produsenter, utviklere, leverandører.*
- Bluelight inkluderte aktører fra ulike næringer, og med ulike behov og interesser knyttet til informasjonssikkerhet. Lå konkrete behov og utfordringer hos brukere med hensyn til informasjonssikkerhet til grunn for de tjenestene og produktene som kom ut av Bluelight?
 - *I litteraturen snakker man om lead users og mediators, det jeg lurer på er hvilke strategier som lå til grunn for å trekke enn meninger og behov fra disse.*

- ØF-rapporten *Evaluering av Bluelight* peker på at behov hos brukere og næringsliv generelt burde legges sterkere til grunn for utviklingen av produkter, tjenester og prosjekter i Bluelight. Var dette noe som Security Valley klarte å løse?
- I ØF-rapporten *Evaluering av Bluelight* snakker Svein Bergum om at det tyder på at det har vært en overflod av kompetanse på informasjonssikkerhet, men underskudd på prosesskompetanse og forretningsmessig kompetanse. Kan du kommentere det?
- Kjenner du til begrepet *kompetansemegling* slik det benyttes i VRI-prosjektet? Hvordan svarer begrepet kompetansemegling til GKPs rolle i Bluelight og Security Valley?
- Hvordan foregikk den eksternt rettede kommunikasjonen i Bluelight og Security Valley (altså mot eksterne kompetansemiljøer, brukergrupper, kunder, osv.)?
 - o Med tanke på relasjonsbygging?
 - o Markedsføring av produktene, tjenestene og kompetansen i nettverket?
 - *ØF-rapporten sier at Bluelight ikke hadde noen strategi på dette, og overlot det til enkeltbedriftene i projisere Bluelight til sine kontakter i næringslivet.*
- Hvordan opplevde du den interne kommunikasjonen i Bluelight og Security Valley (altså mellom medlemmer, partnere, ledelse, støttespillere, osv.)?
 - *Klar og direkte?*
 - *Endret gjennom flere ledd?*
 - *Siktet mot å skape fellesskapsfølelse/organisasjonskultur (videre: autokommunikasjon).*
- Gjennom hvilke media ble det kommunisert? Ansikt-til-ansikt? Ulike kommunikasjonskanaler for ulike formål? Ulik type kommunikasjon i ulike faser?
- Var noe av kommunikasjonen spesifikt rettet mot å skape mottakerkompetanse, og drive kompetansemegling? Hvordan foregikk dette?

- Brukte dere ulike IKT-løsninger til å skape forhandlingsarenaer hvor brukerbehov ble fremsatt, og løsninger ble foreslått? La dette til rette for en kontinuerlig kommunikasjon slik at tjenesten/produktet ble tilpasset behov?
- Tror du at kommunikasjon, kunnskapsdeling og dermed bedriftsutvikling og innovasjon kan understøttes av IKT-løsninger hvor nyheter i nettverket, relevant fagstoff og brukerbehov fra næringsliv kan deles og diskuteres?
 - *For eksempel Microsoft Share Point, Wiki, "lederblogg" etc.*
- I hvilken grad så du behovet for å videreutvikle lærings- og kommunikasjonsprosesser mellom FoU, næringsliv, kunder osv.? Kan du i dag se for deg at dette kan skje i en kombinasjon av fysiske og nettbaserte møteplasser?
- Hvordan gikk dere frem for å skape tillit mellom aktørene i nettverket?
 - *Her vil det kunne være naturlig å pense inn på uformell kommunikasjon.*
- Var det en fellesskapsfølelse innenfor nettverket? Dvs. en slags utvidet organisasjonskultur?
 - Opplevde du tillit mellom bedriftene tilknyttet kunnskapsnettverket?
 - *Dette går på bonding (sammensveising), bridging (brobygging) og linking. Probe.*
 - *Ville fellesskapsfølelse/organisasjonskultur kunne opprettholdes med ledeblogg, medierte forhandlingsarenaer med mer?*
- VS 2010 skrev i 2003 kronikker i HA, GD, OA og Kommunal Rapport. Disse hadde i følge ØF mye å si for intern- og eksternt markedsføring og fellesskapsfølelse i nettverket. Ble denne type arbeid opprettholdt også i Security Valley?
 - Hvorfor ikke? Liten verdi? Kostnad – nytte?
- Kan du definere kunnskap?
- Er det noe du ønsker å tilføye?

Takk for intervjuet.

Vedlegg 2.

Samtykkeerklæring for intervju i forbindelse med masteroppgave.

Intervjuet inngår som datagrunnlag i min masteroppgave i medier, kommunikasjon og IT ved NTNU. Temaet for oppgaven er kommunikasjon og innovasjon innenfor kunnskapsnettverk. Jeg er interessert i å finne ut hvordan kommunikasjon og koblinger mellom noder/aktører i et nettverk tilrettelegges for å fremme kunnskapsdeling, tillit, innovasjon og bedriftsutvikling. Oppgaven skrives i samarbeid med Gjøvik Kunnskapspark.

Datagrunnlaget omfatter 10 – 20 informanter fra kunnskapspark, inkubatorbedrifter, høyskoler og andre bedrifter tilknyttet kunnskapsnettverk. Dette suppleres eventuelt av statistiske analyser og/eller dokumentstudier. Spørsmålene vil i hovedsak dreie seg om informantenes erfaring om arbeid innenfor kunnskapsnettverk, og gå spesielt inn på usikkerhet i innovasjon og bedriftsutvikling, tillit og kommunikasjon mellom noder i nettverket.

Jeg vil bruke båndopptaker og ta notater mens vi snakker sammen. Intervjuet vil ta mellom 30 minutter og en time. Det er frivillig å være med og du har mulighet til å trekke deg når som helst underveis, uten å måtte begrunne dette nærmere. Dersom du trekker deg vil alle innsamlede data om deg bli anonymisert. Data fra intervjuene behandles konfidensielt, og siteringer i den ferdige teksten anonymiseres. Opptaket fra intervjuet slettes etter avlagt eksamen sommeren 2011.

Min kontaktinformasjon:

Frede A. Stenslie
[telefonnummer]
[e-postadresse]

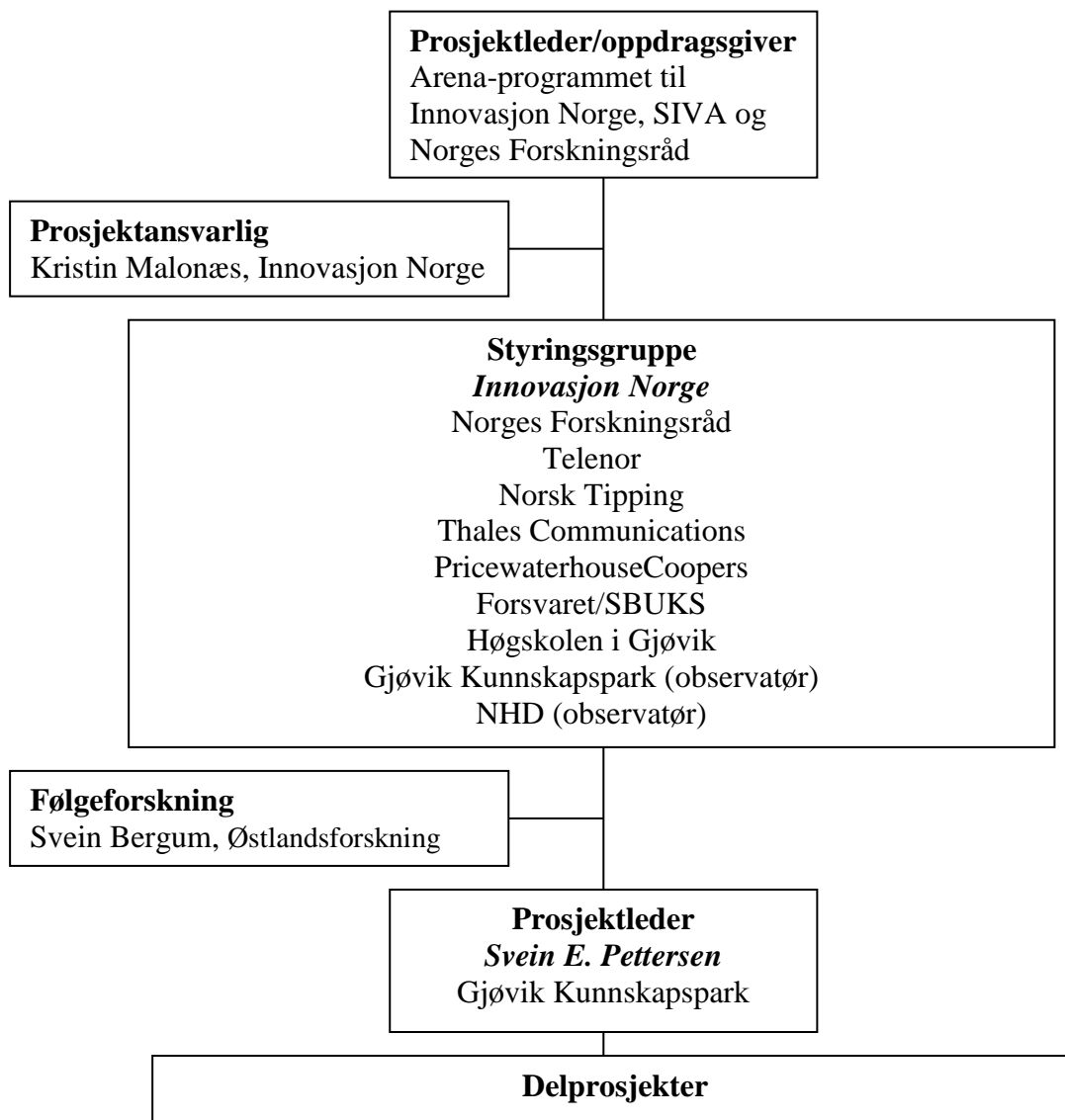
Min veileder ved Institutt for Sosiologi og Statsvitenskap ved NTNU:
Førsteamanuensis Hendrik Storstein Spilker
[e-postadresse]

Samtykkeerklæring:

Jeg har mottatt informasjon om studien og ønsker å stille til intervju.

Signatur

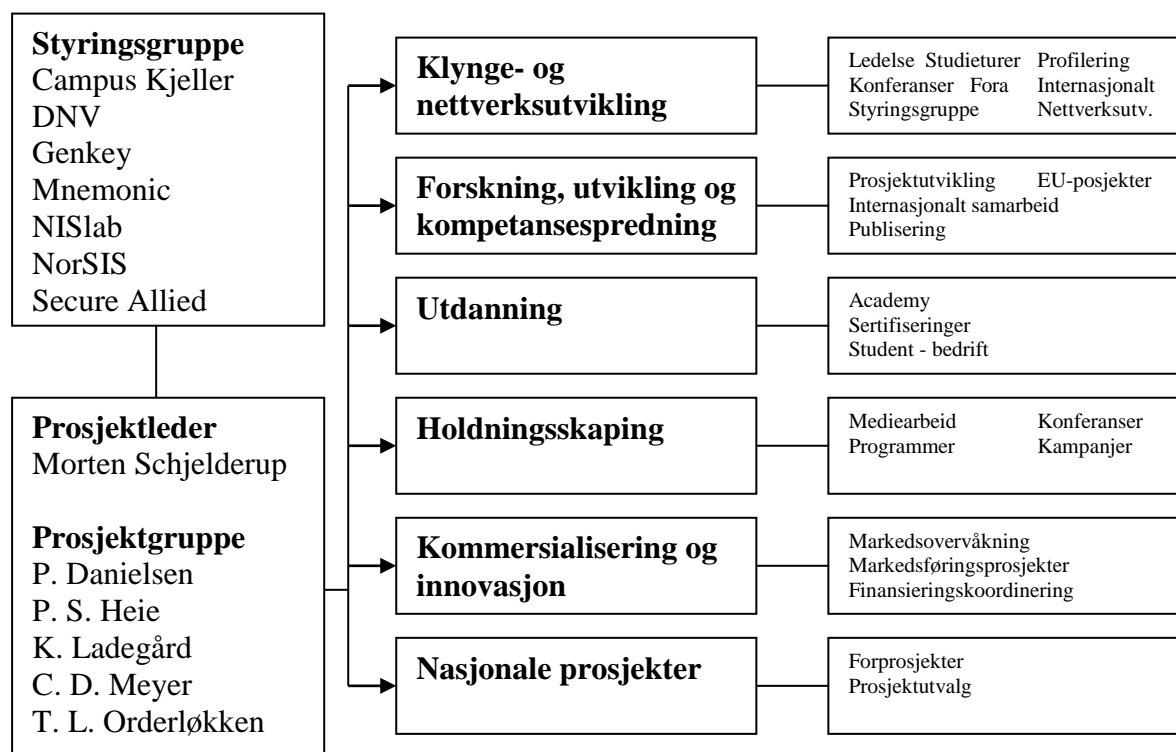
Vedlegg 3: Organisasjonskart for Bluelight



Organisering av Bluelight. Organiseringskart basert på fremstilling i Bergum og Nyhus 2004: 14.

Vedlegg 4.

Organisasjonskart og medlemsoversikt for Security Valley:



Organisasjonskart for Security Valley 2009, basert på fremstilling i Søknad om NCE (Security Valley 2009:14).

Medlemmer og støttespillere i Security Valley:

Kjernebedrifter:

Campus Kjeller	Idex	NISlab
Det norske veritas	Mnemonic	Secure Allied
Genkey	NorSIS	

Medlemmer, inkludert prosjektdeltakere:

Apropos Internett	Afinion International	Brønnøysundregistrene
Datatilsynet	Data-Secure	DnB NOR
Dun & Bradstreet	Experian	Finansnæringens Hovedorg.
Fokus Bank	Forbrukerombudet	Handels og Servicenæringens HO
Hjelp Forsikring	ITAKT (Internett og telebransjen)	ITS Norway
KRIPOS	Lindorff	Nammo
NAV	NorTIB	Oberthur
Politidirektoratet	Post og Teletilsynet	Posten Norge
Powertech	PricewaterhouseCoopers (PwC)	Skandiabanken

Skattedirektoratet inkl. Folkereg.	Sparebankforeningen	Telenor
Universitetet i Oslo, AFIN	Veolia Miljø - Sikkerhetsservice	Watchcom
	Økokrim	

Støttespillere:

Fornyings- og adm. departementet	Justis- og politidepartementet	IBM Norge AS
Nødnett	Universitetet i Agder	Polititets data og materieltjeneste
IKT-Norge	Abelia	Næringslivets Sikkerhetsråd
Forsvaret Jørstadmoen, KKIS	Forsvarets Sikkerhetstjeneste	Næringslivets Hovedorganisasjon
Næringsrådet i Gjøvikregionen	Fylkesmannen i Oppland	Fylkesmannen i Hedmark
Oppland Fylkeskommune	Gjøvik kommune	Østre Toten kommune
Vestre Toten kommune	Søndre Land kommune	Nordre Land kommune

Inkubatorbedrifter:

portAHEAD	Innocrowd	Retoma
SecCon	Stealth Scientific	IntelliStick
SFAS Security	Kontroller.net	Transmatch
Netc@rds	Motion Recording	ETC
JusMed	XpoMedia	ShootandWin
Det var en gang	OPAX (Campus Kjeller)	Lenco Systems (Campus Kjeller)
Odin Aero (Campus Kjeller)	Electric Sensors (TTO pipeline)	Airport Logistics (pipeline)

Tabellene er basert på fremstilling i Søknad om NCE (Security Valley 2009: 2 – 3) og securityvalley.no.