UiO : Senter for teknologi, innovasjon og kultur
Det samfunnsvitenskapelige fakultet

Kappløpet i cyberspace

En komparativ casestudie av fire innovasjoner drevet frem av internettkriminalitet

Emilie Roxanne W. Colle

Masteroppgave ved senter for teknologi, innovasjon og kultur

UNIVERSITETET I OSLO

Vår 2013

Antall ord: 33 402

Bildet på forsiden er lånt fra en artikkel på TechNews (technewspedia.com) i artikkelen *U.S. Air Force wants to improve its ability to "attack in cyberspace"* skrevet av James Edward 31.august 2012. Sist sett 19.mars 2013: http://technewspedia.com/u-s-air-force-wants-to-improve-its-ability-to-attacks-in-cyberspace/

Kappløpet i cyberspace

En komparativ casestudie av fire innovasjoner drevet frem av internettkriminalitet

2013

Kappløpet i cyberspace

Emilie Roxanne W. Colle

http://www.duo.uio.no/

Trykk: Reprosentralen, Universitetet i Oslo

Sammendrag

Er det ikke interessant å tenke på at vi, både brukere og produsenter, er med på å forme og påvirke videre utvikling og innovasjon? At også kriminelle er brukere, som innoverer og er med på å drive frem denne utviklingen? At teknologien vi skaper for å løse ett problem, kan løse et annet og gi nye muligheter, og at dette igjen skaper nye trusler og behov, som igjen kan medføre muligheter for noen andre? Og at denne dynamikken mellom kriminelle og ikke-kriminelles innovasjoner ligner et kappløp?

Internett har gitt muligheter for den kriminelle verden, så vel som i den ikke-kriminelle verdenen. De kriminelles muligheter utgjør en trussel mot de ikke-kriminelle, som dermed må forsøke å finne måter å beskytte seg. Datakriminalitet, som i mange tilfeller er internettkriminalitet, er grovt estimert til å koste det norske samfunn opp mot 20 milliarder kroner årlig. Disse truslene skaper behov som kan anses som enten en markedsmulighet eller imøtekommes med andre typer tiltak uten ønsker om finansielle gevinster.

Denne oppgaven er en kvalitativ komparativ casestudie som omhandler hvordan internettkriminalitet har vært en pådriver for innovasjoner i fire ulike ikke-kriminelle norske organisasjoner. Den ene er en produktinnovasjon fra et datasikkerhetsfirma, den andre en paradigmeinnovasjon i en bank, den tredje en metodeinnovasjon hos en politiorganisasjon og den fjerde er en frivillig, ikke-profittorganisasjon, som jobber mot kriminelle og ondsinnede handlinger på nett, og hvor organisasjonen utgjør en innovasjon i seg selv. Jeg presenterer en modell og begrepet *kontrainnovasjon*, som omhandler hvordan de kriminelles og ikke-kriminelles innovasjoner tvinger hverandre til å kontrainnovere for å imøtekomme de nye truslene og behovene som motparten skaper.

Internettkriminalitet kan være en påvirkende årsak til innovasjon i ikke-kriminelle organisasjoner. Internettkriminalitet skaper ulike behov for samfunnet og for organisasjoner. Konsekvensen av dette er at organisasjoner må prøve å tilpasse seg miljøet og omgivelsene som er endret som følge av endring i kriminalitetsbildet, og disse endringene vil i mange tilfeller kunne tolkes som innovasjon, og mer presist kontrainnovasjon. Casene illustrerer ulike former for kontrainnovasjoner, blant annet som følge av at de er ulike typer organisasjoner som på ulike måter påvirkes av internettkriminalitet. Én av

kontrainnovasjonene er en produsentinnovasjon, og er en respons på potensielle kunders behov som følge av internettkriminalitet. Denne innovasjonen gir hovedsakelig en bedriftsøkonomisk gevinst, og er en konsekvens av markedsmuligheten som er oppstått som følge av internettkriminalitet. Tre av kontrainnovasjonene kan grovt kategoriseres som brukerinnovasjoner. Disse innovasjonene har ikke privat- eller bedriftsøkonomisk gevinst som hovedmål, men gir hovedsakelig en samfunnsøkonomisk- eller velferdsgevinst. To av innovasjonene er mer knyttet til et indirekte behov i organisasjonene, mens den tredje er en ikke-profitt organisasjon hvor behovet ligger hos internettbrukere generelt.

Oppgaven illustrerer en kobling mellom innovasjon og kriminalitet, hvor internettkriminalitet fungerer som en pådriver for innovasjonene i ikke-kriminelle organisasjoner som på en eller annen måte blir berørt av internettkriminalitet og dennes utvikling. De er i samutvikling med teknologi og kriminalitet. Både omgivelser og aktører påvirker hverandre og driver hverandre fremover gjennom blant annet ulike typer innovasjon. Fordi kriminalitet er en uønsket pådriver, men en pådriver som realistisk ikke kan fjernes helt, vil alle kontrainnovasjoner bare være forsøk på en midlertidig utligning. På denne måten driver de frem teknologisk og generell utvikling i et slags kappløp.

Forord

Det har vært utfordrende å studere noe som ikke er særlig studert tidligere ut fra en innovasjonstilnærming, og hvor passede teoretiske rammeverk ennå ikke eksisterer. Men dette har allikevel motivert meg i den grad at jeg synes det er desto viktigere at jeg får frem oppgavens poenger. For selv om det er et lite studert område, betyr det ikke at det bør forbli slik. Man må i blant tørre å ta sjanser, og tørre å gjøre ting på en litt annen måte enn tidligere. Er ikke det essensen i innovasjon?

Arbeidet med denne oppgaven har som nevnt vært utfordrende. Emnet var for sensitivt for mange, så å innhente informanter ble en større utfordring enn først antatt. Derfor må jeg få gi en kjempestor takk til alle informantene mine: Mari Grini, Kristine Beitland, Anders Hardangen, Rune Fløisbonn, Bjørn Lilleeng og Eldar Lillevik, som med entusiasme bidro til og muliggjorde denne oppgaven. Jeg håper at vi alle på hver våre kanter kan være pådrivere for kontrainnovasjon i årene som kommer. Deres entusiasme har vært en svært viktig motivasjonsfaktor i dette arbeidet.

En stor takk til min hovedveileder Helge Godø, med sin positive og entusiastiske holdning, min biveileder Magnus Gulbrandsen og min samboer Bernt Revheim. Takk for all støtte og gode råd.

Det er tre skjønne kvinner og medstudenter som også har utgjort en fantastisk støtte. Marianne Austheim, Olga Furdman og Kristine Czynski. Tusen takk for alle samtaler og diskusjoner gjennom dette siste studieåret.

Emilie Roxanne W. Colle
Oslo, mai 2013

Innholdsfortegnelse

1.0 Introduksjon 1
1.1 Kriminalitet og innovasjon i litteraturen 1
1.2 Innovasjon 2
1.3 Internett 2
1.4 Internettkriminalitet 3
1.5 Teknologiutvikling + kriminalitet = innovasjon 4
1.6 Motivasjon 5
1.7 Nytten av oppgaven 5
1.8 Problemstilling og forskningsspørsmål 6
1.8.1 Formål 7
1.8.2 Begrensninger 7
1.9 Oppgavens struktur og oppbygning 9

2.0 Sentral litteratur og sentrale begreper innen internettkriminalitet 11
2.1 Kyberkriminalitet 11
2.2 Internett og informasjonssamfunnet 12
2.3 Tre generasjoner kyberkriminalitet 13
2.4 Klassifisering av kyberkriminalitet 13
2.4.1 Dataintegritetskriminalitet 14
2.4.2 Dataassistert kriminalitet 15
2.4.3 Datainnholdskriminalitet 15
2.5 Motivasjonsfaktorer for å begå internettkriminalitet 16
2.6 Oppsummering 16

3.0 Sentral litteratur og sentrale begreper innen innovasjon 17
3.1 Overordnet tilnærming 17
3.2 Hva er innovasjon? 18
3.3 De fire P'er i innovasjonsrommet 19
3.4 Kildene til innovasjon: behov, nytte og gevinst 20
3.4.1 Kunnskapsdytt og behovstrekk 20
3.4.2 Det funksjonelle innovasjonsforholdet 21
3.4.3 Innovasjonsgevinst 24
3.5 Oppsummering 25

4.0 Forskningsmetode 26
4.1 Datagrunnlag 26
4.1.1 Valg av case 26
4.1.2 Valg av informanter 27
4.1.3 Dybdeintervju 29
4.1.4 Intervjusituasjon 30
4.2 Koding og analyse av datamateriell 31
4.3 Validitet og reliabilitet 32
4.3.1 Validitet 32
4.3.2 Reliabilitet 34
4.4 Etiske refleksjoner 35
4.5 Oppsummering 36

5.0 Caseanalyser 37

5.1 Case 1: Produktinnovasjon 39
5.1.1 Norman 39
5.1.2 Norman Network Protection 40
5.1.3 Norman SCADA Protection 40
5.1.4 Mulighet i andres behov 42
5.1.5 Innovasjonstype 42
5.2 Case 2: Paradigmeinnovasjon 45
5.2.1 SpareBank 1 og åpenhet 45
5.2.2 Nettvettkampanjen 45
5.2.3 Paradigmeskiftet 46
5.2.4 Innovasjonstype 48
5.3 Case 3: Metodeinnovasjon 51
5.3.1. Kripos 51
5.3.2 Generell innovasjon i Kripos 52
5.3.3 Programvareinnovasjon 53
5.3.4 Økt innovasjonsbehov 54
5.3.5 Innovasjonstype 54
5.4 Case 4: Ikke-profitt organisasjoninnovasjon 57
5.4.1 Grunnleggelsen av Underworld 57
5.4.2 Trusselbildet på Internett og Underworld 58
5.4.3 Informasjonsdeling 59
5.4.4 Ikke profitt, kun frivillighetsarbeid 60
5.4.5 Innovasjonstype 61
5.5 Oppsummering og resultat fra caseanalyser 64

6.0 Drøfting: Internettkriminalitet som pådriver for innovasjon? 67
6.1 Teknologisk utvikling og internettkriminalitet 67
6.1.1 Internettkriminalitetsutviklingen de senere årene 68
6.1.2 IKT-kunnskapsnivå blant kriminelle 69
6.2 Ikke-kriminelle innovasjoner og internettkriminalitet 70
6.2.1 Kriminalitet som skaper av behov 71
6.2.2 Innovasjonsnytte 71
6.2.3 Nødvendighet og mulighet – bruker og produsent 73
6.2.4 Endring, tilpasning og organisasjonsutvikling 74
6.2.5 Innovasjonsnytte og gevinst for organisasjoner 75
6.3 Kontrainnovasjon 76
6.4 Kappløpet i kyberrommet 79
6.5 Oppsummering 81

7.0 Konklusjon 82
7.1 Implikasjoner og forslag til videre forskning 84
7.2 Avslutning 85

8.0 Litteraturliste 87

Vedlegg 95

Figurliste

1.1 *Innovasjon-kontrainnovasjon*……..……**7**
5.1 *Caser i innovasjonsrommet*……64
5.2 *Cyberkriminalitet-, innovatør- og gevinstkategorisering*……..65
6.1 *Kontrainnovasjonsmodell for IK-drevet innovasjonskappløp*……..……78

1.0 Introduksjon

Hver dag skjer det dataangrep på norske organisasjoner, utnyttelser av programsårbarheter, tjenestenektangrep og spredning av virus og trojanere. Samtidig spres det barnepornografiske bilder og svindelmail, og hackere henter ut sensitiv og gradert informasjon for å nevne noe. Trenden ser ut til å øke, og dette tyder på at internettkriminalitet (IK) er et omfattende problem. Konsekvensen av dette omfattende problemet er et økende behov for ulike organisasjoner til å tilpasse seg trusselen og de nye typene IK. Dette kan medføre behov for endring og ulike innovasjoner i mange ulike typer organisasjoner.

I denne oppgaven vil du lese om hvordan IK kan være en medvirkende årsak til innovasjon i helt forskjellige ikke-kriminelle organisasjoner. At det er en medvirkende årsak, gjør at de kan oppfattes som en form for pådriver for disse innovasjonene. Jeg presenterer dette i form av fire caser, som illustrerer ulike innovasjoner i ulike organisasjoner, alle innovasjonene delvis drevet frem av IK.

1.1 Kriminalitet og innovasjon i litteraturen

Det er svært begrenset litteratur om kriminalitet som en pådriver for innovasjon. Dette gjør denne oppgaven sjelden i sitt slag, og vil forhåpentligvis bidra med kunnskap og empiri som gir en forståelse av hvordan IK kan påvirke ikke-kriminelle innovasjoner. Dette er relevant for å få en forståelse av hvordan ulike aktører påvirker hverandre og omgivelsene, og derav former samfunnsutviklingen samt økonomisk og teknologisk utvikling. Den faglige relevansen ligger i at man inkluderer en understudert aktør i innovasjonsutviklingen, som både alene men også gjennom andre driver frem innovasjon.

Det er etter det jeg har funnet kun noen svært få, Stephen Flowers (2007, 2008), og Celine Schulz og Stefan Wagner (2010), som har sett på fenomenet IK på en lignende måte som jeg gjør i denne oppgaven. En pådriver kan innenfor innovasjon omtales som en *endringsagent* (change agent) (Rogers 1983). Dette er en person som påvirker diffusjon av innovasjon, enten for å få fortgang i, eller for å sinke innovasjonsspredningen (Rogers 1983, 28, 312). Som helhet kan man si det er individer som i den kriminelle verden innoverer (outlaw innovation) (Flowers 2007, 2008), sprer (endringsagent) (Rogers 1983, 312) og bruker (outlaw users) (Schulz og Wagner 2010) kriminelle innovasjoner, og på denne måten har de gjort fenomenet IK som helhet til en trussel som krever mottiltak.

Mye av den utvikling som har funnet sted innenfor sikkerhet, teknologi og utbygging av samfunnsstruktur, infrastruktur og bygningsutvikling har vært påvirket av den trusselen kriminalitet utgjør. Trusselen fra krig og kriminalitet har vært to pådrivere for mye av utformingene i hele verden. Internett, mye av romfartsteknologien og atombomben er eksempler på innovasjoner som ble utviklet som følge av militær forskning og utvikling, på grunn av trusselen fra krig og fiender. Hadde man hatt en lovbok, et fengsel, en politiorganisasjon, Securitas, vindusgittere og kommersielt innbruddsalarmutstyr hvis det ikke var for kriminalitet? Dette er innovasjoner som er blitt drevet frem av kriminalitet og formet samfunnet, formet for eksempel rettsstaten.

1.2 Innovasjon

Innovasjoner handler ofte om å sette sammen kjente ting på nye måter, men i slike kombinasjoner kan det også inngå elementer som er helt nye (Schumpeter [1934] 1983, 132; van de Ven og Angle 2000, 12). Innovasjon trenger ikke å være ny for alle og enhver, men må oppleves som ny for de som adopterer den (Rogers 1983, 11; van de Ven og Angle 2000, 12). Innovasjon er et fenomen som ikke bare representerer tiltak for å øke konkurransedyktighet og øke markedsandeler for organisasjoner. Innovasjon kan også være endrings- og tilpasningstiltak i forhold til ulike faktorer som påvirker det miljø en organisasjon opererer i. Ut fra denne forståelsen vil innovasjon kunne være tiltak og strategier hos organisasjoner for å beskytte og tilpasse seg ulike aspekter ved IK. Både muligheter og behov kan oppstå som følge av IK, og ulike perspektiver, strategier, organisasjonsoppgaver og mål kan påvirke hva slags tilpassinger som blir iverksatt. Disse tilpassingene til miljøet og tiltakene kan være innovasjoner.

1.3 Internett

Internettets utvikling begynte allerede på 1960-tallet, og ble en del av et forskningsprogram i det amerikanske forsvaret i en avdeling kalt ARPA (Advanced Research Projects Agency) (Hafner og Lyon 1996, 11-42). I tiårene som fulgte, var det flere vitenskapelige teorier og ideer og tekniske innovasjoner som medvirket til at Internettet ble til den åpne virtuelle infrastrukturen det er i dag. Blant disse var ideen om pakkesvitsjing, først introdusert av Paul Baran og Donald Davis (ibid., 52-67). I tillegg til teknologiene som er integrert i infrastrukturen til Internett, er det innovasjoner innen informasjonsteknologier som datamaskiner, mobiltelefoner og nettbrett, som har gjort at brukersnittet til Internett har utviklet seg og blitt allemannseie. I dag er det trolig ikke en eneste organisasjon i Norge som

ikke har noen form for kontakt med Internett og nettverkstilkoblede teknologier. Ettersom produktutviklingen innenfor informasjons- og kommunikasjonsteknologi (IKT) forsetter i dagens innovasjonstakt, vil internettavhengigheten etter all sannsynlighet bare øke i årene fremover, i tillegg til at antall mennesker og gjenstander i verden som får internettilgang øker. Datamaskiner og Internett er to av de mest anvendte teknologiene i dag (Stefoff 2009, 16).

Internett har gitt uante muligheter de siste årene, som for 20 år siden ville være utenkelige. I dag har man hele bedrifter som er tuftet på nettverksteknologien, kundeinteraksjon foregår over nettet, og intern og ekstern kommunikasjon hos organisasjoner foregår over nett. Organisasjoner bruker Internett til blant annet chat, e-post, bestillingssystemer, betalingssystemer, datalagring, videooverføring, videokonferansesystemer, reklame, hjemmesider, sosiale medier og kundekommunikasjon for å nevne noe. Men Internett gir ikke bare muligheter for ikke-kriminelle organisasjoner. Etter hvert som største delen av den vestlige verdensbefolkningen er på Internett, har dette medført uante muligheter for kriminelle.

1.4 Internettkriminalitet

Kriminaliteten på Internett har de siste årene steget drastisk, og NorCERT[1] har estimert at kostnader forbundet med datakriminalitet, hvor IK utgjør en stor del, ligger på ca. 20 milliarder NOK i året (NorCERT 2011, 19; NorCERT 2012, 21; NSR 2012, 19). Det skal påpekes at dette tallet kun er et estimat nedskalert i forhold til Norges innbyggertall etter britiske kostnader i forbindelse med datakriminalitet i undersøkelsen *The Cost of Cybercrime* utført av Detica og Office of Cyber Security and Information Assurance i UK Cabinet Office (NorCERT 2011, 19; NorCERT 2012, 21; NSR 2012, 19). De kriminelle bruker Internett som et verktøy eller hjelpemiddel til å utføre tradisjonell kriminalitet, som for eksempel svindelbrev, som i dag kan sendes over e-post i stedet for per post, eller til salg og kjøp av våpen og narkotiske stoffer. Men det har også gitt muligheter til nye former for kriminalitet, som baserer seg på internetteknologien. Trolig er de to største paradigmeskiftene i forhold til kriminalitet i kombinasjon med Internett at *informasjonen* på Internett er blitt en viktig *verdikilde,* og at det er *grenseløst.*

[1] **NorCERT** står for Norwegian Computer Emergency Response Team, og er det nasjonale senteret i Norge, som overvåker, forebygger og håndterer alvorlig dataangrep rettet mot norsk samfunnskritisk infrastruktur og informasjon (NorCERT 1; NorCERT 2). Samt at de drifter et nasjonalt sensornettverk på Internett, og varsler om truser og sårbarheter (NorCERT 1; NorCERT 2).

En slik utvikling påvirker det samfunnet vi lever i, og det miljøet og omgivelsene organisasjoner opererer i. For å kunne overleve i et slikt miljø gjelder det, (og vil gjelde i større og større grad, etter hvert som IK øker), å være bevisst rundt disse forholdene og tilpasse seg trusselutviklingen. Dette gjennom tiltak i form av mottiltak som respons på den aktuelle trusselen og hendelsene forårsaket av IK. Disse tilpasningene og mottiltakene vil i noen tilfeller kunne være ulike former for innovasjon.

I tillegg rammer IK ulike organisasjoner på ulike måter, noe som kan medføre at ikke-kriminelle organisasjoner innoverer ulikt fordi de har forskjellige mål, interesser og behov, som må beskyttes som en følge av trusselbildeutviklingen. For eksempel vil en statlig organisasjon ha et annet fokus på IK enn en sikkerhetsprodusent. En nettbank vil igjen ha et annet perspektiv og en annen opplevelse av IK-trusselen enn en liten lokal matbutikk. IK er noe som rammer bredt og kanskje driver det frem ulike innovasjoner i helt ulike organisasjoner, hvor pådriveren IK kan være fellesnevner i disse innovasjonene.

1.5 Teknologiutvikling + kriminalitet = innovasjon

Innenfor IKT ble det tidlig oppdaget kriminalitet. Hacking var et fenomen som fant sin plass tidlig i Internettets utvikling. Denne kriminaliteten var en videreutvikling av *phone phreakers*, som var et fenomen på den tiden da telefonlinjene var eneste verdensnettverk (Stefoff 2009, 15-16). Telefon phreakers var en form for hacking av telefonlinjer, hvor man dupliserte tonesekvenser som signaliserte hvor og til hvem en oppringing skulle (ibid.). På denne måten lurte de systemet, og fikk ringt uten å betale (ibid.). Mange lot det gå sport i dette (ibid., 15, 18). På 1980- og 1990-tallet, ettersom personlige datamaskiner ble tatt i bruk og *WWW* ble åpnet for allmenheten, gikk noen phreakers over til å hacke datasystemer (ibid., 18-19). Hacking kan defineres som uautorisert tilgang til datanettverk og datamaskiner (ibid., 15), og er en av grunnene til at sikkerhet innen informasjonsteknologi (IT) har funnet sin plass som eget fagfelt (Flowers 2007, 7, 14). Hackere viste seg tidlig å være både kreative og innovative, og kom seg inn i systemer, som medførte at disse systemene måtte forbedres og videreinnoveres for å gjøre dem sikrere. Altså kan kriminalitet utvikle kriminelle innovasjoner, dette kalles - *lovløs innovasjon* (outlaw innovation) (Flowers 2007, 2008; Schulz og Wagner 2010).

1.6 Motivasjon

Internettkriminalitet rammer bredt, samtidig som det er lite utforsket i akademisk sammenheng ut fra et innovasjonsperspektiv. Derfor tenkte jeg at det ville være hensiktsmessig å illustrere IK som en pådriver for innovasjon i ikke-kriminelle organisasjoner, ved å vise at dynamikken i IK kan fungere som en innovasjonspådriver. Dette gjorde jeg ved å belyse IK i bredden, gjennom å analysere fire forskjellige innovasjonscaser, belyst gjennom ulike ikke-kriminelle organisasjoner, som på ulike måter må forholde seg til IK.

En ekstra motivasjon og utfordring er det fordi problemstillingen ikke er blitt undersøkt tidligere, ut ifra et eksplisitt innovasjonsperspektiv. I tillegg til at det er et sensitivt tema for mange organisasjoner. Deler av innovasjonsforskningen er preget av et økonomisk perspektiv, hvor teknologi og innovasjon hovedsakelig ses på som noe som gir økonomisk nytte for organisasjoner. I organisasjonslitteraturen rundt organisasjonstilpasning har jeg heller ikke funnet noe som har å gjøre med kriminalitet og dens påvirkning på organisasjonstilpasninger. Derfor ser jeg det som et nyttig bidrag å kunne se på innovasjon på en ny og annerledes måte, ved å illustrere tilknytningen kriminalitet kan ha til noen ikke-kriminelle organisasjoners innovasjoner.

1.7 Nytten av oppgaven

All ny kunnskap som kan bidra til en bredere forståelse og innsikt, kan anses som nyttig. Tematikken i oppgaven er fokusert på en måte som kan minne om militære innovasjoner og militær sjargong, fordi innovasjonene hovedsakelig kommer som en konsekvens av en ikke-kommersiell trussel. Dette vil kanskje bidra til en ny forståelse og tilnærming til noen former for innovasjon, og oppgaven vil derfor forhåpentligvis oppfattes som et nytt og interessant bidrag i innovasjonsforskning og innovasjonslitteratur. Samtidig som dette er noe innovasjonsforskningen kan se på, kan det også gi innsikt til fagfelt innenfor organisasjonsutvikling, informasjonssikkerhet og science and technology studies (STS).

STS-tilnærming til innovasjon fremhever viktigheten av brukerne i teknologisk utvikling (Oudshoorn og Pinch 2003). De mener at brukere ikke bare er passive mottakere av teknologi, de er også aktører som utvikler og former teknologi. De hevder at brukere er blitt neglisjert, og at ved å inkludere brukere får man et perspektiv i samsvar med hva STS og innovasjonsstudier anviser. Internettkriminelle og organisasjoner som prøver å forsvare seg

eller andre, er i denne oppgaven brukere av teknologi. Denne «gjensidigheten» fører til innovasjoner som er med på å forme og videreutvikle selve teknologien, bruken av disse og prosessene rundt.

IK er økende, og derav øker også omfanget av sosiale-, økonomiske- og teknologiske konsekvenser for samfunnet. Forskning på dette under merkelapper som datasikkerhet, er mer aktuelt enn noen gang tidligere og er forskningsfelt som er i sterk vekst fordi behovet generelt for slik forskning og utvikling er økende. Jeg mener at denne oppgaven viser en kobling mellom kriminalitet og innovasjon som er svært aktuell. Casene i denne oppgaven viser blant annet innovasjonsgevinster andre enn de bedriftsøkonomiske og privatøkonomiske, noe som er et viktig aspekt i forhold til å se nytten av innovasjon på dette området. Dette kan igjen medføre mer bevissthet rundt IK hos brukere av Internett, og dermed at flere organisasjoner tilpasser seg trusselbildet, samt at det blir mer tilrettelagt for å få fortgang i å imøtekomme overordnede innovasjonsbehov som følge av IK, proaktive så vel som hendelsesorienterte. Samtidig som det kanskje vil gi en dypere forståelse av internetteknologiens utvikling og de konsekvensene dette har medført for samfunnet. I konklusjonen kommer jeg med ideer og synspunkter som jeg mener hadde vært interessante for videre forskning.

1.8 Problemstilling og forskningsspørsmål

I denne oppgaven skal jeg illustrere et forhold mellom IK og innovasjon i ikke-kriminelle organisasjoner. Dette gjør jeg ved å drøfte problemstillingen:

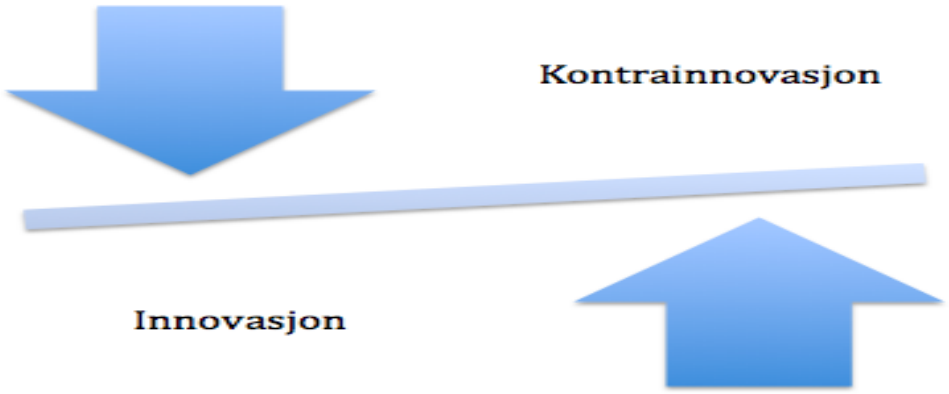
Hvordan kan internettkriminalitet være en pådriver for innovasjon i ikke-kriminelle organisasjoner?

For å kunne gi noe svar på denne problemstillingen skal jeg først analysere og besvare forskningsspørsmålet:

Hva slags innovasjoner kan komme som følge av internettkriminalitet i ikke-kriminelle organisasjoner?
- Hva slags typer innovasjon er dette?
- Hvordan kan disse endringene tolkes som innovasjoner?
- Hva er sammenhengen og utviklingsdynamikken mellom innovasjonene og IK?

1.8.1 Formål

Formålet med oppgaven er å vise hvordan IK kan oppfattes som en pådriver til innovasjon i ikke-kriminelle organisasjoner på ulike måter og hos ulike organisasjoner. Jeg presenterer begrepet *kontrainnovasjon*, som kan brukes om innovasjonene i casene. Generelt er formålet å illustrere hvordan kriminalitet, og IK spesielt, driver frem innovasjon og driver frem og former den teknologiske utviklingen, samt prosessene rundt. På denne måten håper jeg at jeg kan bidra til et nytt perspektiv og en ny forståelse av hva som kan påvirke og drive frem innovasjon og teknologi.



Figur 1.1 *Innovasjon-kontrainnovasjon*

1.8.2 Begrensninger

Denne oppgaven forsøker å illustrere at det kan være en dynamikk mellom IK og innovasjon i ikke-kriminelle organisasjoner, og å påvise hvordan IK kan være en faktor som driver frem innovasjon i ikke-kriminelle organisasjoner gjennom fire empiriske caser. Innovasjon studeres gjerne på systemnivåer som for eksempel nasjonale- (Edquist 2005, 183), regionale- (Asheim og Gertler 2005), sektorielle- (Malerba 2005), og teknologiske (Bergek, Hekkert og Jacobsson 2007), jeg har ikke forholdt meg til disse, men studerer kun en spesiell teknologisk utviklingstype på Internett gjennom fire caser. Oppgaven har som siktemål å illustrere fire ulike innovasjoner i fire ulike ikke-kriminelle organisasjoner, som har et forhold til IK. Dette er blitt gjort ved å foreta kvalitative intervjuer hos fire ulike norske organisasjoner som har innovert som en følge av blant annet et IK-forhold. Det blir drøftet hvordan disse er innovasjoner ut ifra innovasjonstypologiserings- og innovasjonskategoriseringslitteratur. Innovasjonsteorien byr på flere ulike typologiseringer, kategoriseringer og definisjoner av innovasjon, og jeg har derfor måttet begrense meg til de som er mest relevante for analyse og

forklaring av mitt empiriske materiale og mine funn, og i forhold til oppgavens problemstilling. Jeg gir også en rask innføring i hva kyberkriminalitet og IK er, og hvilken kategorisering som anvendes videre i analyse og drøfting. Det finnes også diverse definisjoner på kyberkriminalitet og ulike kategoriseringer. Jeg har forholdt meg til det jeg har funnet som jeg synes gir en fremstilling av fenomenet som passer oppgaven, og som er anerkjent innfor kyberkriminalitetsforskningsmiljøet.

I denne oppgaven har jeg en legalistisk tilnærming til IK, i motsetning til den sosiologiske tilnærmingen som STS bærer preg av, eller den politiske tilnærmingen som blant andre Helge Godø (2002) anvender. Dette vil si at jeg hovedsakelig forholder meg til IK etter den juridiske logikken, noe man kan lese mer om i kapittel to. Derfor problematiserer jeg ikke så mye rundt andre mulig tilnærminger til IK underveis i oppgaven.

Hensikten med å gi en innføring i innovasjon og kyberkriminalitet og IK er å gi leseren en forståelse av min analytiske og teoretiske tilnærming i oppgaven, særlig mot analysen av casene i kapittel fem, og hva jeg utelater. Slik kan leseren bedre forstå hva denne oppgaven faktisk sier noe om. Oppgaven må derfor ikke ses på som noe forsøk på å beskrive alle innovasjonstypologiseringer og defineringer, men kun som et teoretisk rammeverk til støtte for denne konkrete oppgaven. Det er heller ikke en fullstendig beskrivelse av hva IK er og kan være, men kun til for å gi leseren en overordnet forståelse av hva fenomenet blant annet kan innebære.

Datainnsamlingen baserer seg på to hovedkilder: 1) Gjennomgang og analyse av tilgjengelig litteratur og kilder som omhandler IK og innovasjon 2) Kvalitative dybdeintervjuer med én person i de fire ulike caseorganisasjonene og to personer som har erfaring og overordnet kunnskap på IK i Norge. Dette er ikke en fullstendig fremstilling av IK-situasjonen i Norge i dag, og personene i casene snakker ut fra sin erfaring og opplevelse av innovasjonen og IK generelt, og representerer ikke alle involverte parter i innovasjonene.

Jeg har valgt å anvende komparativ casemetode med kvalitative dybdeintervjuer til innsamling av data for analysen. Det er mulig å anvende andre metoder, men fordi jeg ønsker å illustrere det ved å påvise innovasjonsdynamikk hvor IK har vært en medvirkende pådrivende faktor, har jeg sett det som mest hensiktsmessig å velge noen få, og analysere disse mer i dybden. Samtidig kunne jeg da sammen med informantene snakke om det er en dynamikk og et drivende innovasjonsforhold.

Jeg anvender litteratur og teori i drøftingen på bakgrunn av en tilnærming jeg synes forklarer innovasjonsdynamikken best i forhold til valgte problemstilling. I den samfunnsvitenskapelige innovasjonslitteraturen er det to tilnærminger som dominerer: de som ser på innovasjon fra et økonomisk perspektiv, og de som ser på innovasjon fra et ledelsesperspektiv. Den ene preges av økonomiteoretikere, den andre av organisasjons- og ledelsesteoretikere, det som ofte betegnes som «management» - tilnærmingen.

Førstnevnte fokuserer i stor grad på innovasjon og teknologisk utvikling fra et økonomisk perspektiv, hvor innovasjon bør ha en kommersialiseringsverdi og gi nytte i form av effektivisering og produktutvikling, hvor begge til syvende og sist skal gi økt inntjening. Innenfor evolusjonær økonomi for eksempel, fokuseres det ofte på innovasjon og adoptering av teknologi som en nødvendighet for å kunne tilpasse seg markedet man er i, og de som ikke klarer tilpasningen, vil i en naturlig prosess bli avviklet gjennom at kunder velger noen andre. I organisasjon- og ledelseslitteraturen preges fokuset i forhold til innovasjon av organisasjoners lærings- og kunnskapsdelingsevner, lederkarakteristikker og organisasjonsstruktur og prosesser som determinanter for innovasjon. Begge tilnærmingene vedgår også at det er andre aktører som påvirker teknologi, økonomi, organisasjoner og innovasjon, og at dette igjen påvirker større deler av samfunnet. Særlig den evolusjonære tilnærmingen om tilpasning til omgivelser. Det er dette som helt overordnet gjør det til en relevant tilnærming for oppgaven, slik at litteratur om organisasjonstilpasning anvendes i kapittel seks, og knyttes til en viss grad opp mot det overordnede evolusjonærøkonomiske perspektivet.

1.9 Oppgavens struktur og oppbygning

Nedenfor gir jeg en kort oversikt over oppgavens oppbygning og kapitler, og hensikten med en slik oppbygning.

I kapittel to går jeg gjennom hva jeg legger i sentrale begreper i forhold til IK, slik som kyberkriminalitet, som ligger til grunn for min anvendelse av begrepet internettkriminalitet. I tillegg går jeg gjennom valgte kategoriseringer jeg finner relevante, slik at leseren får en bedre forståelse av hva fenomenet IK innebærer i denne oppgaven. Jeg anvender disse kategoriseringene i analysen av casene i kapittel fem.

I kapittel tre går jeg igjennom hva innovasjonsbegrepet innebefatter, og hva jeg innebefatter i mitt innovasjonsbegrep, samt min overordnede tilnærming til problemstillingen. Jeg anvender blant annet Joe Tidd og John Bessant (2009) sitt innovasjonsrom som grunnlag for å definere typer innovasjoner. I tillegg legger jeg frem litteratur om innovasjonsbehov (Tidd og Bessant 2009), nytte og den funksjonelle kilden til innovasjon (von Hippel 1988, 2005), samt gevinst (Godø 2008). Dette anvender jeg hovedsakelig i analysen av casene i kapittel fem.

I kapittel fire vil jeg presentere forskningsmetoden jeg har anvendt i undersøkelsene som er lagt til grunn for denne oppgaven. Her går jeg gjennom metodevalg, case- og informantutvalg, situasjoner som oppsto under datainnsamling, samt koding og analyse. Jeg fokuserer i denne delen på metoden rundt intervjudataen. I denne delen reflekterer jeg også over i hvilken grad jeg vurderer oppgavens reliabilitet og validitet.

I kapittel fem blir casene presentert og analysert opp mot forskningsspørsmålet. Kapittel to og tre er hovedsakelig til for å gi grunnlag for analysen i kapittel fem, som har til hensikt, gjennom fire caser, å illustrere fire innovasjoner som på en eller annen måte kan sies å være drevet frem av IK. Det anvendes også da til å påvise at tilfellene kan defineres som innovasjoner, og hvordan innovasjonen er drevet frem av en form for IK.

I kapittel seks drøfter jeg funnene mine på et mer generelt nivå, i forhold til hvordan IK kan oppfattes som en pådriver for innovasjon i ikke-kriminelle organisasjoner. I dette kapittelet anvender jeg noe ny litteratur og teori basert på den overordnede tilnærmingen i oppgaven, samt ny empiri i drøftelsen av problemstillingen, i tillegg til litteratur og empiri tidligere beskrevet i oppgaven. Jeg anvender i stor grad litteratur fra ulike kilder innenfor innovasjon, organisasjon og økonomi som jeg finner relevant, og som kan være med å forklare det oppgaven har til hensikt å påvise. I tillegg fremlegges en modell som kanskje illustrerer innovasjonsdynamikken som skjer mellom IK og ikke-kriminelle organisasjoner.

Avslutningsvis vil jeg komme med en oppsummering og konklusjon i kapittel syv, samtidig som jeg kommer med forslag til videre forskning som jeg anser som hensiktsmessig.

2.0 Sentral litteratur og sentrale begreper innen internettkriminalitet

«Technological advances have always been used to the advantage of the criminal fraternity.» (McCusker 2006, 257)

Enkelt forklart er Internett en gruppe kollektivt avtalte informasjonsprotokoller (TCP-IP) som muliggjør kommunikasjon og samtrafikk mellom alle nodene og terminalene som er tilknyttet nettet (Wall 2007, 35). I dag har man muligheten til å kommunisere ved hjelp av mobil, tv, nettbrett, elektroniske bøker, pc og lignende, særlig takket være trådløse teknologier som for eksempel GSM (Global System for Mobile) og WiFi. Ettersom data- og kommunikasjonsteknologi i større og større grad har blitt billigere og mer brukervennlig, og tilgangen til Internett er blitt mer utbredt har dette til sammen gjort kyberrommet til et attraktivt marked både for bedrifter men også for kriminelle (Wall 2007, 35).

I dette kapittelet vil jeg presentere kyberkriminalitet og kategoriseringer av dette, og hva jeg legger i begrepet internettkriminalitet (IK). Kategoriseringene anvendes i caseanalysene i kapittel fem. Dette kapittelet er også relevant å ha som bakgrunn i kapittel seks, som skal omhandle IK som pådriver for innovasjon, det vil si kjernen i denne oppgaven.

2.1 Kyberkriminalitet

Begrepet *cyberspace*, eller *kyberrom* som det heter på norsk, henviser til populærbeskrivelsen fra science fiction av det mentalt konstruerte virtuelle miljøet hvor aktivitetene til nettverkstilkoblede datamaskiner finner sted (Wall 2007, 10). Opprinnelig kommer ordet *cyber* fra det greske ordet *kubernetes* som betyr styrmann (ibid., 11). Kyberkriminalitet henviser til kriminalitet som befinner seg eller finner sted i kyberrommet (ibid., 10). David Wall (2007, 10) definerer kyberkriminalitet som kriminell eller skadelig aktivitet som involverer innhenting eller manipulering av informasjon for vinning ved hjelp av nettverksteknologi. Det er denne definisjonen jeg anvender om internettkriminalitet (IK), med avgrensning til at nettverksteknologien som anvendes er Internett.

Et problem med kyberkriminalitet er at det i lang tid, og fremdeles til dels i dag, ikke omfattes av lover, og ikke alltid er en kriminell handling ut fra lovverkets forståelse (Wall 2007, 10). Særlig har dette i lang tid dominert problematikken rundt eierskap og kontroll på Internett

(ibid., 34). Problemet med å få kunnskap om kyberkriminalitet ligger blant annet i det at denne kriminaliteten ikke følger det tradisjonelle mønsteret man vanligvis vurderer trusselnivå og alvorlighetsgrad etter, i tillegg til at statistikken lenge har vært preget av at mye kyberkriminalitet ikke har blitt registrert (NSR 2012, 14-15; Wall 2007, 17, 62).

2.2 Internett og informasjonssamfunnet

«The full social and economic impact of cyberspace upon the individual is only just beginning to be understood.» (Wall 2007, 32)

Manuel Castells (2000, 79) beskriver tre karakteristikker som den nye informasjonsøkonomien kjennetegnes av: *informasjonsmessig* produktivitet, *globalitet* og *nettverk.* Med informasjonsmessig produktivitet mener han at man kan skape/generere kunnskap og bearbeide/administrere informasjon, globalitet vil si at man kan jobbe sammen uavhengig av tid og sted, og med nettverk mener han at man er koblet sammen (ibid.). Disse har skapt en ny æra av økonomiske organisasjoner, både som verktøy for kommunikasjon internt i en organisasjon som kan ha kontorer spredt over hele kloden, men også som et middel til å kommunisere med kunder og ta for eksempel bestillinger over nett, og ikke minst nettverksbaserte forretninger, som for eksempel en nettbank eller Finn.no. I kyberrommet uttrykkes økonomisk verdi gjennom ideer og symboler, i motsetning til tidligere, hvor verdi kom i form av håndfaste produkter og fysisk eiendom (Barlow 1994). I takt med at internettbruken blir mer utbredt blant bedrifter, organisasjoner og enkeltindivider, vil kriminelle prøve å utnytte dette for egen vinning. Kyberkriminelles interesse ligger hovedsakelig i å utvinne verdi gjennom innhenting av informasjon, og dette kan gjøres på tvers av kulturer og landegrenser (Wall 2007, 36-37).

Wall (2007, 34) har laget en tommelfingerregel for kyberkriminalitet, kalt *transformeringstesten* (transformation test). Den innebærer at man skal fjerne nettverksteknologien fra kriminelle hendelser, og dermed se hva som står igjen (ibid.). På denne måten får man en bedre forståelse av i hvilken grad den kriminelle handlingen er avhengig av denne teknologien. Gjennom en slik tommelfingerregel ønsker han at man i større grad skal forstå hvordan Internett er blitt et medium i utførelsen av kriminell aktivitet (ibid.).

2.3 Tre generasjoner kyberkriminalitet

Wall (2007, 43-48) omtaler kyberkriminalitet i tre generasjoner. I første generasjon kyberkriminalitet bruker man datamaskiner som hjelpemiddel til å utføre tradisjonell kriminalitet (ibid., 44). Eksempelvis brukes datamaskiner i forberedelsesstadiet til innhenting av informasjon eller som kommunikasjonsmiddel (Wall 2007, 45; Brodeur 1983). I denne type kriminalitet kan datamaskiner og nettverksteknologi bidra til den kriminelle aktiviteten, men fjernes disse teknologiene, vil kriminaliteten fremdeles finne sted, men ved bruk av andre midler som for eksempel bøker og telefon (Wall 2007, 45).

Annengenerasjons kyberkriminalitet innebærer den muligheten for kriminalitet på tvers av landegrenser og hav som nettverksteknologien har gitt mulighet for. Internettet har skapt en mulighet ved at tradisjonell kriminalitet kan utføres på globalt nivå. Tar man vekk Internett og kriminaliteten vil fremdeles finne sted, men ikke på samme globale og transnasjonale nivå og ikke med like stor effekt. Eksempler på denne type kriminalitet kan være deling av barneporno og svindel e-post, som begge har dype historiske røtter (Wall 2007, 45-46).

Tredjegenerasjons kyberkriminalitet er «ekte» kyberkriminalitet. Med dette menes det kriminalitet som er helt skapt av de muligheter nettverksteknologien har medført. Den har en distribuert og automatisert programvarestyrt karakteristikk. Disse kriminelle aktivitetene er i mye mindre grad avhengig av sosial manipulasjon[2], i motsetning til første- og annen generasjons kyberkriminalitet. Dette er kriminalitet som ikke ville kunne funnet sted uten bredbåndsteknologi og Internett, da det kun kan foregå i kyberrommet. Et eksempel på denne type kriminalitet er spamming [3] (Wall 2007, 47-48).

2.4 Klassifisering av kyberkriminalitet

Det finnes flere ulike klassifiseringer av kyberkriminalitet og kyberangrep (Kshetri 2010, 10-11). Wall (2007) anvender klassifisering hvor man skiller kyberkriminalitet i tre kriminologier; dataintegritetskriminalitet, dataassistert kriminalitet og

[2] **Sosial manipulasjon,** på eng. social engineering, er en metode å innhente nødvendig informasjon for å bistå annen type kriminalitet, som for eksempel koder til et datasystem (Wall 2007, 59). Man manipulerer offeret gjennom å utgi seg for å være en annen person, som for eksempel en medarbeider, slik at offeret i god tro oppgir eller på en annen måte tilgjengeliggjør nødvendig informasjon for forfalskeren (ibid.). Dette kan gjøres over for eksempel e-post, chat, telefon eller personlig møte.

[3] **Spamming** er uønskede e-poster, gjerne reklamepost, som sendes ut til mange på en gang (Rush m.fl. 2009, 95).

datainnholdskriminalitet. Førstnevnte omhandler angrep på sikkerheten til nettverkstilgangsmekanismer, som for eksempel tjenestenektangrep[4], hacking[5] og cracking[6] (Wall 2007, 49). Dette kan typisk være kriminelle handlinger som skal understøtte andre former for kriminalitet, som for eksempel phishing[7] (ibid.). Dataassistert kriminalitet bruker datamaskiner som er koblet på nett til for eksempel å skaffe varer og penger (ibid., 50). Datainnholdskriminalitet handler om ulovlig innhold på nettverkstilkoblede maskiner, som for eksempel barneporno og distribuering av dette (ibid., 50). Disse begrepene skal utdypes nedenfor.

2.4.1 Dataintegritetskriminalitet

Dataintegritetskriminalitet er den formen for kriminalitet som innebærer hacking, cracking og tjenestenektangrep på datamaskiner i nettverk (Wall 2007, 52-53). Dette er angrep som svekker integriteten og kompromitterer hva datasystemer står for (ibid.). Slik kriminalitet kan videre medføre svekket tillit til dem som anvender datasystemer under angrep. Slike angrep kan være forløper til annen kriminalitet, som for eksempel at man har laget en bakdør i et system som kan brukes for å komme inn i systemet igjen ved et senere tidspunkt, slik at kriminelle kan hente ut informasjon som kan brukes senere. Eksempler på slik informasjon kan være brukernavn og passord, personopplysninger eller bedriftsopplysninger. Kriminelle

[4] **Tjenestenektangrep**, ofte omtalt som DDOS (distributed denial of service attack), er angrep hvor det forsøkes å hindre legitime brukere tilgang til et spesifikt nettverk eller datasystem, ved å skape kommunikasjonssammenbrudd via jamming (Rush m.fl. 2009, 93; Wall 2007, 61-62). Motivasjonen bak slike angrep kan være politiske og ideologiske eller finansielle, som utpressere, eller andre ytre motivasjoner (Rush m.fl. 2009, 93; Wall 2007, 61).

[5] **Hacking** omhandler den aktivitet å programmere, og en hacker er ofte en IT-entusiast med høye IT-kunnskaper (Godø 2002, 9-10). Hackere blir ofte forvekslet med crackere (ibid., 10). Forskjellen mellom de to er at hackere er «etiske» etter de tradisjonelle hackernes etikk og tro på fri tilgang til offentlig informasjon (Godø 2002, 10; Wall 2007, 54-55). Dette betyr at deres aktivitet kan falle både innenfor og utenfor hva som er lovlig, men i de fleste tilfeller i dag vil hacking juridisk sett være ulovlig og anses i stor grad som en form for cracking (Wall 2007, 54-55). Hackere blir ofte kalt *white hat hackers* (Wall 2007, 54). Wikileaks er et eksempel på «politisk» hacking, og de mener de er etiske etter tradisjonell hackeretikk.

[6] **Cracking** omhandler å innhente, stjele eller ødelegge informasjon i datasystemer ved ulovlig å ta seg inn i systemene, og kan være motivert av ytre motivasjoner som finansiell vinning eller indre motivasjoner som personlig hevn (Godø 2002, 10; Wall 2007, 54). Crackere blir ofte kalt *black hat crackers* (Wall 2007, 54).

[7] **Phishing** er en form for sosial manipulasjon og innebærer, gjennom anvendelse av IKT, å lure sine ofre til å tro at man er noe annet for å lure til seg sensitiv informasjon som for eksempel passord. Det kan for eksempel være å videresende ofrene til en annen nettside som ser lik ut som en ekte nettbankside, for å få dem til å oppgi for eksempel passord (Rush m.fl. 2009, 94).

kan hacke en nettside slik at besøkende blir videreført til en ondsinnet side som videre kan få en nettbruker til for eksempel å laste ned virus for å nevne noe. Hacking er hovedsakelig tilsiktet å brekke sikkerhetssystemer på en PC i et nettverk ved å angripe datasystemets integritet, for slik å få uautorisert tilgang til områder hvor det er etablert rettigheter i forhold til eierskap og tilgang (ibid., 53).

2.4.2 Dataassistert kriminalitet

Dataassistert kriminalitet innebærer lovbrudd hvor kriminelle anvender nettverkstilkoblede datamaskiner. Wall (2007, 71) trekker frem tre tydelige grupper under denne formen for vinningsforbrytelse. Det er virtuelt tyveri, -bankran og -svindel (ibid.). Førstnevnte innebærer tyveri av immaterielle verdier, den andre omhandler misbruk av finansielle internettjenester, og den siste innebærer internettassistert svindel (ibid.). Innenfor disse gruppene finner man alt fra phishing til svindelauksjoner og falsk reklame (se bl.a. Wall 2007, 61-102). Denne type kriminalitet utvikler seg i takt med den teknologiske utviklingen (Wall 2007, 101).

2.4.3 Datainnholdskriminalitet

Datainnholdskriminalitet omhandler distribusjon av ord og bilder via Internett, hvor innholdet er skadelig og i strid med loven (Wall 2007, 104). Slik kriminalitet kan være for eksempel oppskrifter på å lage våpen og narkotiske stoffer, cyber-stalking[8] og grooming[9], barneporno, å henge ut grupper og underforstått oppfordre til vold, mobbing og hatefulle og rasistiske ytringer (ibid., 109-125). Selv om kyberrommet ligger utenfor nasjonal jurisdiksjon, betyr det ikke at det er et anarki og at man kan gjøre hva man vil der. Det er en hårfin grense mellom det som er ytringsfrihet og det som er sjikane, rasisme og lignende. Ord og bilder og det inntrykk de kan gi, kan medføre et samspill mellom hva som bare er og blir ved tanken og hva som fører til faktisk handling (ibid., 128). Å lese oppskriften på hvordan man lager narkotiske stoffer eller bomber, er i seg selv ikke ulovlig, men det å lage det er det.

[8] **Cyber-stalking** er når noen velger seg ut et offer, og trakasserer ofret på bakgrunn av informasjon eller en karakteristikk som offeret har offentliggjort på Internett (Wall 2007, 124).

[9] **Grooming** er i likhet med phishing en form for sosial manipulasjon, og innebærer å bli venner og skape tillit med ofrene slik at de til slutt lar seg overtale til personlig møte (Wall 2007, 125). Pedofile groomer gjerne barneofrene sine over Internett ved å late som de selv er barn eller mye yngre enn de i virkeligheten er, slik at ofret etter hvert møter den pedofile, og videre blir utsatt for seksuelle forbrytelser (Aas-Hansen 2004, 7; Wall 2007, 125). Dette er en form for sosial manipulasjon og den kan foregå i kyberrommet og i den virkelige verden.

2.5 Motivasjonsfaktorer for å begå internettkriminalitet

«Old crimes in new bottles» (O'Neill 2000, 237).

IK kan både være kriminelle gjerninger som blir utført helt eller delvis på Internett, men også det å dele informasjon på Internett om hvordan man kan gjennomføre kriminalitet (Wall 2007). Det er mange ulike typer mennesker som bedriver IK (Rasch 1996, I. Introduction). Det antas at det er mange ofre av IK, privatpersoner og organisasjoner, som velger ikke å anmelde av ulike årsaker, noe som medfører store mørketall (NSR 2012, 14-15; Wall 2007, 62). Når man hverken vet hvem ofrene eller lovbryterne er, er det vanskelig å finne ut hva som er lovbryternes motivasjon for å begå disse handlingene (Wall 2007, 62). Allikevel har det blitt funnet noe, og mye av det har vist seg å være sammenfallende med motivasjonen bak tradisjonelle forbrytelser, med noen unntak (ibid.).

Wall (2007, 62-65) deler kyberkriminell motivasjon i disse syv gruppene: selvtilfredshet, behov for respekt fra likemenn, ønske om å imponere potensielle arbeidsgivere, kriminell vinning eller konkurransefordeler, hevn, avstand til ofre og politisk motivert protest. Angrep på Internett handler i like stor grad om materielle goder og immaterielle hensyn (Hirshleifer 1998; Kshetri 2010, 21). De immaterielle målene kan være stolthet, ære og dominans (Hirshleifer 1998, 10). Dette er motivasjon kjent fra krig, og derfor kan man til en viss grad sammenligne angrep på Internett med krig i den fysiske verden (Kshetri 2010, 21).

2.6 Oppsummering

I dette kapittelet har man fått en innføring i IK og kyberkriminalitet, som er blitt forklart som det samme i denne oppgaven, med det unntak av at IK forutsetter at nettverksteknologien som anvendes i de kriminelle aktivitetene er Internett. Hensikten med dette kapittelet er å gi en innføring i hva fenomenet IK kan innebære, og hva jeg definerer det som i denne oppgaven. I tillegg gir kapittelet et kategoriseringsrammeverk av IK som anvendes i analysen av casene i kapittel fem.

3.0 Sentral litteratur og sentrale begreper innen innovasjon

Internettkriminalitet (IK) i kombinasjon med innovasjon har i liten grad vært tematisert i innovasjonsforskning. Rammeverket i denne oppgaven er primært evolusjonært, og jeg vil først introdusere den overordnede tilnærmingen som er grunnlag for litteraturen som blir introdusert og anvendt i drøftingskapittelet for å svare på problemstillingen. Men for best å kunne svare på oppgavens forskningsspørsmål og problemstillingen, og illustrere den dynamikken jeg ønsker, har jeg valgt å legge frem noen teorier, begreper, typologier og kategoriseringer som jeg mener er relevant for å analysere og drøfte forskningsspørsmålet. Dette for å rydde opp i en komplisert innovasjonsverden. Hensikten med dette kapittelet er hovedsakelig å gi et grunnlag for å forstå hvordan jeg velger å analysere de enkelte casene i kapittel fem.

3.1 Overordnet tilnærming

Innovasjonsforskningen har helt siden Joseph Schumpeter, en av de første og største økonomiske forskerne som omtalte fenomenet innovasjon, vært påvirket av økonomisk tankesett. Som en konsekvens av dette har innovasjonsforskning ofte fokusert på markedsstruktur og bedriftsstørrelser som determinanter for bedriftsinnovasjon når man ser på faktorer som driver teknologiske innovasjoner (Teece 2006, 1132). I tillegg har mye fokusert på at innovasjon skal innebefatte økonomisk nytte. En slik tilnærming vil kunne begrense innovasjonsbegrepet til å utelate andre former for innovasjon enn de teknologiske, og andre pådrivere for teknologiske innovasjoner og teknologisk utvikling, hvor visse former for kriminalitet kanskje vil kunne sies å være en pådriver (Flowers 2008, 178).

Allikevel tar den økonomiske tilnærmingen samt organisasjons- og ledelsestilnærmingen det som en forutsetning at det er flere faktorer som påvirker innovasjon og teknologisk utvikling. Den evolusjonære økonomiske retningen drar linker til biologien, ved å se på teknologisk utvikling som en evolusjonær prosess som påvirker økonomien, og hvor organisasjoner og innovasjoner må tilpasse seg omgivelsene, og at etter hvert som tilpasninger skjer, skjer det endringer i organisasjoner, teknologier og i de sosiale omgivelsene. Richard Nelson (1994) beskriver teknologi, industrielle strukturer og omgivelsene rundt, som i *samutvikling* (coevolution). Altså at endringene i teknologi påvirker økonomi, institusjoner, incentiver, industrier og firmaer. I tillegg er teknologisk utvikling og innovasjoner en *stiavhengig*

prosess, fordi dagens teknologier og innovasjoner bygger videre på tidligere ideer og teknologier (Nelson 1994, 50).

Nelson (1994, 53) mener at politiske og sosiale krefter er med på å påvirke den økonomiske endringen som teknologiutvikling og innovasjon medfører. Offentlig institusjoner, frivillige organisasjoner, politiske avgjørelser og lover er eksempler på kontekstuelle forhold som ofte endres i takt med en teknologisk evolusjon, og viser at det er en kompleks prosess (ibid., 55-57). Christopher Freeman (1991) og Carlota Perez (1983) anvender i sin beskrivelse begrepet *tekno-økonomisk paradigme* (techno-economic paradigm). De bruker blant annet dagens informasjons- og telekommunikasjonsperiode, som et eksempel til å forklare hvordan nasjonale institusjoner har måttet tilpasse og tilrettelegge for denne utviklingen (Freeman 1991; Perez 1983, 2010). Dette kan medføre innovasjoner, som for eksempel organisatoriske og inkrementelle innovasjoner (Freeman 1991). Det sosiale miljøet, det menneskeskapte og de offentlige institusjonene både hemmer og fremmer teknologi og innovasjoner (ibid.).

Denne tilnærmingen til teknologi og innovasjon er relevant i forhold til denne oppgaven, for å forstå hvordan innovasjonene i oppgaven er en del av en evolusjonær prosess, som er kommet som følge av den teknologiske innovasjonen Internett. Casene i denne oppgaven illustrer kanskje en samutvikling med IK. De representerer ulike bransjer og organisasjoner som forholder seg til Internett på ulike måter, og hvor kriminalitet er en del av det sosiale miljøet, også på Internett. Organisasjoner er i kontinuerlig endring på bakgrunn av endringer i de eksterne forhold (Child og Kieser 1981, 28). Man tilpasser seg de omgivelsene man er i, og dette medfører endringer som medfører andre endringer (Lipsey, Carlaw og Bekar 2005, 4; Normann 1971, 1; Zaltman, Duncan og Holbek 1973, 6, 110). Ny teknologi og anvendelsen av dette kan medføre både positive og negative konsekvenser, og man må videreinnovere for å håndtere de negative konsekvensene (Simon 1971, 48-51). I casenes forsøk på å hemme IK utvikler de teknologien og prosessene rundt, samt tvinger frem en motreaksjon, og driver den teknologiske utviklingen fremover.

3.2 Hva er innovasjon?

Innovasjoner omhandler ofte å sette sammen kjente ting på nye måter, men kan noen ganger gjelde en oppfinnelse (Schumpeter [1934] 1983, 132; van de Ven og Angle 2000, 12). En innovasjon trenger som nevnt ikke å være ny for alle og enhver, men må oppleves som ny for dem som implementerer den (Rogers 1983, 11; van de Ven og Angle 2000, 12). Godø (2008,

10) deler opp konteksten som avgjør om noe oppfattes som nytt etter kriteriene nytt i verden, nytt i samfunnet, nytt i bedriften eller lokalsamfunnet, og nytt for meg. Han påpeker allikevel at denne opplevelsen ikke avgjør om noe er en innovasjon, fordi innovasjon forutsetter diffusjon (spredning) (ibid., 11). Det forutsetter at samfunnet, eller i hvert fall en gruppe i samfunnet, anvender eller benytter seg av det (ibid.,11).

Man skiller mellom oppfinnelse og innovasjon, hvor innovasjon handler om å ta ideen eller oppfinnelsen og få den i utbredt bruk, og blir ofte koblet til kommersialiseringsprosessen (Flowers 2008, 178; Teece 1986). Men å forbeholde innovasjon til kommersielle produkter og tjenester er begrensende når dette dermed utelukker en god del innovasjonsaktivitet, som for eksempel lovløse innovasjoner og brukerinnovasjon (Fowlers 2008, 178; von Hippel 2007). Lovløse innovasjoner kan ikke patenteres, og en del innovasjon som ikke er produsentinnovasjon, vil grovt sagt sies å være brukerinnovasjon, og kan være av administrativ-, immateriell-, og ikke-salgbar karakter, og trenger nødvendigvis ikke å gi økt inntjening eller økt effektivitet i organisasjonen. Et annet eksempel er innovasjon i offentlige organisasjoner (Flowers 2008, 178). En innovasjon kan være basert på en oppfinnelse, men en innovasjon er *noe* nytt som blir tatt i bruk av samfunnet. Innovasjon handler også om å dekke sosiale behov, dette vil si at innovasjonsbegrepet ikke er forbeholdt kommersielle markeds- og konsumbehov (Tidd og Bessant 2009, 235-236). I tillegg har man det aspektet vi skal komme tilbake til senere i kapittelet, som omhandler innovasjonsgevinst og det faktum at selve ideen eller oppfinnelsen ikke nødvendigvis blir spredt og anvendt av samfunnet, men gevinsten den gir, blir det (Godø 2008, 22-25).

I denne oppgaven forholder jeg meg til at en innovasjon ikke trenger å bli spredt til store deler av samfunnet. Så lenge en idé blir utviklet og implementert, oppleves som ny for dem som implementerer den (van de Ven og Angle 2000, 12), og medfører endring av rutiner hos dem som implementerer (Nelson og Winter 1982, 128; Zaltman, Duncan og Holbek 1973, 158), er det en innovasjon.

3.3 De fire P'er i innovasjonsrommet

I kapittel fem forsøker jeg å analysere fire innovasjonscaser forbundet med IK. I den forbindelse har jeg valgt å forholde meg til de fire dimensjonene av innovasjoner, omtalt i *Managing Innovation: Integrating Technological, Market and Organizational Change* skrevet av Tidd og Bessant (2009, 21-22), når jeg forsøker å typologisere innovasjonene. Grunnen til

at jeg anvender denne typologiseringen, er at den beskriver et innovasjonsrom med fire dimensjoner, slik at man åpner opp for at innovasjoner kan plasseres mellom de overordnede innovasjonstypene innenfor dette rommet. Det er endringer som tar ulike former, det vil si at det finnes utallige forskjellige innovasjoner, som kan bære preg av, og være en kombinasjon av flere ulike typer innovasjoner og ligger mellom flere innovasjonsdimensjoner (ibid., 21). De fire dimensjonene er prosess-, produkt-, paradigme- og posisjonsinnovasjon, samtidig som rommet gir rom for en gradvis overgang fra radikal til inkrementell innovasjon (ibid. 21-22).

I Tidd og Bessant (2009, 21, 23) sitt innovasjonsrom innebefatter *prosessinnovasjon* endringer i måten en organisasjon skaper noe på, og hvordan organisasjoners tilbud leveres. *Produktinnovasjon* omfatter endringer på selve tilbudet organisasjonen tilbyr, som både kan være nye for hele verden (radikale) eller mindre forbedringer (inkrementelle) på tidligere produkter eller tjenester (ibid.). *Posisjonsinnovasjon* er når man tar et produkt eller en service fra én kontekst og implementerer det i en annen kontekst som den er ny for (ibid., 21, 24). Når man endrer en organisasjons underliggende tankesett, og dette medfører endring i rutiner, kalles det en *paradigmeinnovasjon* (ibid., 21, 24). Radikale innovasjoner er gjennombrudd som endrer hvordan vi anvender og tenker om den aktuelle innovasjonen og det miljøet den operer i, og de er nye for hele verden (ibid., 27). En inkrementell innovasjon handler om å gjøre det man gjør bedre (ibid., 27). Ofte er en inkrementell innovasjon ikke ny for hele verden, men kun ny for den organisasjonen som tar den i bruk.

3.4 Kildene til innovasjon: behov, nytte og gevinst

En innovasjon må fylle et behov for at den skal ha noen nytte og dermed gi en ønskelig gevinst. I denne delen skriver jeg om litteratur jeg har funnet og anvender i analysen, for nettopp å illustrere behovet, nytten og gevinsten caseinnovasjonene gir. Dette er viktige aspekter å se på for å kunne si noe om i hvilken grad tilfellene er innovasjoner og hvordan de er satt inn i en innovasjonssammenheng som er koblet opp mot IK.

3.4.1 Kunnskapsdytt og behovstrekk

«Necessity may be the mother of invention, but procreation still requires a partner.»
(Freeman og Soete 1997, 201)

Kunnskapsdytt (knowledge push) og *behovstrekk* (need pull) blir omtalt som nøkkeldrivere for innovasjon. Dette fordi de komplementerer hverandre, og innebærer at man må forstå

behov og finne måter å dekke behovene på for at en innovasjon skal lykkes (Tidd og Bessant 2009, 232-233).

Kunnskapsdytt innebærer at man gjennom forskning og utvikling eller spesialister er satt til å løse spesielle teknologiske utfordringer og problemer. Denne forskningen fører i blant til gjennombrudd, som videre kan anvendes på andre bruksområder og derav blir innovasjoner. Det omhandler at man utnytter de mulighetene som kommer som et resultat av vitenskapelig forskning. Dette vil si at kunnskapen er fremme og dyttes inn i muligheter, men allikevel er man som oftest avhengig av en form for etterspørsel (Tidd og Bessant 2009, 229-232).

Behovstrekk omhandler det behovet som gjør at innovasjonsmuligheter kan fylle en etterspørsel. Det er dette som åpner innovasjonsmuligheter og som også kan tvinge frem ny kunnskap. Man er avhengig av dette behovet, slik at brukere ser en nytte av å adoptere innovasjon eller er motivert til endring. Dette er trekket (pull) som komplementerer dyttet (push). En innovasjon er i de fleste tilfeller en respons på et behov, enten det er oppfattelsen av et behov eller et ekte behov, men uten et slikt behov vil en innovasjon ha liten sjanse for å lykkes (Tidd og Bessant 2009, 232).

3.4.2 Det funksjonelle innovasjonsforholdet

Store deler av forskning innen teknologisk endring har vært fokusert på tilbudssidens dynamikk, det vil si leverandør- og produsentsiden (Adner og Levinthal 2001, 611). Det mest logiske stedet for produkt- og serviceinnovasjoner har tradisjonelt blitt ansett for å være hos produsenter (von Hippel 1988, 2005, 2007). Dette fordi det er blitt antatt at privatfinansielle incentiver for å innovere hos produsenter er høyere enn for private person- og bedriftsbrukere, da brukerinnovatører hovedsakelig forventer en verdi gjennom intern bruk (von Hippel 2007, 297). Dette har medført lite fokus på etterspørselsomgivelsene, og disses påvirkning på utvikling og teknologisk evolusjon (Adner og Levinthal 2001, 611). Det finnes dog noen unntak, deriblant Eric von Hippel.

Eric von Hippel skriver i boken *The Sources of Innovation* (1988) om hvordan kilden til innovasjon i stor grad tradisjonelt har blitt antatt kommet fra produktprodusenter. Man har først og fremst sett på hvem innovatøren er (von Hippel 1988, 3). Men i denne boken illustrerer von Hippel hvordan både produsenter og brukere kan innovere. Dette sier han kommer an på den funksjonelle kilden til innovasjon (ibid.). Dette er interessant for denne

oppgaven fordi ikke-kriminelles innovasjoner som respons på IK ikke nødvendigvis vil være produsentinnovasjoner.

For å identifisere den funksjonelle kilden til innovasjon kategoriserer man firmaer og individer etter hvilken funksjonell nytte de skaffer seg av en viss produkt-, service- eller prosessinnovasjon (von Hippel 1988, 3). Forskjellen mellom en produsent som innoverer og en bruker som innoverer, er at produsenten har fordeler ved å *selge* et produkt, mens en bruker har fordeler av å *bruke* et produkt (von Hippel 2005, 3). Man kan også skille dem med begrepene innovatør og innovasjon, hvor en bruker er innovatør fordi hun/han har en *direkte nytte* eller fordel av innovasjonen, mens en produsent, hvor alle som ikke går under definisjonen bruker, må *selge* innovasjonsrelaterte produkter eller tjenester *til brukere* for å kunne få noen direkte eller indirekte fordeler/profitter av innovasjonen (ibid.). Bruker og produsent er de to hovedinnovatørkategoriene, men det vil også finnes andre funksjonelle innovasjonsforhold mellom innovasjon og innovatør, samt at det funksjonelle forholdet til forskjellige innovasjoner kan variere (von Hippel 1988, 4; 2005, 3).

En innovatør er den som først utvikler en innovasjon til en brukbar tilstand, noe som bevises gjennom nyttig avkastning, enten dette er et individ eller et firma (von Hippel 1988, 4). I mange tilfeller har brukerinnovatører ledebrukerkarakteristikker (von Hippel 2005, 4, 23). En *ledebruker* (leade user) er en bruker som er foran flertallet av brukere innenfor en markedstrend (ibid., 4). Dette gjør at de innovasjoner som ledebrukere skaper for å dekke sine behov, vil være attraktive for produsenter å kommersialisere (ibid., 4, 19, 23).

Vanligvis vil brukere i motsetning til produsenter kun tenke på sin egen personlige eller interne nytte av en innovasjon, mens produsenter kun er interessert i innovasjoner hvor de ser at mange brukere har nytte av den, da dette vil øke det potensielle markedet (von Hippel 1988, 7). Innenfor brukerinnovasjon er det mange som sprer innovasjonen sin fritt for at andre skal kunne bruke den, uten noen finansiell interesse, og det er en mer åpen innovasjonsprosess (von Hippel 2005, 77-78). Dette skriver Henry Chesbrough (2003) om under begrepet *åpen innovasjon*. Åpen innovasjon omhandler i grove trekk det å åpne organisasjonen opp for å ta inn kunnskap og ideer utenfra, og kan også innebære å ta kunnskaper og ideer ut fra organisasjonen, uten at det nødvendigvis er ferdige produkter (Chesbrough 2006, 1).

Det er flere begrensninger med von Hippels (1988) teori om kilden til innovasjon. I forhold til min oppgave gjelder det blant annet at han i sine undersøkelser har fokusert på produkt- og

prosesskategorier, i tillegg til at innovatørene kun har hatt én funksjonell rolle i forhold til disse innovasjonene, som enten produsent eller bruker (von Hippel 1988, 8). I virkeligheten ville man trolig i mange tilfeller sett en innovatør med ulike funksjonelle forhold til innovasjon, hvor for eksempel innovatøren samarbeider med andre, eller hvor rollene bruker, produsent eller leverandør ikke kan omfatte innovatørens funksjonelle innovasjonsnytteforhold (ibid., 4, 8). Grunnen til at denne teorien for kategorisering er interessant for denne oppgave, er at jeg i oppgaven blant annet viser hvordan ulike typer organisasjoner innoverer som følge av IK. Og for å vise at de har en nytte, er det viktig å se hvorfor de innoverer, hva innovasjonen er og hvilken nytte innovasjonen er ment å gi. På denne måten kan kilden til innovasjon benyttes som en måte å kategorisere det funksjonelle forholdet på som ikke-kriminelle organisasjoner har til noen av sine innovasjoner, og som kanskje delvis er drevet frem av IK.

von Hippel (2005, 1, 13, 121) mener at det er skjedd en *demokratisering av innovasjon*, ved at brukeres evne til å innovere øker som følge av software og hardware til datamaskiner. Dette har gitt mer utbredt tilgang til verktøy og deler som trengs for å innovere for seg selv, samtidig som det har økt tilgangen til et økende og rikere innovasjonsfellesskap (ibid., 13, 121). Tilsvarende verktøy var tidligere kun tilgjengelig for noen få i bedrifter og organisasjoner (ibid., 13). Fordelen ved at brukerinnovasjoner øker er blant annet at den sosiale velferden øker gjennom at brukere får nøyaktig det de trenger (ibid., 2, 11-12). Dette fordi det ikke er noe kompromiss i forhold til hva den enkelte bruker ønsker fra produsentens side, når produsent er interessert i å kunne selge samme produkt eller tjeneste til flere (ibid., 5).

Lovløs innovasjon

En form for brukerinnovasjon er *lovløs innovasjon* (outlaw innovation) (Flowers 2007, 2008). Kriminelle er også brukere av teknologi. Flowers definerer kriminelle brukere som følgende:

> […] lovløse brukere er brukere som, enten individuelt eller som del av en gruppe, aktivt motsetter seg eller ignorerer begrensningene de støter på av foreslåtte eller etablerte tekniske standarder, produkter, systemer eller lovens rammer. Lovløse brukere kan skape eller bruke nye hardware- eller softwaremodifikasjoner til eksisterende produkter, eller utnytte sikkerhetshull for uautorisert adgang til systemer. (Flowers 2008, 180: egen oversettelse)

Flowers' begrep handler hovedsakelig om produsent- og brukerforholdet hvor man, i tillegg til å dele informasjon, endrer et produkts funksjon eller tiltenkte bruk, og utnytter designerfeil for å angripe og bryte sikkerheten (Flowers 2008, 178). Dette kan igjen føre til at produsenter og ikke-lovløse forbedrer og innoverer for å imøtekomme de nye behovene (Flowers 2007, 3,7; Flowers 2008, 178). Det er ikke bare innenfor software det finnes lovløse brukere. All lovløs bruk er ikke lovløs innovasjon, mange er *lovløse brukere* som for eksempel laster ned musikk ulovlig, altså brukere som bruker lovløse innovasjoner (Flowers 2007, 5). Lovløs innovasjon kan omhandle for eksempel brukere som ulovlig frigir spillkoder, og hackere som bryter med en bedrifts intellektuelle eiendomsrett og utgjør en direkte trussel.

3.4.3 Innovasjonsgevinst

Innovasjon kan ha ulik nytte. von Hippel (1988) forsøker å se på det funksjonelle forholdet til innovasjon, for å kunne stadfeste hvem som er innovatøren, gjennom hva slags nytte en innovasjon har for innovatøren. En annen måte å se på innovasjon på, for å få en forståelse av nytten, i hvilken utstrakt grad innovasjon kan berøre og hvordan det kan oppfattes som en innovasjon, er gjennom å se på nytte etter tre distinksjoner: bedriftsøkonomisk/privatøkonomisk gevinst, samfunnsøkonomisk gevinst og velferdsmessig gevinst (Godø 2008, 22-25).

Bedriftsøkonomisk gevinst og/eller privatøkonomiske gevinst omhandler det å gi økt fortjeneste. Dette skiller den privatøkonomiske gevinsten fra en brukerinnovasjon, når brukerinnovasjon ikke trenger ha en finansiell gevinst, verken direkte eller indirekte for brukeren. I denne kategoriseringen innebærer privatøkonomisk- og bedriftsøkonomisk gevinst den finansielle avkastning man kan vente å få av en innovasjon, hvis man har investert i den (Godø 2008, 23). Ifølge undersøkelser foretatt av Edwin Mansfield går det frem at de samfunnsøkonomiske- og velferdsmessige gevinstene overgår den bedriftsøkonomiske avkastningen ved en rekke teknologiske innovasjoner (Mansfield m.fl. 1977, 144-166). Godø (2008, 24) viser til vaksinen som et eksempel. Vaksinene har gitt store samfunnsøkonomiske og velferdsmessige gevinster, men den bedriftsøkonomiske gevinsten har ikke nødvendigvis vært like stor.

En brukerinnovasjon kan gi både privatøkonomisk gevinst, bedriftsøkonomisk gevinst, men også samfunnsøkonomisk og velferdsmessig gevinst. Som von Hippel (2005, 2) skriver, kan brukerinnovasjoner øke den sosiale velferden, og dette er noe som i de fleste tilfeller trolig vil

påvirker den velferdsmessige- og samfunnsøkonomiske gevinsten. En innovasjon trenger derfor ikke gi direkte eller indirekte finansiell nytte for bedrifter eller privatpersoner, men kan gi en velferdsmessig og/eller samfunnsøkonomisk gevinst.

Denne fordelingen av gevinst kan også stille seg kritisk til kravet om spredning for å kvalifisere som innovasjon. Kanskje kan resultatet eller konsekvensen av en innovasjon spres, og gi en gevinst, uten at selve innovasjonen spres. Og kan dette allikevel kalles innovasjon? I denne oppgaven tar jeg utgangspunkt i at så lenge innovasjonen medfører en gevinst som spres til en gruppe, fordi den har dekt et behov, er det en innovasjon. Et eksempel kan være en paradigmeinnovasjon, som kanskje kun skjer i én organisasjon, men konsekvensen av denne innovasjonen kan ramme mange kunder i positiv forstand.

3.5 Oppsummering

Innovasjon er et fenomen som ikke bare representerer tiltak for å øke konkurranseevne og øke markedsandeler for organisasjoner, eller noe som skal gi finansiell nytte. Innovasjon kan også være tilpasningstiltak i forhold til ulike faktorer som påvirker miljøet og omgivelsene en organisasjon opererer eller befinner seg i. I tillegg til at det kan være en løsning på et problem organisasjoner står overfor. Innovasjon blir ofte drevet frem av behov, dette blir kalt behovstrekk, og kombineres ofte med det som kalles kunnskapsdytt.

Det er ikke bare produsenter som innoverer, men også brukere. Brukere har ofte ikke finansielt utbytte som motivasjon for innovasjonen sin. Brukere er alle som innoverer som ikke har en direkte eller indirekte nytte av å *selge* innovasjonen, men en direkte nytte av å *bruke* den. Kriminelle kan også være brukere, som kan påvirke andres innovasjoner og de kan innovere selv, dette kalles lovløs innovasjon. Økt informasjonstilgang gjennom økt bruk av data- og nettverksteknologi medfører flere brukerinnovasjoner, noe som øker den sosiale velferden. Innovasjoner kan medføre ulike gevinster som privat- og bedriftsøkonomiske, samfunnsøkonomiske og velferdsmessige gevinster.

4.0 Forskningsmetode

I denne oppgaven forsøker jeg å svare på problemstillingen: *Hvordan kan internettkriminalitet være en pådriver for innovasjon i ikke-kriminelle organisasjoner?* Denne problemstillingen stiller et *hvordan*-spørsmål. Dette vil ofte medføre at mest passende forskningsmetode er casestudie (Yin, 2009, 2). Denne metoden kan anvendes til å belyse og gi kunnskap om fenomener på mange ulike nivåer (ibid., 4). Jeg anser dette som den mest passende metoden å anvende i denne oppgaven, fordi formålet er å få mer kunnskap om internettkriminalitet (IK) som et fenomen som kan være en medvirkende årsak til innovasjon på ulike måter i ulike ikke-kriminelle organisasjoner. Jeg anvender komparativ casestudie på fire helt ulike norske ikke-kriminelle organisasjoner. De har alle til felles at de på en eller annen måte har blitt påvirket av eller har arbeidet med kriminell internettaktivitet på en måte som har medført innovasjon. En komparativ casestudie er en metode hvor man anvender flere caser for å illustrere forskjeller og likheter mellom dem (Ragin og Amoroso 2011, 146). Gjennom denne metoden forsøker jeg å dra en felles konklusjon ut fra de ulike og sammenfallende funnene casene gir (Yin 2009, 176-177). Dette vil bidra til å styrke oppgavens validitet og reliabilitet.

4.1 Datagrunnlag

I denne oppgaven har jeg samlet data gjennom undersøkelser ved søk på Internett og litteratursøk, samt dybdeintervjuer. Dybdeintervjuene har en sentral plan i analysen, derfor skal dette forklares nøye nedenfor.

4.1.1 Valg av case

Min utvalgsstrategi var strategisk utvelging, der casene og informantene ble valgt på bakgrunn av at de representerer den empiriske virkeligheten jeg ønsker å illustrere for å belyse problemstillingen (Johannessen, Kristoffersen og Tufte 2004, 109). Felleskravet var at alle casene skulle ha innovert som følge av IK, mens det var ulike krav til hva slags innovasjon og organisasjon hver enkelt case skulle være. Ikke-caseinformantene, to informanter utenfor casene som bidro med generell kunnskap om IK, ble valgt ut fra sin kompetanse og sitt yrke. Formålet med å velge fire ganske ulike organisasjoner i casene var å påvise at samme fenomen, IK, kan drive frem innovasjon på ulike måter. Dette vil si at det var forventet resultater som både var ulike og like (Yin 2009, 54). Selve enkeltcasene vil vise en forskjell, men at det er en overordnet fellesnevner, IK, slik at ulikhetene viser bredden i

hvordan IK kan ramme ikke-kriminelle organisasjoner og dermed være en pådriver for innovasjon.

Bakgrunn for valg av antall caser er basert på at det var fire forskjellige typer innovasjoner jeg på forhånd kunne tenke meg å illustrere, og som det var realistisk å kunne gjennomføre innenfor oppgavens gitte rammer. Jeg tror ikke de fire casene er uttømmende - jeg forsøker å illustrere det potensielt omfattende og store ved problemstillingen gjennom noen få. De fire casene viser en bredde, som samtidig kan få leseren til å innse mulighetene for mange andre potensielle caser til videre forskning. Samt at det gir et datagrunnlag for å kunne drøfte problemstillingen.

4.1.2 Valg av informanter

For å velge ut potensielle informanter startet jeg med å liste opp norske organisasjoner som jeg tenkte kunne være potensielt passende caser i forhold til å ha innovert som følge av et IK-forhold. I dette arbeidet anvendte jeg medier, bekjente og nøkkelinformant. Jeg begynte med å kontakte potensielle caseorganisasjoner ved å kontakte personer jeg fant i hver organisasjon, som jeg antok ville være personer med kunnskap på feltet, og som hadde noe myndighet i organisasjonene. Denne identifiseringen ble gjort ved undersøkelser på blant annet organisasjonenes hjemmesider. Første kontakt ble i hovedsak gjort gjennom en informativ e-post, hvor jeg presenterte meg og forklarte hva det gjaldt (Dunn 2010, 112-113; Yin 2009, 73). Dette førte til intervju eller ingen svar. Jeg valgte å ringe noen potensielle informanter som ikke hadde svart på e-post, eller hvor jeg ikke var sikker på hvem jeg burde henvende meg til i organisasjonen. Dette førte til både negativt og positivt svar. I en periode var jeg litt bekymret for om jeg ville klare å få inn nok data gjennom dybdeintervjuer, da det å få informanter var en større utfordring en først antatt.

De som ønsket å stille opp, var veldig positive og så sammenhengen med problemstillingen klart. Det var tydelig at disse visste hva innovasjon kunne innebære, og hadde tanker rundt aspekter ved problemstillingen på forhånd. De var også godt forberedt til intervjuene, og hadde gjort seg tanker om spesifikke innovasjoner i organisasjonen hvor IK hadde vært en medvirkende årsak. Dette styrket i større grad min tro på at kvalitativ casemetode var den mest passende, så tidlig i forskning rundt dette fenomenet. Dette fordi denne oppgaven tydeliggjør hva innovasjon kan være, og hvordan IK kan være en pådriver for casene. Det

viste også at dette er et sensitivt tema, og i mye større grad enn det jeg hadde vurdert det til å være før jeg startet med å kontakte potensielle informanter.

Jeg ser tre mulige årsaker til at det var særlig utfordrende å få informanter: Det ene kan rett og slett være at jeg ikke var viktig nok, og at min henvendelse druknet i mailboksen. En annen grunn kan være at de ikke skjønner at organisasjonen kan ha innovert som følge av IK, noe som kanskje også har med forståelsen av innovasjonsbegrepet å gjøre. Kanskje kunne jeg formulert meg tydeligere, eller valgt andre begreper i mine henvendelser. En tredje grunn kan være, noe jeg er sikker på også forekom etter en spesifikk opplevelse med en potensiell caseinformant, at de anser emnet om IK som så sensitivt at de ikke var interessert i å la seg intervjue. Dette kan kanskje komme av at de fryktet at de ville fremstå som en organisasjon med dårlig sikkerhet eller mye angrep. Andre metoder, som for eksempel kvantitativ spørreundersøkelse, ville kunne gjort det enda mer utfordrende å få informanter til å stille opp eller få svar. Dette kan man for eksempel se fra undersøkelser som delvis berører samme tema, se for eksempel Mørketallsrapportenes™ svarprosent.

Et annet aspekt ved informantene i denne oppgaven, og som ikke var kjent for meg da jeg avtalte de fleste intervjuene, er at flere av informantene kjente til hverandre gjennom sikkerhetsmiljøet i Norge. Dette er kanskje ikke så rart, for dette er et relativt lite miljø, og flere av informantene er ildsjeler rundt emnet sikkerhet og internettkriminalitet. Disse individene er av dem som er forkjempere for aspekter rundt IK og sikkerhet, og de er ansatt i organisasjoner med særlig mye kunnskap om IK og IT-sikkerhet og med gode praksiser i organisasjonene.

Seleksjonsbias

Strategisk utvalg, samt at informantene jeg til slutt endte med representerer miljøet hvor man ønsker å være åpen og være forkjempere for sikkerhet og bekjempelse av IK, gjør at oppgaven har seleksjonsbias (Ragin og Amoroso 2011, 29). Men ettersom dette var et mye mer sensitivt tema enn først antatt, måtte jeg benytte meg av de informantene som ønsket å stille opp, og som dermed så sammenhengen med problemstillingens tema. Ellers hadde jeg trolig ikke kunnet svare på problemstillingen, og i hvert fall ikke kunnet bruke case og dybdeintervju som metode, og dermed ville oppgaven trolig ikke fått samme forklaringsevne som de empiriske casene gjennom dybdeintervju gir. Allikevel tror jeg ikke at casene mine illustrerer noe mindre valid data, men representerer organisasjoner som er klar over den

påvirkningen IK har på deres egen organisasjon og deres brukere og kunder. Hensikten er å påvise at IK kan være en pådriver for innovasjon, dette uavhengig av om dette gjelder i organisasjoner som kanskje er mer bevisst rundt IK enn den vanlige organisasjon i Norge. Innovasjonene deres er i like stor grad drevet frem av IK, og oppgaven forsøker ikke å dekke alle mulige aspekter ved hva slags innovasjoner og hvilket forhold det er mellom innovasjonene og IK, og heller ikke alle ikke-kriminelle organisasjoners mulige innovasjonsforhold med IK. Det er kun ment som et bidrag til å se at IK *kan* være en pådriver for innovasjon i ikke-kriminelle organisasjoner, og at det kan skje på ulike måter og i ulike organisasjoner ved å gi noen empiriske eksempler gjennom caseanalysene. I tillegg gir det et empirisk grunnlag for å drøfte mer overordnet hvordan IK kan være en pådriver for innovasjon i ikke-kriminelle organisasjoner. Oppgaven kan bare si noe sikkert om de fire casene som kommer frem i denne oppgaven. Allikevel er denne seleksjonsbiasen en svakhet i forhold til å kunne si noe om hvorvidt problemstillingen kan omhandle andre typer organisasjoner. Derfor vil det være nyttig for fremtidige undersøkelser på dette å innhente empiri fra enda flere og mer ulike organisasjoner, hvor bevisstheten rundt IK kanskje ikke er like stor som hos mine informanter.

4.1.3 Dybdeintervju

Det ble gjennomført seks semistrukturerte dybdeintervju av informanter i løpet av september og oktober 2012 (se vedlegg 1). Dybdeintervju er blant de vanligste datainnsamlingsmetodene i kvalitativ metode innen samfunnsvitenskapelig forskning (Ragin og Amoroso 2011, 122). Dybdeintervju forsøker å avdekke betydning og mening gjennom å undersøke ideer og bygge forhold og koblinger med informantene (ibid.). Dette gjøres ved å ta utgangspunkt i informantenes innfallsvinkel og synspunkter rundt det som i hovedsak undersøkes (ibid.).

Informantene var personer som var koblet mot casene og individer som har spesielt god kunnskap om IK i Norge. Dette medførte anvendelse av forskjellige semistrukturerte intervjuguider (Dunn 2010, 104-105, 110). Intervjuguiden til caseinformantene var den samme og hadde blant annet spørsmål knyttet til den konkrete innovasjonen og organisasjonen (se vedlegg 2). Intervjuguiden til informantene utenfor casene var mer generelle rundt IK i Norge og deres tanker rundt hvordan de opplever IK som en potensiell pådriver for innovasjon og teknologisk utvikling. Intervjuene var ikke veldig låst til intervjuguiden, men spørsmål ble stilt ettersom de falt naturlig under intervjuet og som en forsikring om at nødvendig informasjon ble tatt opp. Intervjuene skulle ta cirka 60 minutter,

men flere av informantene ga beskjed på forhånd om at de satte av opp mot halvannen til to timer. Disse ga da gjerne innføring i sine spesialinteresser i forhold til IK i tillegg.

Under intervjuene ble det hovedsakelig anvendt lydopptaker, og intervjuene ble i ettertid transkribert (Dunn 2010, 118-119). Samtidig tok jeg noen notater underveis i intervjuet. Dette fungerer blant annet som en forsikring i tilfelle tekniske problemer skulle oppstå med opptakeren (ibid., 119-120). Det var allikevel ett unntak hvor opptaker ikke ble anvendt, da dette intervjuet befant seg i en organisasjon hvor sikkerhet er svært høyt prioritert. Tillatelse om bruk av lydopptaker ble avklart før intervjuene startet (ibid., 114).

Før hvert intervju startet, ble det skrevet under på en avtale om informert samtykke mellom informantene og meg selv (se vedlegg 3) (Dowling 2010, 29). I denne kontrakten fremgikk det hva slags rettigheter informanten har i forhold til å delta i undersøkelsen.

4.1.4 Intervjusituasjon

Intervjuene foregikk i informantenes arbeidslokaler. Dette var et passende sted, da det gjorde det praktisk for informantene. Samtidig var ikke intervjuinnholdet av slik karakter at jeg vurderte det som at disse lokasjonene ville påvirke negativt hva slags informasjon som ble gitt av informanten. Før selve intervjuet startet, ble formelle ting ordnet, som avtale om informert samtykke og klarering om lydopptaker skulle anvendes eller ikke (Dowling 2010, 29; Dunn 2010, 114). Jeg begynte alle intervjuene med å fortelle litt om oppgaven og hva jeg var ute etter, og i de aller fleste tilfeller medførte dette at informantene begynte å prate av seg selv, og de svarte på mange av spørsmålene mine uten at jeg trengte å stille dem. Jeg forsøkte også å få en god *rapport* under intervjuet, som omhandler det å forstå hvilken verdensforståelse informantene har, og kommunisere dette gjennom blant annet kroppsspråk (Dunn 2010, 112-118). Hensikten med dette er at informantene skal føle seg komfortable og i størst mulig grad åpner seg, slik at data blir mest mulig korrekt (ibid.).

Jeg holdt avtalt tid i intervjuene, som i all hovedsak var på 60 minutter, utenom de to der informantene selv hadde et ønske om et lengre møte. Det var ett unntak. Dette var i tilfellet hvor jeg ikke kunne ta lydopptak, noe som medførte at jeg måtte ta mer nøyaktig notater underveis. Vi gikk 15 minutter over, men dette ble klarert med informanten da vi nærmet oss forhåndsavtalt tidsslutt. Jeg kunne selvfølgelig ha avsluttet i tide, men dette ville medført at jeg måtte ha fått denne informasjonen av informanten siden, eller ikke fått den i det hele tatt. Jeg beklaget i tillegg dette overfor informanten etter intervjuets slutt, og i en e-post siden.

De aller fleste informantene var veldig engasjerte og pratsomme, noe som medførte veldig mye informasjon og mye transkribering i etterkant av intervjuene. Jeg brukte i gjennomsnitt cirka fem til seks timer på transkribering per intervju. Jeg førte også en forskningsdagbok, hvor jeg noterte opplevelser og hvordan jeg følte intervjuetsituasjonen gikk, rett etter hvert enkelt intervju. Dette gjorde jeg for at jeg skulle tenke over og vurdere situasjonen og ting som eventuelt kom opp under intervjuet, samt min egen posisjon. Dette er en metode som også er hensiktsmessig i forhold til den refleksive prosessen under forskningsarbeidet (Dowling 2010, 31).

Alle transkriberingene og alt opptaksmaterialet ble tatt godt vare på og har under hele prosessen vært utilgjengelig for alle utenom meg selv. Dette er generelt viktig for å ivareta konfidensialiteten til informantene (Dowling 2010, 28-29). I mitt tilfelle var dette særlig viktig fordi en av informantene som representerte en caseorganisasjon ikke hadde bestemt seg for om de ønsket å fremstå som anonym i oppgaven eller ikke. Dessuten hadde jeg lovet alle informantene godkjenning av sitater før publisering, og ved å slurve med oppbevaring av transkribering og opptak har man mistet noe av kontrollen på mulige publiseringer fra tredjeparter som eventuelt kunne få tak i dette materialet.

Alle sitater av informantene som jeg anvender i oppgaven, ble sendt til godkjenning. Dette ga informanten anledning til å sørge for at jeg ikke hadde misforstått, og eventuelt til å trekke sitater. I tillegg fikk det forhåpentligvis informantene til å føle seg komfortable med hva som skulle med i oppgaven, særlig med tanke på at de ikke fremstår som anonyme i oppgaven. Det var i denne perioden den ene informanten og organisasjonen også tok avgjørelsen på om de skulle fremstå som anonyme.

4.2 Koding og analyse av datamateriell

Kodingsprosessen er en del av analysen, når man gjennom kodingsarbeidet samtidig analyserer datamaterialet (Cope 2010, 284). Dette er en formell prosess omkring noe vi bevisst og ubevisst kontinuerlig gjør i vår tilværelse (ibid., 292-293). Min kodingsstrategi var å lage det man kaller en kodebok, en liste over de temaer jeg ønsket å kode datamaterialet etter (ibid., 285). I mitt tilfelle var det mer snakk om en perm enn en bok. I denne permen samlet jeg alle utskriftene av transkriberingen fra intervjuene, samt noen rapporter funnet under internettsøk. I tillegg laget jeg på forhånd og underveis i datainnsamlingen en liste over temaer jeg ønsket å kode etter. Denne vokste også etter at datainnsamlingen var ferdig og jeg

hadde hørt og lest gjennom intervjuene igjen. Noen av temaene ble også sjaltet ut etterhvert i analysearbeidet (ibid., 288). I kombinasjon med dette laget jeg en slags datamatrise, for å lette analysearbeidet i forhold til casene. Jeg valgte å kode manuelt. Dette gjorde jeg ved å fargekode temaer med ulike fargetusjer, skrive i margen på utskriftene og anvende fargelapper. Dette synes jeg fungerte godt. Deretter begynte jeg å anvende fargekodene og legge inn under større temaer, og jeg anvendte også oppgavedisposisjonen min og videreutviklet denne i dette arbeidet.

Jeg hadde to former for intervjumateriale: caseintervjuene og ikke-caseintervjuene. Ikke-case-intervjuene var intervju med informanter som ikke hadde noe med de konkrete casene å gjøre, men var intervju om IK mer generelt. I tillegg inneholdt caseintervjuene deler som tenderte mer mot ikke-caseintervjuene også. Dermed anvendte jeg bricolage som analysemetode. Dette er en metode hvor man fritt kan bevege seg mellom ulike metoder, noe jeg synes var best i mitt tilfelle (Kvale 2007, 115-117). Dette fungerte bra, fordi jeg fra starten av datainnsamlingsperioden i stor grad visste hvordan jeg ville gjøre arbeidet og hva jeg var ute etter.

I kodings- og analysearbeidet må man være bevisst på hvilket perspektiv og hvilken bakgrunn man har, og hvordan dette påvirker arbeidet og det ferdige resultatet gjennom hvordan dette farger våre tolkninger (Cope 2010, 292). Jeg har derfor i oppgaven bevisst satt av stor plass til innovasjon og IK, i den hensikt å gjennom teorier og litteratur å analysere casene, for gjennom dette å argumentere for at casene illustrer en form for innovasjon i kapittel fem. Dette fordi jeg kommer fra et perspektiv hvor innovasjonsbegrepet favner mye som enkelte innovasjonsteoretikere ikke er enige i. I tillegg ble case-analysene og sitater av informantene sendt til sjekk, slik at jeg styrker reliabiliteten til oppgaven. Jeg forsøkte også å være bevisst hvilken rapport det hadde vært under intervjuet og andre ting som kunne påvirket svarene jeg fikk under intervjuet, ved å lese gjennom forskningsdagboken min under dette arbeidet (Dowling 2010, 31; Dunn 2010, 112).

4.3 Validitet og reliabilitet

4.3.1 Validitet

Validitet omhandler i hvilken grad man reelt har undersøkt det oppgaven var ment å undersøke, og i hvilken grad en forskningsundersøkelses resultatet kan benyttes til å trekke

gyldige slutninger (Johannessen, Kristoffersen og Tufte 2004, 228; Ragin og Amoroso 2011, 23; Yin 2009, 40). Man deler validitet gjerne opp i intern- og ekstern validitet.

Intern validitet

Intern validitet innebærer blant annet at en forsker ikke kan konkludere med at en årsakssammenheng finnes på grunn av en viss variabel hvis den i virkeligheten skyldes en annen variabel (Yin 2009, 42-43). Min komparative casestudie tar sikte på å være forklarende. Hovedfokuset i oppgaven er ikke å forklare hvorfor IK førte til innovasjon i den konkrete caseorganisasjonen, men å se på og forklare overordnet og felles for de fire casene hvordan IK kan ha fungert som en pådriver for innovasjonene. Dette betyr at jeg ikke tar sikte på å forklare alle mulige faktorer som også kan ha påvirket de konkrete innovasjonene i casene. Jeg tar det som en forutsetning at det er andre faktorer som har vært med å påvirke at de konkrete innovasjonene ble til og at de tok den form de gjorde. Dette kan være alt fra mennesker til kunnskap og tilfeldigheter for å nevne noe. Casene tar sikte på å vise hvordan IK har vært en medvirkende årsak for ulike innovasjoner i ulike organisasjoner, og at uten IK hadde kanskje ikke innovasjonen blitt til eller tatt nøyaktig den form den har gjort. Ved hjelp av å beskrive hvordan undersøkelsen er blitt gjennomført og planlagt, og en klar idé om hva og hvordan jeg skulle undersøke fenomenet, ved drøfting av funnene opp mot eksisterende teori, i tillegg til å ha anvendt den forskningsmetoden jeg anser som mest hensiktsmessig for problemstillingen, vil jeg hevde at de kausale slutningene er holdbare. Ifølge Johannessen, Kristoffersen og Tufte (2004, 128) kan også validiteten styrkes ved å tilbakeføre resultatene til informantene, noe jeg delvis har gjort ved å få dem til å sjekke casefremstillingene og sitatene.

Ekstern validitet

Ekstern validitet omhandler i hvilken grad funnene ervervet gjennom den konkrete caseundersøkelsen kan generaliseres, det vil si ha gyldighet utenfor de undersøkte casene (Yin 2009, 43). Generelt blir caseundersøkelser, særlig enkeltcaseundersøkelser, kritisert for ikke å kunne gi generaliseringsgrunnlag på grunn av få forskningsobjekter (ibid.). Innvendingene blir imøtegått av tilhengere av casemetoden, som skriver at casestudiet kan gi *analytisk* generaliseringsgrunnlag (ibid.). Analytisk generalisering innebærer at man forsøker å anvende en større teori som de empiriske funnene kan kobles opp mot, og på denne måten kan den konkrete casen for eksempel bidra til å identifisere caser som resultatet kan generaliseres til ved at man allerede har en hypotese å ta utgangspunkt i for utvalg av case i lignende

undersøkelser (ibid.). I denne oppgaven benytter jeg meg av flere caser med ulike organisasjoner og innovasjoner for nettopp å kunne bevise en felles årsakssammenheng mellom IK og innovasjon. På denne måten illustrerer jeg den bakenforliggende variabelen, IK, opp mot forskjellige organisasjoner hvor samtlige har medført en form for innovasjon – en avhengig variabel.

Funnene i denne undersøkelsen kan ikke generaliseres til alle ikke kriminelle-organisasjoners innovasjoner, og heller ikke til alle lignende organisasjoner som casene i oppgaven, fordi jeg i mitt utvalg bevisst har valgt caser hvor årsakssammenhengen er den samme, selv om casene på mange måter er ulike. Men man kan kanskje anta at lignende årsakssammenheng mellom IK og ikke-kriminelle organisasjoners innovasjoner kan forekomme i andre organisasjoner, hvor både type innovasjon, type organisasjon og andre bakenforliggende medvirkende årsaker vil kunne være ganske sammenfallende med mine caser, men også annerledes enn i denne oppgavens caser.

4.3.2 Reliabilitet

Reliabilitet, eller pålitelighet (Johannessen, Kristoffersen og Tufte 2004, 227), omhandler i hvilken grad man vil få samme resultat i undersøkelsen om studiet utføres igjen (Yin 2009, 45), det vil si replikasjon. Det innebærer at det er nøyaktig samme undersøkelse som skal gjentas, og at man følger samme prosedyrer som første gang, men at en annen forsker skal kunne gjennomføre undersøkelsen, og komme frem til samme resultat (ibid.). For å styrke reliabiliteten har jeg forsøkt å dokumentere prosedyrene mine gjennom arbeidet. Dette har jeg gjort ved blant annet å anvende en forskningsdagbok hvor opplevelser og tanker fra datainnsamlingen ble notert ned slik at de ikke skulle bli glemt, jeg anvendte lydopptaker i de fleste intervjuene og transkriberte dette materialet, og jeg sendte casene til de relevante intervjuobjektene og sitater til gjeldene informant, slik at de kunne sjekke at det ble riktig benyttet og godkjenne dette. I tillegg har jeg lagt den semistrukturerte intervjuguiden anvendt i case-intervjuene i vedlegg. Hvem informantene er, kommer også tydelig frem utover i oppgaven.

Samtidig er det slik at den dynamikken og eksakt hva en informant sier til forskeren, vil variere etter personen som intervjuer (Dunn 2010, 112-114). Dette kan bli et problem med henblikk på repliserbarhet av en undersøkelse, særlig på grunn av bruk av dybdeintervju til datainnsamling. I tillegg ble det i flere av intervjuene slik at det ikke var nødvendig for meg å

stille mange av spørsmålene i intervjuguiden, fordi informantene var veldig entusiastiske og hadde tenkt ut på forhånd hva jeg ville være interessert i. Slik entusiasme kan kanskje komme an på dagsformen til informantene, og det er en mulighet at informantene ikke alltid vil være like selvgående, og da kan informasjon jeg ikke ville ha tenkt på å stille spørsmål om, kanskje ikke komme frem under intervjuet. Dette kan være en svakhet ved semistrukturert intervju, fordi jeg i større grad åpner for å la informanten snakke og forholder meg mest til overordnede spørsmål som forhåpentligvis leder videre. Allikevel er det trolig at den grunnleggende historien i casene ville gitt samme resultat, og de generelle intervjuene ville ledet til lignende sitater og essensen ville vært den samme.

Jeg har også anvendt manuell fargekoding, og min logikk og mitt perspektiv vil kanskje avvike fra en annen forskers, og dette kan påvirke hvordan man koder og tolker dataen. Men fordi jeg har fått informantene til å sjekke materialet, som jeg direkte anvender i oppgaven, vil dette kunne styrke påliteligheten til min tolkning og analyse av datamaterialet.

4.4 Etiske refleksjoner

I dybdeintervju kan man få mye og sensitiv informasjon fra enkeltindivider, og både informasjonen og individene må derfor behandles etisk. De etiske retningslinjene jeg tar utgangspunkt i her er: informert samtykke, konfidensialitet, potensielle konsekvenser som følge av deltakelse i undersøkelsen, og min integritet som forsker (Kvale 2007, 25-30).

Som tidligere nevnt var det til alle intervjuene informert samtykke. Jeg fikk informantene til å skrive under på en kontrakt om informert samtykke, hvor deres rettigheter kom tydelig frem, og som jeg selv også underskrev. Konfidensialiteten bevarte jeg ved at jeg har tatt godt vare på lydopptak og datamaterialet fra intervjuene. Alt av datamaterialet destrueres ved oppgavens ferdigstillelse. Informantene har fått gjennomgå materialet slik det skulle fremgå i oppgaven før publisering, slik jeg lovet. Samt at den organisasjonen som ønsket å vurdere sin eventuelle anonymitet ut fra dette materialet fikk anledning til dette. Jeg tok på forhånd en vurdering av om jeg burde anonymisere organisasjonene og informantene, men anså ikke dette som nødvendig i forhold til hva og hvordan de empiriske funnene skulle benyttes i oppgaven. Jeg lot allikevel personene og organisasjonene ha det siste ordet i dette, da de best vet hvilke potensielle konsekvenser denne informasjonen kan ha for dem. Den eneste som før informantene fikk anledning til å gå over sitater og case-fremstillinger, var min hovedveileder

i hans arbeid med å veilede meg i oppgaveprosessen. Dette var informantene klar over på forhånd.

Under intervjusituasjonene opplevde jeg aldri at det var noen skjevhet i forhold til autoritet mellom informantene og meg som forsker, og jeg opplevde det som et forhold preget av gjensidig interesse og nytte av oppgaven (Dowling 2010, 32). Dette var profesjonelle folk som var interessert i temaet i oppgaven. Temaet gjorde det slik at jeg heller ikke så det som noe negativt at intervjuene foregikk på deres arbeidsplasser med tanke på hvordan dette påvirket svarene deres og negative konsekvenser dette kunne ha for dem, da det i hovedsak var dette arbeidet som gjorde det relevant å ha dem med som informanter fra starten av.

4.5 Oppsummering

I dette kapittelet har jeg raskt gått igjennom den metodiske fremgangsmåten i forhold til valg av komparativ casemetode, utvalgsstrategi og valg av informanter, intervjusituasjonen og koding og analyse av empirien. Jeg gikk deretter gjennom faktorer som kan ha påvirket validiteten og reliabiliteten i forhold til empirien, samt etiske refleksjoner rundt informantbehandlingen.

5.0 Caseanalyser

«They will accept the inevitable unpredictability and irregularity of the innovative or creative approach.» (Stacey 1992, 168)

I dette kapittelet vil jeg presentere og analysere casene som jeg anvender for å forsøke å illustrere innovasjonsdynamikk mellom internettkriminalitet (IK) og innovasjon i ikke-kriminelle organisasjoner. Kapittelet forsøker å svare på forskningsspørsmålet; *hva slags innovasjoner kan komme som følge av IK i ikke-kriminelle organisasjoner?*, ved å presentere, analysere og drøfte hver enkelt case opp mot innovasjonslitteraturen omtalt i kapittel tre, og koble det med litteraturen rundt IK omtalt i kapittel to.

Casene er fire ulike organisasjoner, som har innovert på ulike måter. Jeg forsøker etter å ha presentert organisasjonen og den konkrete innovasjonen, å typologisere og kategorisere innovasjonen gjennom å se på hva slags innovasjon det er og hvor jeg anser det som mest passende å plassere innovasjonen i innovasjonsrommet. Videre drøfter jeg hvorvidt det er en brukerinnovasjon eller en produsentinnovasjon gjennom å se på det funksjonelle forholdet til innovasjonen, hva slags behov den dekker og hvilken gevinst innovasjonen hovedsakelig medfører. Deretter drøfter jeg kort hva slags forhold og kobling det er mellom IK og den konkrete innovasjonen. Jeg analyserer og drøfter hver case for seg. Dette ser jeg som mest hensiktsmessig for å illustrere enkelte innovasjoner drevet frem av IK hvor casene er forskjellig fra hverandre. Jeg forsøker ikke gjennom denne fremstillingen å gå inn i selve innovasjonsprosessen ved de forskjellige innovasjonene.

I hver av de påfølgende casene illustrerer jeg fire forskjellige innovasjoner, som alle på en eller annen måte delvis er drevet frem av IK. De fire casene er:

- Case 1: Produktinnovasjon i Norman
- Case 2: Paradigmeinnovasjon i SpareBank 1
- Case 3: Metodeinnovasjon i Kripos
- Case 4: Ikke-profitt organisasjoninnovasjon, Underworld

Jeg har som nevnt anvendt kvalitativ metode og gjennomført dybdeintervjuer om fire ulike innovasjoner hos fire ulike organisasjoner. Det er kun data fra disse caserelevante intervjuene, som vil bli analysert og anvendt i dette kapittelet. Kilden til hver enkelt casefremstilling er

informanten presentert i innledningen til casen så lenge ikke annen referansehenvisning fremkommer, med unntak av siste underkapittel i hver casefremstilling, hvor innovasjonen blir analysert mot de teoretiske begrepene og litteraturen fra kapittel to og tre.

I slutten av dette kapittelet oppsummerer jeg funnene i to modeller. Den ene modellen er basert på Tidd og Bessant (2009, 22) sitt innovasjonsrom, hvor jeg har plassert caseinnovasjonene i innovasjonsrommet. Den andre modellen er en kombinasjon av de ulike kategoriseringene og typologiseringene anvendt i caseanalysene. I kapittel seks drøfter jeg funnene opp mot problemstillingen og annen relevant litteratur som kan forklare dynamikken på et mer overordnet og generelt nivå. I kapittel seks anvender jeg også empiri fra ikke-case intervjuene.

5.1 Case 1: Produktinnovasjon

I denne casen presenterer jeg sikkerhetsløsning som produktinnovasjon i Norman. Den konkrete innovasjonen er Norman SCADA Protection, som er utviklet i samarbeid med en kunde, og baserer seg på et tidligere produkt Norman har utviklet. Dette er en innovasjon rettet mot dataintegritetskriminalitet i form av tredjegenerasjons kyberkriminalitet, samt at det er en produsentinnovasjon med hovedsakelig en bedriftsøkonomisk gevinst. Casen baserer seg på et intervju med Bjørn Lilleeng, Technology Integration Manager i Norman.

5.1.1 Norman

Norman ASA er et firma som lager datasikkerhetsprodukter, og ble opprettet i Oslo i 1984. De er en av mange i dette markedet, men de har allikevel noen unike produkter som for eksempel Norman SandBox®. De tilbyr proaktiv teknologi mot ondsinnet programvare[10] (OP) for anvendelse i sikkerhetsprodukter og løsninger verden over. I den proaktive strategien har de flere hjørnesteinsprodukter for bekjempelse av internettbasert kriminalitet (Norman).

> *Det er veldig premissdrevet, markedet legger premisser for oss. Siden vi jobber med beskyttelse mot malware, og det blir generert cirka 80 000 nye eksemplarer av malware per dag, må vi stadig utvikle vår teknologi for å gi våre kunder beskyttelse mot denne stadig økende trusselen.*

Det er markedet som legger premissene for hva Norman skal utvikle og hvordan de skal jobbe. Et eksempel er den økende graden av OP, hvor det dukker opp gjennomsnittlig 80 000 nye hver eneste dag. Dermed må de jobbe for å kunne beskytte kundene sine mot den stadig økende OP trusselen. Derfor har Norman nå maskinell behandling av de fleste OP, men i noen tilfeller må det menneskelig ressurser til. De erkjenner at de stadig må finne bedre teknologi, som blant annet kan finne ukjent OP.

«*Spesielt utfordrende er det å ligge i forkant, utvikle teknologi som greier å skille ukjente eksemplarer av malware fra legitim programvare. Her ser vi altså etter generelle kriterier for å skille det dårlige fra det gode, i motsetning til det å benytte signaturer for enkeltfiler.*»

[10] **Ondsinnet programvare (OP)**, kalt malware/malicious software på engelsk, er en fellesbetegnelse for all uønsket programvare (Rush m.fl. 2009, 94).

5.1.2 Norman Network Protection

Norman hadde en stor kunde i Danmark, en stor produsent av meieriprodukter. Dette betydde at kunden hadde et produksjonsmiljø som besto av mange PCer. Disse PCene drev prosesser som for eksempel å få melkekartonger til å bli fylt opp. Disse maskinene var virksomhetskritiske for at produksjonen av produkter skulle fungere normalt. Det var helt kritisk at ingen av disse maskinene ble infisert av virus, men de var typisk koblet til Internett på en eller annen måte. Denne kunden hadde vært kunde hos konkurrenter av Norman tidligere. Det typiske svaret på deres behov var å isolere normalprogramvare, men dette hadde de allerede testet med både konkurrenter og Norman, med det resultat at det medført for mye treghet som ikke var en aktuell løsning for de kritiske prosessene som de berørte maskinene drev. Dette resulterte i at Norman og kunden satte seg sammen for å finne en god løsning på kundens problem. Kunden foreslo at Norman i stedet for å ha et system på hver maskin heller skulle ha systemet på ett felles punkt før det kom til maskinene, inn fra Internett. Med dette i tanken dro Norman og utviklet det som i dag heter Norman Network Protection (NNP).

NNP er en dedikert boks, en virtuell sandboks Norman utviklet på tidlig 2000-tallet. NNP analyserer alt som kommer inn gjennom Internett i en virtuell sandboks, slik at mistenkelige programvarer ikke når maskinene før det er grundig analysert og godkjent som ikke-truende. Denne løsningen er mye bedre å holde kontroll på når det er flere maskiner som skal beskyttes, og den blir oppdatert med nye malwaresignaturer hele tiden.

«*[…] vi lager hva pokker vi vil av programvare, men vi må ha en idé, en grunn til å gjøre det.*»

5.1.3 Norman SCADA Protection

Norman hadde en annen stor kunde innen maritime løsninger, Kongsberg Maritime. Denne kunden kjørte det som kalles SCADA-nettverk, som vil si PCer som har installert en programvare som skal kontrollere og overvåke kontrollsystemer.
SCADA[11] har virksomhetskritiske oppgaver og noen ganger samfunnskritiske oppgaver, et eksempel kan være kontroll over gradene på kjølevann i et atomkraftverk. Fordi SCADA

[11] **SCADA**, supervisory control and data acquisition, er et datasystem ofte anvendt til kontrollering og overvåkning av utstyr og anlegg (Webopedia™). SCADA samler inn og analyserer sanntidsinformasjon, og har ofte kritiske (også samfunnskritiske) oppgaver og kommer i ulike kompleksitetsgrader og anvendes i mange forskjellige industrier (ibid.).

kontrollerer kritiske maskiner, er det svært alvorlig hvis uvedkommende kommer inn i SCADA-nettverket og overstyrer det. Det kan medføre manipulering av programmer slik at de oppfører seg annerledes eller totalt saboterer det, slik tilfellet var i Irans atomutviklingsprogram.

Kunden sa at NNP er en slik løsning de hadde behov for, da de heller ikke ønsket lokale programvarer på hver enkelt PC. De trengte superraske maskiner, og ønsket ikke noe som kunne forstyrre maskinen og dens funksjonalitet, særlig med tanke på oppdateringer som følger med sikkerhetssystemer. De testet dette ut, men fortalte at de ønsket noe mer, da de ikke var sikre på om NNP løsningen alene var nok for å dekke deres behov. For det var et annet problem. Maskinene måtte, som alt annet med software, oppdateres. Maskinene var koblet til Internett hvor NNP kontrollerte, men oppdateringene ble som oftest gjort ved at personer gikk rundt med USB-minnepinner fra maskin til maskin og oppdaterte. Men her var det plutselig en menneskelig faktor, mennesker var et mellomledd i oppdateringene. Menneskelig svikt er dessverre et stort og reelt problem. Det er fort gjort å glemme til hva og hvor USB-minnepinnen var i går. Denne USB-pinnen kan være en smittebærer, hvis den har blitt brukt med noe som er lastet ned fra Internett.

Norman er ikke ekspert på SCADA, men eksperter på sikkerhet. Kunden derimot er ikke eksperter på sikkerhet, men eksperter på SCADA. De ble enige om å møtes en dag i april 2011, hvor Norman skulle representeres gjennom fem ansatte med forskjellig kompetanse. Det var utviklere, salgsdirektør, prosjektledere, det var eksperter. Kunden kom også med fem personer, teknologieksperter, kommersielle eksperter og industrieksperter. De satte seg ned og delte ideer og kunnskap, og hver person på møtet hadde kritisk kompetanse som medførte det spesifikke resultatet. Klokken tre denne dagen, etter et svært kreativt møte, gikk de hvert til sitt, og visste nøyaktig hvordan SCADA-systemene skulle beskyttes.

Resultatet ble et produkt som er en liten vri på NNP, gjennom den nye kompetansen de fikk på møtet. De analyserte kundens ønskede funksjonalitet og la til noen egenskaper i NNP, som dermed gjorde den spesielt velegnet for Norman SCADA Protection (NSP). De la til en komponent med den funksjonalitet, at den godkjenner USB-pinner som man ønsker å benytte for å oppdatere systemene. Denne komponenten sjekker at USB-pinnen er ren og fri for OP og godkjenner den i 30 minutter, slik at man må gå direkte for å oppdatere systemene med USB-pinnen før den slutter å fungere i maskinene. De har gitt USB-pinnen en utløpsdato slik

man gir ferskvarer. På denne måten blir det så å si umulig å forurense USB-pinnen i mellomtiden, ved å bruke den på private og mulig infiserte produkter.

«*Slik at en ting er altså å bruke den teknologien vi allerede har utviklet til analyse. Noe annet er at vi videreutvikler selve verktøyene vi bruker, og tilpasser dem til nye elementer i trusselbildet.*»

5.1.4 Mulighet i andres behov

Norman har et innovasjonsforum hvor alle i organisasjonen kan bidra, en systemutviklingsavdeling og en forretningsutviklingsavdeling, som jobber med å utvikle nye ideer og løsninger som kan bli produkter som kan selges. Men Norman beskriver også at god kontakt med kunder gjør at de fanger opp ideer til produkter og løsninger det er behov for.

> *Man må ha kompetanse fra forskjellige steder, både fra sikkerhetssiden, men også fra industrisiden. Slik at industrien, som ligger helt i forkant av utviklingen innen sitt felt, og vet nøyaktig hva som skjer der, kan gi oss tilbakemeldinger om teknologi som må beskyttes. Og da benytter vi vår sikkerhetskompetanse til å finne hva som skal til for å beskytte disse komponentene. Så jeg vil si at SCADA Protection-produktet er et skoleeksempel på hvordan sikkerhetsprodukter kan utvikles gjennom et samarbeid mellom oss og en industripartner.*

«*Ikke sant, det skaper mye, det gir grobunn for innovasjon og kreativitet.*»

5.1.5 Innovasjonstype

Innovasjonseksempelet er NSP, men NNP ble også introdusert for å vise at dette var en videreutvikling av et tidligere produkt for å kunne tilfredsstille kunders utviklende og endrede behov. Begge innovasjonene vitner om en organisasjon som utnytter åpen innovasjon som en produktinnovasjonsstrategi (Chesbrough 2003, 2006). Norman SCADA Protection er en produsentinnovasjon (von Hippel 1988, 3; 2005, 3), men hvor man gjennom åpen innovasjon har benyttet seg av ledebrukere for å utvikle et produkt som svarer på kunders behov (von Hippel 2005, 4). Dette er en produsentinnovasjon på grunn av det funksjonelle innovasjonsforholdet fordi den direkte nytten innovasjonen gir for organisasjonen Norman er gjennom salg av løsningen (von Hippel 1988, 3; 2005, 3). Det skal nevnes at Norman ikke selger NSP til olje- og gassektoren, dette er det Kongsberg Maritime som gjør, men de får en prosent av salget. De kan derimot selge det til andre SCADA-brukere utenfor denne sektoren. Å tjene penger gjennom en slik avtale som Norman har med Kongsberg Maritime, er også noe som omtales innenfor åpen innovasjonslitteraturen (Chesbrough 2003, 37).

Innovasjonen gir en bedriftsøkonomisk gevinst i form av direkte inntekter for Norman gjennom salg og økt markedsandel (Godø 2008, 23-24). Dette er hovedgrunnen til at Norman har innovert. Men allikevel gir innovasjonen NSP en velferdsgevinst gjennom at det er en kriminalitetsbekjempende- og anti-terrorbekjempende innovasjon (ibid.), som minimerer skadeomfanget til OP rettet mot SCADA-nettverk. Dette gir en gevinst for de som anvender NSP, som dermed slipper de økonomiske utgiftene som kan komme som følge av å bli rammet av OP og de ikke-økonomiske negative konsekvensene slike angrep kan medføre for organisasjoner og deres brukere og virksomhetsoppgaver igjen. Den samfunnsøkonomiske gevinsten NSP kan gi (ibid.), er at færre blir rammet av IK og OP spesielt, noe som dermed minimerer samfunnskostnadene ved behandling av anmeldelser og etterforskning, og eventuelt samfunnskostnadene som kan komme som følge av at SCADA anvendes i flere samfunnskritiske systemer.

Denne innovasjonen er en produktinnovasjon, med preg av posisjonsinnovasjon (Tidd og Bessant 2009, 21, 23). Dette fordi løsningen tar form som et produkt som kan selges, i tillegg til at den delvis baserer seg på en tidligere innovasjon, som nå benyttes innen et nytt produkt og segment. Det er ikke en fullverdig posisjonsinnovasjon, fordi det ikke er nøyaktig samme produkt som anvendes i et nytt segment eller til en ny kundegruppe, men deler av et tidligere produkt i et nytt produkt som selges til en delvis ny kundegruppe. Det vil nok heller ikke oppfattes som en fullverdig radikal innovasjon, hverken blant kunder eller produsent, men heller ikke som en fullverdig inkrementell innovasjon (Tidd og Bessant 2009, 27). Dette fordi den løser et kjent problem med SCADA-sikkerhet på en ny måte, som dermed vil gjøre det tryggere for SCADA-brukere.

Internettkriminalitet som innovasjonspådriver

Forholdet innovasjonen har til IK, er at det er IK som har skapt trusselen og risikoen for sikkerhetshendelser for SCADA-brukere. SCADA er et system som gjerne benyttes innenfor tungt tekniske og krevende, og ofte samfunnsviktige prosesser. Derfor kan angrep mot SCADA-systemer være svært kritiske, og de senere årene har man sett eksempler på at uvedkommende har kommet seg inn og kunnet overstyre SCADA-systemer. De som ønsker å gjøre slike ting, har ikke vennlige hensikter. Behovet som kunden til Norman følte, kom som en direkte konsekvens av denne trusselen. Hadde det ikke vært kriminelle aktører som utgjør en potensiell trussel mot SCADA-systemer, ville ikke SCADA-brukere følt dette behovet, og Norman ville ikke blitt kontaktet for å løse problemet og ville heller ikke tjent penger på å

produsere en slik løsning. Innovasjonen Norman SCADA Protection hadde etter all sannsynlighet ikke blitt til hadde det ikke vært for dataintegritetskriminalitet i form av tredjegenerasjons-IK (Wall 2007, 47-48, 52-53).

5.2 Case 2: Paradigmeinnovasjon

I denne casen vil man lese om en paradigmeinnovasjon i en bank. Casen baserer seg på et intervju med Mari Grini, Leder IT i SpareBank 1, og viser hvordan SpareBank1 sin IT-avdeling paradigmeinnoverte, etter Nettvettkampanjen organisasjonen hadde i 2008. Paradigmeinnovasjonen kom blant annet som en respons på annen- og tredje generasjons dataassistert kriminalitet. Det er delvis en brukerinnovasjon, med hovedsakelig velferdsgevinst.

5.2.1 SpareBank 1 og åpenhet

I april 2007 holdt konserndirektøren i SpareBank 1 (SB1), Eivind Gjemdal et foredrag om nettbanktrojanere mot SB1 på en sikkerhetskonferanse. Ledelsen i SB1 har alltid sett på åpenhet mot kunder som en viktig del av kunde-bank-forholdet, men det var først etter dette foredraget at man fikk et bevisst forhold til at man kunne være åpen mot kunder og medier rundt sikkerhetsforhold. Frykten for at tilliten hos bankens kunder ville synke hvis de var åpne om sikkerhetsforhold, viste seg å være ubegrunnet. Det å vise bankkundene og sikkerhetsmiljøet at de hadde et bevisst og åpent forhold til sikkerhet, ble positivt mottatt.

> *Egentlig er det rart at sikkerhetsmiljøene er såpass introverte som de egentlig er da, og har så mye fokus på en måte på medarbeidere. Hvordan medarbeidere ofte ter seg og hva de gjør, fremfor å se på hva kundene våre skal ha av sikkerhets…, både informasjon og kunnskap og den type ting.*

I dag er de typer IK som SB1 opplever mest av nettbanktrojaner, phishing og en del kortkriminalitet på nett. De har tekniske systemer for å oppdage mye av angrep, overvåkningssystemer, og systemer for utveksling av informasjon om hendelser som skjer, som for eksempel hvis en database med kortinformasjon har hatt innbrudd. I dag i forhold til for noen år tilbake er sikkerhetsarbeidet i banken mer preget av hendelseshåndtering, mens det tidligere var større fokus på preventivt sikkerhetsarbeid.

«*[…] vi gjør ikke sikkerhetsarbeid for oss selv, vi gjør det først og fremst for kundene våre. Jeg har merket at det er faktisk ikke så vanlig å tenke sånn i sikkerhetsmiljøene.*»

5.2.2 Nettvettkampanjen

Etter hvert som sosiale medier ble en viktigere og viktigere del av samfunnet, og kommunikasjonsavdelingen i SB1 brukte disse flittig, merket Grini at hun måtte ta et møte med kommunikasjonsavdelingen. For Grini som kommer fra sikkerhetsmiljøet, er det viktig å

kunne stå for slik bruk av sosiale medier i en faglig sammenheng. Så i 2008 startet de et prosjekt for å bygge en bro mellom to synspunkter, Nettvettkampanjen, en holdningskampanje internt i organisasjonen. Blant annet slik at Grini selv kunne lære om nytten fra kommunikasjonsavdelingens perspektiv, samtidig som de kunne lære litt fra et sikkerhetsperspektiv, og forhåpentligvis komme klokere ut av det alle sammen. Kommunikasjonsavdelingen, men også toppledelsen i SB1, er opptatt av *gjennomsiktighet*, at man skal være så åpen som mulig.

«*Det var veldig lærerikt både for dem og for oss da, for da får du kunnskapsoverføring mellom oss og hva vi tenker, og så fikk vi kunnskapsoverføring fra dem om hvordan de tenker.*»

«*Og da lærte vi, jeg følte selv at jeg lærte veldig mye om hvordan vi…, de har jo av natur et mye mer utadvendt forhold til verden, og det tror jeg var veldig sunt for oss, at vi fikk del i hvordan de tenker om akkurat det.*»

Det som gjør sosiale medier så spennende for kommunikasjonsmiljøene, er det som er det skremmende i sikkerhetsmiljøene: at ting kan spres fort. For kommunikasjonsmiljøene er dette en ressurs hvor man kan nå mange raskt med et budskap, for sikkerhetsmiljøene er dette en påminner om hvor sårbar man er på nett med tanke på spredning av ondsinnet programvare (OP) og lignende.

«*Og da har jeg også begynt å tenke at sikkerhet må jo være en integrert del av merkevaren din og hvordan du kommuniserer.*»

«*Og jeg tror de lærte en del om at det er ikke bare på grunn av at vi ønsker å mase at vi skriker om sikkerhet da, da er det fordi det er relevant for kunder også.*»

5.2.3 Paradigmeskiftet

Mari Grini fikk en grundigere forståelse av sosiale medier som en ressurs, og inkorporerte dette i IT-avdelingens arbeid. I forbindelse med sikkerhetshendelser og medieoppslag samarbeider de nå med kommunikasjonsavdelingen for å finne ut hvilket budskap de skal ut med til kundene. Sikkerhetsavdelingen og kommunikasjonsavdelingen har begynt en slags samarbeidsprosess når det er ting sikkerhetsavdelingen er opptatt av, og som kommunikasjonsavdelingen dermed skal nå ut til kundene med, gjennom blant annet bruk av

sosiale medier og bankenes nettsider. På denne måten får sikkerhetsavdelingen nådd ut med viktig informasjon til mange kunder raskt og enkelt, slik at de kan gå videre med det viktige sikkerhetsarbeidet. Det nye i denne prosessen er at de nå aktivt bruker sosiale medier som en kanal for å nå ut til kunder med sikkerhetsinformasjon, som tidligere var en mer tidkrevende prosess. Slik når de ut til flere mye raskere enn tidligere, samtidig som de viser kundene at de er der de er og at de er opptatt av og åpne om sikkerhetsaspekter i forhold til kundenes bruk av internettbank.

«*En kan være litt sånn proaktiv raskt, og så kan du jo gi samme informasjon til kundesenteret i bank, sånn at de som ringer inn og lurer på noe får samme informasjon.*»

Den nye prosessen til sikkerhetsavdelingen kommer som følge av to ting ifølge Grini. Det ene er at fordi det er flere sikkerhetstrusler mot internettbank enn tidligere, er behovet for å kommunisere sikkerhet ut mot kundene større. I tillegg kommer dialogen mellom kommunikasjonsmiljøet og sikkerhetsmiljøet i måten å kommunisere på.

«*Siden det har jo vi sett nytten av å nå ut med et budskap på den måten. Det er jo mye enklere.*»

Dette er dermed blitt en integrert del av sikkerhetsarbeidet, som i dag handler mye mer om hendelseshåndtering. Store deler av sikkerhetsarbeidet er tekniske tiltak, men nytten av å være åpen mot kunder og spre sikkerhetsrelatert informasjon over sosiale medier er blitt en nyttig del av det å minske konsekvensen av hendelser, særlig som en proaktiv strategi fra IT-sikkerhetsavdelingen i SB1.

«*Jeg vet ikke om det kan være en innovasjon, men det er i hvert fall en annerledes måte å tenke på sett ut ifra mange andre organisasjoner jeg vet om tenker på det da.*»

Bevis på at dette har gjort nytte og blitt lagt merke til, fikk de høsten 2012, da SpareBank 1-alliansen mottok Fidusprisen. Dette er en pris som gis av Norsk senter for informasjonssikkerhet og TNS Gallup. Prisen gis til en bedrift eller offentlig aktør som har utmerket seg innenfor informasjonssikkerhet, og formålet med prisen er å skjerpe bevisstheten hos næringslivet og hos privatpersoner om behovet for informasjonssikkerhet (NorSIS 2012).

5.2.4 Innovasjonstype

Gjennom Nettvettkampanjen og en tolkning av SB1 sin filosofi om å gi tilbake til samfunnet har IT-avdelingen dannet et nytt paradigme i organisasjonen IT-avdelingen utgjør, hvor de skal dele sikkerhet med kunder og innbyggere i Norge. Gjennom dette gir de informasjon om hvorfor internettsikkerhet er viktig, og hvilke relevante hendelser man må ta ekstra forholdsregler mot. Ved å bruke sosiale medier aktivt i dette arbeidet har de effektivisert sikkerhetsinformasjonsprosessen sin ut mot kunder og internettbrukere generelt, og er dermed med på å bidra til et tryggere internettsamfunn i Norge som helhet.

> *Det med samfunnsansvaret vårt er noe som ligger i SpareBank 1 sin kultur, fordi det er en av filosofiene til sparebankene, det at vi skal gi tilbake til lokalsamfunnet. Og det er på en måte en del av sparebankinstitusjonene, at en del av overskuddet også går tilbake til lokalsamfunnet. Og på sikkerhetsområdet så sier vi at en del av kunnskapsoverskuddet vårt da, eller det vi sitter på, som vi vet og som vi lærer gjennom sikkerhetsarbeidet i SpareBank 1, det skal også tilbake til lokalsamfunnet.[…] grunntanken vår er samfunnsansvaret, og det er på en måte en annen og ny måte å ta samfunnsansvar på sett i forhold til en sparebank. Som sett i forhold til å bidra til guttelaget lokalt for eksempel eller bidra til en eller annen forening lokalt som kunne drive frivillighetsarbeid og den type ting, så tenker i hvert fall jeg det med at det å ta samfunnsansvar på Internett. Det handler for eksempel om det å forklare folk hvordan de kan ha en sikker hverdag på nett. Så det er en videreføring av ansvaret på en ny måte da.* (Grini, SB1, dybdeintervju)

Dette er en paradigmeinnovasjon (Tidd og Bessant 2009, 21), hvor IT-avdelingen og organisasjonen som sådan har fått en ny tankeprosess rundt bruk av sosiale medier i en prosess om det å være åpne ut mot kunder om sikkerhetsaspekter ved bruk av Internett. Gjennom å sette sammen kommunikasjonsperspektivet, sikkerhetsperspektivet og SB1 sin filosofi om åpenhet og det å gi tilbake til lokalsamfunnet har SB1 innovert. Særlig er det i SB1 sin IT-avdeling selve paradigmeinnovasjonen har skjedd, og denne har medført endringer i IT-avdelingens kommunikasjonsprosesser. Innovasjonen er ikke radikal (Tidd og Bessant 2009, 27), da deler av organisasjonen har hatt dette perspektivet lenge, som mange andre typer organisasjoner i verden, selv om kombinasjonen av dette og IT-perspektivet var ny for SB1, og denne tilnærmingen noe fremmed for norsk banknæring. Allikevel vil jeg kategorisere paradigmeinnovasjonen som inkrementell. Nytten de får er hovedsakelig koblet opp mot det proaktive arbeidet mot IK. Bankene har en interesse av at kundene føler seg trygge i bruken av deres tjenester. Det gir høyere kvalitet på servicen SB1 leverer, noe som trolig har ringvirkninger i forhold til hvor fornøyde kundene er.

Konsekvensene av endringer som kommer som følge av innovasjonen, kommer gjennom at organisasjonen åpner opp, og gir mer tilbake til dem utenfor. Gjennom dette får organisasjonen trolig fordeler av blant annet høyere tillit blant kunder og av at kunder blir gjort oppmerksomme på sikkerhetstrusler og sikkerhetshendelser, og derav kan ta de nødvendige forholdsregler. Selve innovasjonen er en brukerinnovasjon (von Hippel 2005, 3), fordi nytten er direkte koblet mot bruken av det nye tankesettet, paradigmeinnovasjonen, i IT-avdelingen. SB1 profitterer ikke på å selge innovasjonen eller informasjonen som paradigmeinnovasjonen har tilgjengeliggjort for bankkundene, og dermed kan det ikke karakteriseres som en produsentinnovasjon (ibid.), men de unngår ikke-målbare tap. Dette kan ses i sammenheng med en velferdsgevinst (Godø 2008, 23-24), hvor banken og kundene sammen, på grunn av IT-avdelingens paradigmeinnovasjon, minimerer skadeomfanget fra IK. Dette gir en velferdsgevinst ved at det er kriminalitetsbekjempelse, som minimerer ikke-målbare tap og negative konsekvenser IK kan medføre for folk. En samfunnsøkonomisk gevinst er det også trolig (ibid.), ved at det resulterer i mindre kostnader ved eventuell etterforskning og lignende som følger med en del ofre for IK.

Kundene får også en nytte gjennom mye mer tilgjengeliggjort sikkerhetsinformasjon. Dette er en konsekvens av at IT-avdelingen har paradigmeinnovert. Dette har medført endring i informasjon- og kommunikasjonsprosessen i forhold til IT-sikkerhet ut mot kunder, som igjen har medført økt tilgjengelighet av relevant sikkerhetsinformasjon. Det er fullt mulig at det ville være hensiktsmessig med et annet mer passende begrep på dette funksjonelle innovasjonsforholdet. Kanskje ett hvor man kan omfatte ikke-profitt-innovasjoner hvor den direkte nytten fra innovasjonen samt hovedgevinsten ikke først og fremst ligger hos brukerinnovatøren, når denne innovasjonen kanskje vil kunne beskrives slik.

Internettkriminalitet som innovasjonspådriver

Nettbanker generelt, og SB1 spesifikt, blir hovedsakelig rammet av dataassistert kriminalitet i form av både annen- og tredje generasjons kyberkriminalitet (Wall 2007, 45-47, 71). Selv om bankene ikke kan klandres for kriminaliteten kundene kan bli rammet av ved nettbankbruk, handler det allikevel for bankene om at kundene skal kunne anvende de internettjenester banken tilbyr, og føle seg trygge med dette. Derfor er det viktig å minimere skadeomfanget når sikkerhetshendelser forekommer, og gi brukere informasjon om generell nettvett.

Internetteknologien har gitt rom for å effektivisere banktjenester, men denne effektiviseringen har også gitt muligheter for kriminelle. Dette igjen har medført behov for kontinuerlig å finne bedre løsninger og kontinuerlig sikkerhetsarbeid. Det er det økende omfanget av IK, som har gitt grobunn for og nytte av paradigmeinnovasjonen i IT-avdelingen i SB1. Hadde det ikke vært noen IK som rammet og påvirket deres kunders bankbruk, ville ikke denne paradigmeinnovasjonen hatt noen nytte. Det var en behovstrekking som ble fylt ved kombinasjon av ulike perspektiver som allerede eksisterte i SB1 (Tidd og Bessant 2009, 232), på en ny måte.

5.3 Case 3: Metodeinnovasjon

I denne casen vil man lese om metodeinnovasjoner som følge av IK generelt i Kripos og en spesifikk metodeinnovasjon i Kripos. Den spesifikke metodeinnovasjonen er et infiltreringsfildelingsprogram utviklet i forbindelse med en barnepornosak Kripos arbeidet med. Metodeinnovasjonene i Kripos er brukerinnovasjoner og en form for prosessinnovasjoner. Den spesifikke metodeinnovasjonen bærer preg av både produkt- og prosessinnovasjon, og er rettet mot annengenerasjons datainnholdskriminalitet. Gevinsten er hovedsakelig av velferdsmessig karakter. Casen baserer seg på et intervju med Rune Fløisbonn, avdelingsdirektør for Datakrim hos Kripos.

5.3.1. Kripos

> *I årene framover har norsk politi behov for å øke sin innsats i forebygging og bekjempelse av datakriminalitet. Politiet må ha en god tilstedeværelse på Internett, og styrke sin evne til å etterforske alvorlig datakriminalitet. En kritisk suksessfaktor er anskaffelse og utvikling av kompetanse og egnede verktøy for behandling av elektroniske spor og store datamengder.*

Kripos er et nasjonalt kompetansesenter for norsk politi, med hovedmål å forebygge og bekjempe organisert og annen alvorlig kriminalitet. Organisasjonen etterforsker og fører i retten alvorlige og komplekse saker. I tillegg yter de bistand i teknisk og taktisk etterforskning, og innehar funksjonen som det nasjonale kriminaltekniske laboratorium. De har også funksjon som kontaktpunkt mellom utenlandske og norske politimyndigheter. Kripos består av cirka 500 ansatte, hvorav halvparten er sivilt ansatte, og de resterende jurister og politiutdannede (Kripos).

> *[…] Internettkriminalitet er jo en følge av den raske teknologiske utviklingen. […], så skapes det muligheter for å utføre nye typer kriminalitet og dessuten utøve tradisjonell kriminalitet med ny teknologi. Teknologi gir muligheter for å utøve kriminalitet over landegrenser, der lovbryter har ukjent identitet og kan utøve kriminalitet uten tilstedeværelse eller i lang avstand til offer og åsted. Dette krever at politiet må arbeide i et nærmere internasjonalt politisamarbeid, utvikle nye måter å etterforske, sikre og utnytte elektroniske spor på og ikke minst bearbeide store datamengder slik at det kan brukes i straffesaksbehandlingen. Politiet må hele tiden utvikle nye kunnskaper og nye metoder, og samfunnet må sørge for at lovverket er relevant og harmonisert internasjonalt. Dette er avgjørende faktorer. For at politiet skal kunne forebygge og etterforske moderne kriminalitet slik at skadevirkningene i samfunnet begrenses, må ny teknologi tas i bruk. Gapet mellom politiets evne til å utnytte ny teknologi og organiserte kriminelle gruppers teknologibruk, må ikke bli for stort til fordel for de kriminelle. Gjennom elektronisk bevissikring, etterforskning og*

> *iretteføring vil politiet føre saker for retten i Norge eller bistå andre land som gir straffereaksjoner overfor dem som utfører kriminelle handlinger i det virtuelle rom.*

Politiet har tradisjonelt vært organisert som en kommandoorientert hierarkisk organisasjon. Det moderne samfunn og bruk av ny teknologi i utøvelse av kriminalitet har utviklet politiet i retning av en kunnskapsorganisasjon som utnytter en stor bredde av kompetanse i sitt arbeid, og bruker flatere organisasjonsstrukturer og bedre tilrettelegging for kunnskapsutvikling. Et eksempel er Datakrimavdelingen i Kripos som bekjemper kriminalitet på Internett. Grunnen til at man trenger kunnskapsorganisasjonens karakteristikker er at man har behov for at ting skal kunne skje raskt, kunnskap må utvikles, ny kunnskap må anvendes raskere enn det man har vært vant til i politiet tradisjonelt. Kripos er et politiorgan som tar spesielt alvorlige saker, spesielt komplekse saker, og eventuelle prinsippsaker, som er en type som skal fremmes for retten for første gang. Blant annet har dette vært tilfelle i en banktrojanersak, hvor Kripos nå har anket til høyesterett. De har anket den to ganger fordi de mener at straffeutmålingen har vært for lav. Fløisbonn påpeker hvordan lovverket har intensjon om å være teknologiuavhengig, men hvor bruk av ny teknologi i kriminalitet viser mangler i lovverket som må oppdateres eller gis nye formuleringer. Lovverk som benyttes ved utøvelse av kriminalitet på Internett eller bruk av elektroniske spor i straffesaker er eksempler på dette.

«[…] man er ikke like bevisst at tryggheten på Internett skal være den samme, […], og vi og vår virksomhet er veldig opptatt av det […].»

Kripos tar saker som rammer privatpersoner og virksomheter. Internett og nye typer elektronisk utstyr og medier blir anvendt som et hjelpemiddel for å gjennomføre tradisjonell kriminalitet, og dernest utføres kriminalitet som er rettet mot selve teknologien (datamaskiner, datasystemer, Internett osv.). Det er førstnevnte saker som ifølge Fløisbonn gjør at elektroniske spor har fått stor betydning i alle typer straffesaker. Kriminalitet som er rettet mot teknologien, har blitt en økende trussel mot enkeltpersoner, privat og offentlig virksomhet der en nasjonal informasjonsteknologisk infrastruktur er sårbar. Det er i slike saker viktig for Kripos i det forebyggende og etterforskningsmessige arbeidet å sikre og behandle elektroniske spor som kan bli avgjørende bevis i eventuell staffebehandling.

5.3.2 Generell innovasjon i Kripos

Ifølge Fløisbonn kjennetegner det Datakrimavdelingen i Kripos at det foregår innovasjon og metodeutvikling i stort sett alle saker. De har utviklet nye metoder og verktøy, som på noen

områder gjør at fagmiljøet utøver dette blant de fremste i Norden og Europa. Metodeutvikling er en av Kripos' seks kjernevirksomheter (Kripos' strategi 2011-2015, 12). Særlig innoverer de når de skal finne spor på mobiltelefoner som ikke er «main stream», som eldre modeller. Å vite nøyaktig hvor man skal gå inn for å lese ut data fra internettkommunikasjon over mobiltelefon, er utfordrende. Det fins tusenvis av forskjellige mobiltelefoner. Mobiltelefoner er blitt en vesentlig faktor for å avdekke informasjon som har foregått gjennom en eller annen tradisjonell kriminalitet. De kan inneholde e-postmeldinger, med hvem og når det er surfet på Internett, og hvor vedkommende har befunnet seg. Denne informasjonen kan gi gode bevis som enten frikjenner eller forsterker mistanke. Mobiler kan knuses, kjøres over med bil, kastes i vann og ha slettet innhold, og allikevel klarer Kripos i stor grad å tappe ut informasjon. De har mobiler de ikke vet hva er skjedd med, hvor de lodder ut chiper de vet inneholder data og prøver å finne de riktige kontaktpunktene å tappe for å finne rester av kommunikasjon og geolokasjoner. Dette kalles hardware forensic, og Kripos er de eneste i Norden som har kompetanse og verktøy for å gjøre denne formen for arbeid.

I tillegg jobber Kripos med innovasjon innen dekoding av kryptert informasjon, slik at innholdet kan leses i klartekst. De har metodeutvikling som har klart å dekryptere informasjon gjennom tallknusing og gjennom chip-kirurgi, for å få tilgang til dekryptert informasjon, som Fløisbonn mener er en ny type innovasjonsmetodikk.

5.3.3 Programvareinnovasjon

Kripos har utviklet nye metoder for å infiltrere fildelingsnettverk som blant annet deler seksuelle overgrepsbilder av barn. En av disse metodene er en programvare som ble anvendt første gang i nordisk sammenheng, og senere i en aksjon i Interpolsammenheng.

De pedofile over hele verden anvender visse fildelingssystemer på Internett, hvor de bruker konferansesystemer i fildelingsnettverk, for å utveksle seksuelle overgrepsbilder av barn. På disse kreves det som oftest at man identifiserer seg og at man dekker over hvem man er. Det er spesielle vilkår for at man får være medlem i slike nettverk, i tillegg til at man må produsere og legge inn bilder i databasen. Dette gjør det vanskelig for politiorganisasjoner å infiltrere disse uten å bli oppdaget. For å kunne straffeforfølge norske borgere må programvare kunne infiltrere nettet og finne aktive norske IP-adresser som utfører denne type bildeutveksling. Lykkes dette, kan man dra hjem til mistenkte og beslaglegge datamaskin og sanke eventuelle bevis for videre å få dem dømt. En slik infiltreringsprogramvare mot

barneporno (IPbp) ble utviklet av teknologer, spesialister på programutvikling, hos Kripos, og var en viktig innovasjon i den saken.

5.3.4 Økt innovasjonsbehov

I dag legger folk igjen mer spor enn tidligere, fordi man har flere varianter av spor. Før var det bare fingeravtrykk, så kom DNA og kjemiske spor, og nå har man elektroniske spor i tillegg. Sistnevnte er blitt stadig mer viktig og avgjørende. Men den teknologiske utviklingen går så fort, og politiet må ha kompetanse og verktøy.

Innovasjonene Kripos har, vil i bred forstand domineres av metodeinnovasjon innenfor etterforskningsfeltet. De må finne nye metoder for å kunne finne frem til det de har behov for av data og informasjon. Dette for å kunne gjøre den samfunnsviktige jobben å skaffe nødvendig bevis i straffesaker, slik at skyldige blir dømt og uskyldige ikke blir dømt.

Når IKT er blitt så utbredt i samfunnet, legger folk igjen mye mer elektroniske spor. Mye av IKT er tilkoblet Internett, og på den måten kan Kripos finne ut hva slags informasjon dataen på internettrafikken på elektroniske gjenstander kan gi. Internett blir oftest brukt som et hjelpemiddel til å utøve tradisjonell kriminalitet, det vil si at det er førstegenerasjons IK (Wall 2007, 44-45), og det kan derfor være kritisk å få ut data fra internettbruken, som avgjørende for skyldspørsmålet i straffesaker. I tillegg har man behov for å infiltrere nett hvor den kriminelle handlingen delvis foregår på Internett, som i den ovennevnte barnepornosaken. Samtidig har man de sakene hvor Kripos må sanke bevis hvor hele den kriminelle handlingen gjennomføres på Internett, som for eksempel banktrojanere som er en tredje generasjons IK (Wall 2007, 47-48).

5.3.5 Innovasjonstype

Kripos står overfor nye utfordringer i så å si hver sak, og må finne nye metoder. Dette kan resultere i nye teknikker eller verktøy, som eksempelet med infiltreringsprogramvaren i barnepornosaken. De står overfor nye problemstillinger, som krever nye løsninger. Dette gjør de ved å sette sammen kunnskapen de har ervervet seg på nye måter, for å løse et hittil ukjent problem for organisasjonen. Dette er en velkjent måte å innovere på, når innovasjon i stor grad handler om å løse problemer på en ny måte, gjennom å koble gamle eller kjente ting på nye måter, gjerne kombinert med nye elementer (Schumpeter [1934] 1983, 132; van de Ven og Angle 2000, 12). Kjente eller gamle ting kan også innebefatte kunnskap man allerede

innehar. Kanskje er ikke disse metodene alltid nye for hele verden, men de er i hvert fall nye for organisasjonen Kripos.

Innovasjonene i Kripos er hovedsakelig koblet til metodeutvikling og vil nok i all hovedsak kunne plasseres under prosessinnovasjoner (Tidd og Bessant 2009, 21, 23), fordi det er en ny måte å utføre kjernevirksomheten på, som er å etterrette, etterforske og innhente bevis. Men Kripos har ingen kommersiell interesse av disse innovasjonene. Det konkrete innovasjonseksempelet, IPbp, var ikke et produkt for kommersialisering, men et verktøy for å sanke bevis ved kriminelle handlinger. Den er rettet mot en form for annengenerasjons datainnholdskriminalitet (Wall 2007, 104, 109-125, 45-46). Kripos er et politiorgan, underlagt staten. De skal ikke tjene penger, men gjøre en jobb innenfor de budsjetter de er gitt. Det skal nevnes derimot at Kripos som de fleste offentlige organisasjoner har budsjetter som må holdes, og at de må vurdere om innovasjonens nytte kan rettferdiggjøres med de ressursene som eventuelt må benyttes for å kunne realisere innovasjonen. Dette er et eksempel på innovasjon i offentlig sektor (Tidd og Bessant 2009, 60), og hvor denne konkrete innovasjonen hovedsakelig gir en velferdsgevinst for samfunnet, men også en samfunnsøkonomisk gevinst (Godø 2008, 23-24). Velferdsgevinsten er at man får straffet flere pedofile, og avslørt deres nettverk. Dette medfører at skadeomfanget de pedofile kunne forvoldt, blir minimert, og færre barn vil bli rammet av de konkrete pedofile som ble tatt gjennom bruken av denne innovasjonen. Også generell kriminalitetsbekjempelse og rettferdighet inngår i velferdsgevinsten. Det er i tillegg en samfunnsøkonomisk gevinst ved at utgiftene samfunnet må ut med for å følge opp ofre av pedofili blir minimert, fordi skadeomfanget er blitt mindre ved denne kriminalitetsbekjempelsen.

I Tidd og Bessant (2009, 21-23) sitt innovasjonsrom vil jeg plassere denne konkrete innovasjonen, IPbp, mellom prosess- og produktinnovasjon. Dette fordi det er et fysisk produkt og fordi den er skapt i den hensikt å brukes av innovatørene selv som et verktøy i en metode. Det er utviklet som et hjelpemiddel i en del av en større prosess. Det kan også klassifiseres som en brukerinnovasjon (von Hippel 1988, 2005). Det er drevet av et behovstrekk for å løse et problem som, sammen med kunnskapsdytt i form av kompetanse Kripos innehar, er det som muliggjør innovasjonen, men uten forventninger om en privatøkonomisk eller bedriftsøkonomisk gevinst (Tidd og Bessant 2009, 232; Godø 2008, 23).

Jeg vil påstå at innenfor Kripos og lignende organisasjoner må anti-pedofil programvare kunne sies å være en delvis radikal innovasjon mot barneporno (Tidd og Bessant 2009, 27). Ingen hadde tidligere utviklet et slikt verktøy innenfor politiet, og det løste et velkjent problem for mange organisasjoner som arbeider med bekjempelse av barneporno. Ringvirkningene av denne innovasjonen var, for samfunnet generelt, at pedofile ble avslørt, og forhåpentligvis at flere pedofile blir tatt, samt at livet for barn blir tryggere.

Som nevnt er programvaren og alle metodeinnovasjonene til Kripos brukerinnovasjoner (von Hippel 1988, 2005). Dette fordi det funksjonelle forholdet til innovasjonene ligger hos Kripos i bruken av metodene eller verktøyene de utvikler (von Hippel 1988). Nytten fra den konkrete programvareinnovasjonen for Kripos er at flere pedofile blir avslørt og mer avgjørende bevis blir funnet, at dette forsterker folkets tillit til rettstaten, og at samfunnet Norge blir tryggere. Kripos kan sies å være en leverandør av bevis til staten Norge, men den direkte nytte av innovasjonene har Kripos internt i organisasjonen. Dermed er dette en brukerinnovasjon, og dette innovasjonstilfellet vil være med på å øke den sosiale velferden (von Hippel 2005, 2, 11-12).

Internettkriminalitet som innovasjonspådriver

Forholdet mellom kriminalitet og innovasjonen ligger i at dette infiltreringsprogrammet er drevet frem av økende bruk av Internett blant kriminelle, som et medium til å utføre annengenerasjons datainnholds-IK (Wall 2007, 45-46, 104).

For Kripos er disse metodeinnovasjonene generelt viktige for både å avsløre kriminell aktivitet og sanke elektronisk bevis, men også for å finne metoder for å kunne håndtere nye former for kriminalitet. Banktrojanersaken er et eksempel på sistnevnte kriminalitet, og er blitt en prinsippsak i et forsøk på å skape endringer i lovverk, potensielt en paradigmeinnovasjon i rettsvesenet, fordi lovverket ikke omfatter de nye formene for IK.

Hadde det ikke foregått ulovlig fildeling på Internett blant pedofile, ville Kripos ikke skapt omtalte programvare. I hvert fall ikke på det tidspunktet og i den hensikt det den gang ble utviklet. Det vil si at for denne innovasjonen var IK en pådriver, fordi uten IK hadde problemet og derav behovet for en innovasjon ikke vært tilstede, og dermed ville incentivet for innovasjonen ikke eksistert.

5.4 Case 4: Ikke-profitt organisasjoninnovasjon

I denne casen vil man lese om hvorfor og hvordan Underworld ble etablert. Dette er en 100 prosent ikke-profitt frivillig organisasjon, som jobber aktivt i motarbeidelse av IK. Det er selve organisasjonen som er innovasjonen casen fokuserer på, og den er rettet mot tredje generasjons kyberkriminalitet, og dataintegritets- og dataassistert kriminalitet. Casen baserer seg på et intervju med Anders Hardangen, en av grunnleggerne av Underworld.

5.4.1 Grunnleggelsen av Underworld

I perioden mellom 1996 og 2003 var det populært å kommunisere gjennom Internet Relay Chat (IRC), som på den tiden ble kalt mIRC. Det er en gammeldags måte å kommunisere over Internett på, som gikk på tvers av landegrenser, og som besto kun av tekst. På denne tiden var det mange såkalte Script Kiddies[12], og det var også norske grupperinger som hacket seg inn på andres maskiner og brukte ressursene til onde handlinger. Disse kom i form av for eksempel angrep på nettsider, angrep på andre brukere og at de tok kontroll over kanaler eller brukerrom på Internett. Hackergrupperinger rekrutterte nye og kompetente mennesker, og de hadde mye å friste med av ressurser. I 1997/98 samlet det seg derfor fire gutter på IRC, som mislikte disse ugjerningene på Internett og ønsket å bruke evnene sine på noe godt. De delte en hobby og en interesse innenfor IRC, så de bestemte seg for gjennom en felles ønsket idé om å motarbeide disse ugjerningene å dele ressurser, drive servere og kanaler, og være en positiv kraft på Internett. De skulle drive holdningsskapende arbeid på IRC. De kalte seg Underworld (UW). De sammenlignet seg litt med Kandu, norsk kreativ dataungdom, som blant annet er de som utgjør styret i The Gathering. UW prøvde å overbevise brukere på IRC om at man kunne gjøre spennende ting og allikevel være på den gode siden, få et godt rykte på Internett, kanskje bli med i The Gathering, og at man gjorde noe positivt.

> *Internett er så fullt av hackere, skurker, det blir mer og mer penger i kriminalitet på Internett. FBI sier jo at det har gått forbi både prostitusjon og narkotika i omsetning. Det er laginnsats for å gjøre noe på det. Så det er noen som melder seg inn i Røde Kors og leter etter savnede i skogen, vi er vel ikke den gjengen som flyr i skogen, så vi har valgt å bruke den kunnskapen vi har på vårt område på altså frivillig arbeid. Så jeg tror det er den dugnadsånden, man har lyst til å gjøre noe positivt, og så er det samholdet. Samholdet med å ha en hobby uavhengig av om det er leirdueskyting eller frimerkesamling eller hva det nå er, dette er noe vi kan og føler vi er gode på og da har vi lyst til å gjøre det sammen. Det å sitte alene på det mørke gutterommet det er*

[12] **Script Kiddie** er en hacker, som anvender ferdig automatiserte hackerverktøy (Rush m.fl. 2009, 95).

fra fortiden, det er mer moro å sitte sammen, innovative ideer, finne på nye ting, være banebrytende på det man gjør. Og det klarer vi veldig bra i Norge.

Disse guttene møttes via IRC, én fra Kongsberg, to fra Hallingdal og én fra Oslo. Guttene var i tenårene og i overgangen til arbeidslivet da de startet UW. Fra oppstarten og til langt ut på 2000-tallet fokuserte UW på IRC, hvordan beskytte IRC-kanaler, hvordan beskytte IRC-servere man koblet seg opp på, og hvordan bygge et positivt og godt miljø på IRC. På det meste var det over 300 personer som var medlemmer i UW. De var og er trolig fremdeles den eneste frivillige gruppen på Internett i Norge som har sikkerhet som fokus. De registrerte seg i Brønnøysundregisteret i 1999. Bakgrunnen for dette var hovedsakelig at de måtte ha registrert et foretak for å få opprettet en internettadresse.

Fokuset var ikke sikkerhet fra dag én, men IRC, hvor de driver en del av de store pratetjenestene og hvor det kan være opp mot 40 000 brukere på samtidig hver eneste dag. Det var for cirka 6 år siden at sikkerhet ble en integrert del av UW. I dag er UW delt opp i flere undergrupper. En del er de som synes det er moro å drive med servere, nettverk, e-post og lignende. Så er det delen som driver med IRC, dette er den største og eldste delen, og den innebærer tilstedeværelse på en del forskjellige nettverk med veldig mange brukere, som for eksempel EFnet, IRCnet og UnderNet. Og så har UW i tillegg noen sikkerhetsprosjekter. De gjør en god del mer hjelpearbeid underveis, men dette er de tre hovedleveransene inn mot sikkerhetsmiljøet i dag.

«*[…] Underworld er jo 100 prosent non profit, […]*.»

Etterhvert som disse guttene er blitt voksene, og flere av dem i dag har yrker innenfor IT-sikkerhet, har arbeidet glidd over i hobby. I dag fokuserer de mer på IK, og har spesialisert seg på trojanere i Norge. Blant grunnene til dette er at man ikke kan være gode på alt, så de har siktet seg mot å være veldig dyktige på trojanere. De har avgrenset det til hovedsakelig Norge, mye på grunn av språket.

5.4.2 Trusselbildet på Internett og Underworld

Trusselbildet på Internett har endret seg de siste årene. Tidligere kunne noen få antivirus-selskaper samle inn virus fra hele verden, men i dag har virus og trojanere en mer målrettet spredning. Dermed er det blitt vanskelig å innhente alle virus og trojanere sentralt og lage effektiv beskyttelse for antivirus-selskapene. Dette kan være en konsekvens av at motivene bak IK har endret seg med tiden.

«*Det var kanskje for å spre et budskap eller for å ødelegge for andre, men det var ikke for å tjene penger.*»

De siste årene har virus og trojanere blitt målrettede, de siktes inn på spesifikke grupper som bakmennene ønsker. De klarer å avgrense hvor virus og trojanere skal ramme ned på geografiske områder. Dette gjør at det er en umulig oppgave for en global aktør å få tak i alt av virus og trojanere. UW er langt fremme i å hente og lete opp trojanere på norske websider og analysere enkelttyper trojanere. Det er få land som har de systemer UW anvender, på hobbybasis. De får utstyr gjennom donasjoner av brukt utstyr, og de får lov å plassere utstyr hos mange ulike bedrifter og organisasjoner. De jobber 100 prosent ikke-profitt, de tar ikke imot penger og har aldri noen planer om å prøve å tjene penger på de tjenestene de i dag gir.

«*Det er veldig hobby- og interessedrevet. Så det vi har gjort i nyere tid er at vi gir hver av de som er med og har en interesse i det, mulighet til å være med i et fellesskap, hvor vi deler infrastruktur, vi deler tilgang til data og tilgang til hvert sitt prosjekt.*»

5.4.3 Informasjonsdeling

På sikkerhetsområdet prøver de å bidra inn i det internasjonale samfunnet. UW gir alltid beskjed til NorCERT med informasjon av nytte, slik at NorCERT kan gå videre med det og informere eventuelt berørte parter. De gir også informasjon til den internasjonale organisasjonen Shadowserver, som samler data om den kriminelle siden av Internett (Shadowserver). Denne organisasjonen er internasjonalt kjent, og holder foredrag og er til stede på nesten alle sikkerhetskonferanser. Denne organisasjonen blir også til tider kontaktet av føderale myndigheter og utenlandsk politi om tilleggsinformasjon i saker, men de har også mye mer ressurser enn UW.

«*Så er det mye lagjobbing, vi deler på mye av infrastrukturen i bunn, vi deler informasjon som vi klarer å få ut og inn av de forskjellige systemene, og det er en modell vi synes fungerer godt.*»

UW er som nevnt hobbybasert, så hvordan de jobber, er mer flytende. Det går i rykk og napp. De rekrutterer helst folk som allerede har ideer, som de kan tilby et felleskap og en infrastruktur. Tillitt til dem som får være med i UW er viktig, og ingen av medlemmene er derfor tidligere hackere som gjør opp for gamle synder. De har valgt noen nisjer de er gode

på, og de utvikler nye systemer, teknikker og løsninger i prosessen med å få tak i den informasjonen og dataen de er ute etter. Disse gjenspeiler trendene på blant annet ondsinnet programvare (OP). Eksempler på dette er to av prosjektene i det å opprette en malvaredatabase, Vsheild Norge og Malware Collector. Vsheild er et globalt prosjekt i å se trafikkflyt på Internett, og UW ønsket å lage dette med bedre dekning kun for Norge. I Vsheild Norge satte de opp passive datamaskiner rundt på Internett for å lokke til seg OP, for å se hva som kom inn. Men på denne tiden endret trusselbildet seg veldig, og gikk over til at man ble infisert gjennom spam eller ved at man aktivt besøkte en hjemmeside. Dermed startet de Malware Collector, som genererer en liste basert på antall Google-søk, hvor topp 20 treff på Google besøkes, i den hensikt å besøke tilfeldige nettsider. Samtidig har de en liste over de mest besøkte nettsidene i Norge som besøkes cirka åtte ganger om dagen. Dette prosesseres og henter ut hvis den finner noe ondsinnet. Når UW er ferdig med sin analyse, sender de det videre til diverse prosjekter som Malware Databasen, Shadowserver, NorCERT og Virus Total. Målet er å hjelpe andre med data. De ønsker å bidra med tilgjengeliggjøring og deling av data om angrepskoder og angrepsmetoder, slik at man er bedre rustet til å forsvare seg. De ønsker å være en bidragsyter innen informasjonssikkerhetsmiljøet nasjonalt og internasjonalt.

5.4.4 Ikke profitt, kun frivillighetsarbeid

«*[…] Underworld er jo 100 prosent non profit, vi tar ikke imot penger fra noen, og vi bruker egentlig veldig lite penger. Det vi er avhengig av er sponsing av noe av infrastrukturen vi trenger for å overleve for å si det pent.*»

De får hjelp av noen organisasjoner og firmaer til å drifte datautstyr som er gitt til UW. De får blant annet kassert utstyr, særlig fra UW-medlemmenes arbeidsplasser, som mange organisasjoner er nødt til å kvitte seg med på grunn av serviceavtaler. Dette er datautstyr som ellers ville gått i kontainere.

«*[…] de ser hvor mye glede de har av at det kan bygge kunnskapsnivået på fritiden, og har et sosialt nettverk som hjelper han og dine problemer underveis.*»

Anerkjennelse er de ikke ute etter. De gjør dette arbeidet fordi de har lyst og brenner for området, enten det er sikkerhet eller IRC. De får anerkjennelse fra dem som jobber med UW, de som får data fra UW og gir data tilbake.

«*[…] egentlig glede er å kunne være en del av flere forskjellige større miljøer hvor man kan dele, det er fellesskap.*»

> *Men jeg tror de som jobber best på dette området her jobber litt under radaren. For vi prater jo om organisert kriminalitet der ute. Det er utrolig mange milliarder penger i alle mulige valutaer, så det å stå fram og si at vi aktivt motarbeider, det tror jeg ikke er noen investering for fremtiden.*

5.4.5 Innovasjonstype

Innovasjonen til UW er selve UW som organisasjon. En slik type organisasjon, tuftet på hobbybasis, ikke-profitt og frivillighet, innenfor området internettkriminalitet, er ny i norsk sammenheng. Det finnes trolig ingen andre organisasjoner som UW, som jobber spesielt rettet mot IK, i Norge i dag. Det er en slags forretningsmodellinnovasjon, samtidig som det ikke er det fordi det er ikke-profitt. Organisasjonsmodellen bærer preg av *open source,* som innebærer frivillig samarbeid i utvikling, ofte av programvare, og er stort sett internettbasert (se bl.a. von Hippel 2001; von Hippel 2005, 97-103; von Krogh og von Hippel 2003). De har skapt en frivillighetsorganisasjon som passer inn i tiden og som har utviklet seg i takt med internetteknologien og dens medfølgende sikkerhetstrusler. Man kan kalle det en slags videreføring av natteravner til Internett. Men noe som igjen skiller denne organisasjonen ut fra de fleste ikke-profitt- og frivillighetsorganisasjoner, er at de ikke tar imot noen former for tilskudd, kun donasjoner av brukt datautstyr og tillatelse til å få plassere utstyr hos organisasjoner.

UW har mange brukerinnovasjoner (von Hippel 1988, 3; 2005, 3), ting de har skapt av metoder og verktøy til intern bruk slik som Kripos gjør. Men innovasjonen UW er litt mer komplisert, og det er denne innovasjonen som fremheves i denne oppgaven. UW både produserer og leverer tjenester og informasjon, men de selger dem ikke. von Hippel (1988, 4; 2005, 3) påpeker at det finnes andre innovatører enn produsent og bruker, og kanskje er UW en av disse. Som nevnt under paradigmeinnovasjonen til SB1, er det vanskelig å klassifisere ikke-profitt innovasjon, når nytten hovedsakelig kommer andre enn innovatøren til gode, for da har man ut fra von Hippels definisjon heller ikke oppfylt kravene til en brukerinnovasjon (von Hippel 1988, 3; 2005, 3). Allikevel har UW som organisasjon i større grad muliggjort arbeidet som medlemmene gjennom årene har gjort, derfor kan UW som innovasjon forstås som en brukerinnovasjon, da det er organiseringen som har blitt brukt til å gjennomføre UW sitt arbeide. De fire guttene som startet UW er entreprenører, og ifølge Benz (2006) og Rose-

Ackerman (1996) karakteriseres entreprenørskap ofte best som en ikke-profittsøkende aktivitet.

Nytten av innovasjonen UW får alle som bruker Internett, særlig i Norge og innenfor de spesifikke delene de har spesialisert seg på. Men også medlemmene i UW har en nytte av å bruke kunnskapen de har og utvikle ny gjennom å bidra til noe godt og positivt i et felleskap med andre likesinnede. De får glede av å bedrive en interesse og hobby, som gir mening og utretter noe positivt. Men nytten er hovedsakelig et litt tryggere Internett for de som ferdes der.

At det finnes lignende, men ofte større og mer formelle, ikke-profitt organisasjoner som driver innenfor samme felt i andre land, gjør ikke UW til noen mindre innovasjon i Norge. For innovasjonen trenger ikke være ny for hele verden, men må oppleves som ny for dem som adopterer den (Rogers 1983, 11; van de Ven og Angle 2000, 12), noe Anders Hardangen sa at de mente det var da de startet og delvis føler til den dag i dag. Måten de organiserer seg på kan også minne litt om open source software miljøene (Krogh og von Hippel 2003). Dette fordi det er uformelt, det skapes et felles gode, og fordi det meste skjer over Internett. Nytten fra UW er hovedsakelig velferdsgevinsten for alle de hjelper og som får nytte av informasjonen UW fremskaffer (Godø 2008, 23-24). Dette er i stor grad ikke-målbare gevinster, men ut ifra de estimerte kostnadene til datakriminalitet som NorCERT har publisert (NorCERT 2011, 19; NorCERT 2012, 21-22), kan man anta at UWs arbeid medfører en samfunnsøkonomisk gevinst. Samtidig som det trolig kan medføre en bedriftsøkonomisk gevinst gjennom unngåelse av tapte inntekter for bedrifter (Godø 2008, 23-24), som ved hjelp av informasjon fremskaffet av UW, i større grad kan beskytte seg mot sikkerhetstrusler og minimere skadene fra sikkerhetshendelser.

Internettkriminalitet som innovasjonspådriver

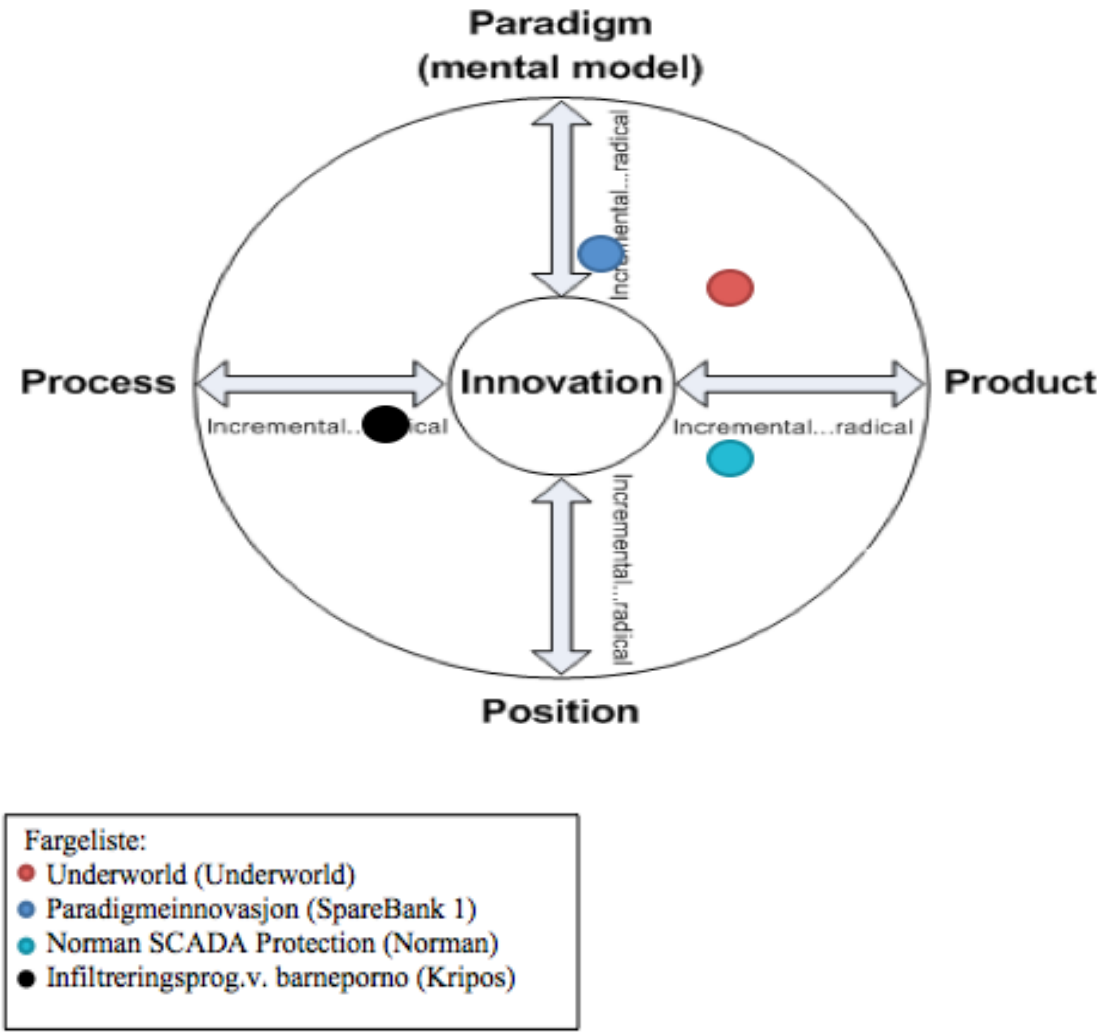
UW startet som en organisasjon med unggutter som ønsket å motarbeide onde handlinger på IRC, utført av dem som hacket og ødela for andre fredelige brukere. Hacking var og er i de aller fleste tilfeller ulovlig, og jeg vil derfor karakterisere dette som motarbeidelse av kriminalitet. Senere har det delvis glidd over i sikkerhetsarbeid og motarbeidelse av avansert IK, som banktrojanere. De motarbeider hovedsakelig tredjegenerasjons kyberkriminalitet, men både dataassistert- og dataintegritetskriminalitet (Wall 2007, 47, 52-53, 71). UW startet som en reaksjon mot IK for å dekke behovet for gode krefter på IRC, og senere mot andre

typer kriminelle handlinger på andre deler av Internett. Hadde det ikke vært for slike kriminelle aktiviteter på Internett, hadde ikke UW hatt det sysselmålet de hadde og har, og UW ville ikke hatt noen grunn for å starte opp det virket de gjorde.

5.5 Oppsummering og resultat fra caseanalyser

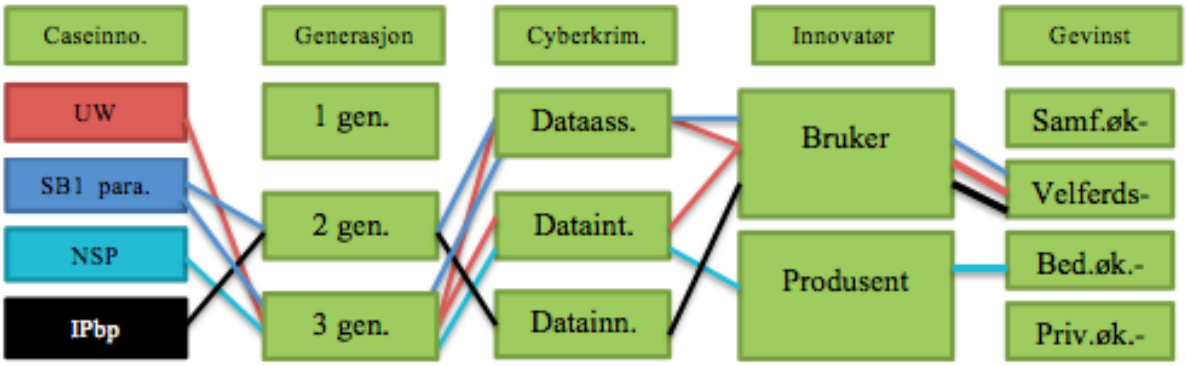
I hver av casene forsøker jeg å illustrere en form for innovasjon, som alle er ulike. I løpet av hver casebeskrivelse viser jeg problemet som informanten forklarte at innovasjonen skulle løse eller bidra til å løse. Jeg forsøker også å vise hvordan IK har vært en medvirkende årsak til at samtlige av caseinnovasjonene ble til.

Under har jeg plassert hver innovasjon i Tidd og Bessant (2009, 22) sitt innovasjonsrom, slik jeg oppfatter det som mest riktig. På denne måten ser man hva slags type innovasjon casene har illustrert, og at alle casene illustrerer ulike innovasjoner.



Figur 5.1 *Caser i innovasjonsrommet.* Modellen er basert på Tidd og Bessant (2009, 22) sine 4 P'er i innovasjonsrommet, og er funnet på BLOG.DATA.ORANGE.DE (Schulze 2007).

I neste figur summeres analysene av casene. I denne viser jeg hvilken generasjon og kategori av kyberkriminalitet/IK de enkelte caseinnovasjonene hovedsakelig tar sikte på å motarbeide (Wall 2007). Samt om det er av typen brukerinnovasjon eller produsentinnovasjon (von Hippel 1988, 2005), og hvilken hovedgevinst innovasjonene gir (Godø 2008).



Figur 5.2 *Cyberkriminalitet-, innovatør- og gevinstkategorisering.*

I siste kolonne under gevinst illustrerer jeg kun det jeg mener er hovedgevinsten fra hver enkelt caseinnovasjon. For eksempel vil de med hovedsakelig en velferdsgevinst i mange tilfeller også medføre en samfunnsøkonomisk gevinst, og kanskje til om med en privatøkonomisk- og/eller en bedriftsøkonomisk gevinst. NSP for eksempel, som hovedsakelig gir en bedriftsøkonomisk gevinst, vil trolig også gi en velferdsgevinst og en samfunnsøkonomisk gevinst, fordi SCADA ofte brukes i samfunnskritiske systemer. Og kanskje gir NSP også en privatøkonomisk gevinst for aksjonærene i Norman. Det kan altså være flere innovasjonsgevinster til caseinnovasjonen fordi det er en synergi i nytteverdi, men figur 5.2 forholder seg kun til den mest åpenbare hovedgevinsten.

Casene illustrer hvorfor og hvordan organisasjonene har innovert eller er innovasjoner i seg selv som følge av IK i de konkrete casene. Det omhandler det overordnede endringsbehovet som IK i lengere tid har skap, og at dette har medført tilpasninger som blant annet har medført innovasjoner. Innovasjonene er skjedd i løpet av de siste 18 årene, og de er et resultat av den tids endring i teknologi og kriminalitet.

Kun én av innovasjonene gir hovedsakelig bedriftsøkonomisk gevinst, alle gir velferdsgevinst og samfunnsøkonomisk gevinst. Tre av fire caser vil ha velferdsgevinsten som hovedgevinst. Flere av casene vil indirekte bidra til privatøkonomisk- eller bedriftsøkonomisk gevinst. Den som hovedsakelig gir bedriftsøkonomisk gevinst, er den som har utnyttet IK som en

markedsmulighet, i motsetning til Kripos og SB1 som har innovert på bakgrunn av et mer indirekte behov hos egen organisasjon. UW har innovert for å dekke andres behov, men uten å utnyttet dette for økonomisk gevinst. Dette illustrerer ulike forhold til IK, som medfører ulike typer innovasjoner.

Alle casene viser et forhold til IK, hvor IK har vært en medvirkende årsak for innovasjonene. Casene viser at dette forholdet kan variere mellom ulike ikke-kriminelle organisasjoner, og at innovasjonene, innovatørene og innovasjonsgevinstene kan variere som følge av organisasjonstype og hvilket forhold IK har hatt til den konkrete situasjonen som medførte den konkrete innovasjonen. Det er også andre medvirkende faktorer som har vært avgjørende for at de konkrete innovasjonene ble det de ble, men IK har også vært avgjørende for dette, da det har vært IK som har skapt behovstrekket i alle casene.

6.0 Drøfting: Internettkriminalitet som pådriver for innovasjon?

Internetteknologien er blitt en altomfattende teknologi og en radikal innovasjon. Det er en sammensatt teknologi, som har gitt nye muligheter og tilfredsstiller ulike behov. Men den har på samme tid medført mange nye trusler og nye behov. Både kriminelle og ikke-kriminelle har sett mulighetene som Internett har gitt, og i takt med at den ene håndterer truslene fra den andre, har denne håndteringen medført nye trusler mot internettbruken til den andre.

Organisasjoner innoverer som følge av internettkriminalitet (IK) av ulike grunner. Dette kan være avhengig av hva slags organisasjon det er snakk om, men i denne oppgaven har den, i samtlige caser, kommet som en respons på muligheter og behov IK har medført. Mulighetene som kan oppstå innenfor for eksempel sikkerhetsområdet, er premissdrevet, ut ifra at det er et behov som kommer som kan fylles. Å lage sikkerhetsløsninger uten at det er behov for det, vil ikke gi noen nytte og heller ingen gevinst. Premissene blir skapt som følge av en trussel. Beskyttelse mot trusselen fremstår som en nødvendighet, et klart behov. Det skapes ny kunnskap ved at det er et behov for en løsning i casene.

I dette kapittelet vil jeg drøfte innovasjon som følge av IK i ikke-kriminelle organisasjoner og IK på et mer overordnet nivå, ved å benytte ulik litteratur. Jeg skal drøfte problemstillingen; *Hvordan kan internettkriminalitet være en pådriver for innovasjon i ikke-kriminelle organisasjoner?* Jeg vil se på litteratur om organisasjonsutvikling og -tilpasning opp mot empirien fra datainnsamlingen.

6.1 Teknologisk utvikling og internettkriminalitet

Hovedutfordringen med IK, som samtlige av informantene uthever, er globaliseringssiden ved Internett. Fordi Internett er grenseløst, går kriminaliteten på tvers av grenser og juridiske områder. Det finnes ingen internasjonal lovgivning eller et internasjonalt politi med myndighet som opererer på hele Internett.

> *En verden som blir stadig mer «connected», vil også gi mer rom for kriminelle aktører. Dette så vi veldig klart da Facebook fikk et stort omfang. Plutselig så vi mye mer malware som også benyttet seg av sosiale nettverk. Og dette er en tendens som forsterker seg mer og mer.* (Lilleeng, Norman, dybdeintervju)

Dette gjør at trusselen kan komme fra hvor som helst i verden, og kan dermed være umulig å iretteføre hvis norske organisasjoner eller nordmenn eller Norge generelt blir rammet. Dette medfører en større trussel, fordi det ikke bare er kriminelle i Norge som utgjør trusselen, i tillegg til at forbryterne er vanskelige å ta.

Dagens Internett er en årsak til og en konsekvens av globaliseringen. Internett har koblet verden mer sammen, og dette har medført flere brukere, noe som har formet og utviklet Internett ytterligere. Internett har blitt formet av brukere, men Internett har formet brukere og samfunn siden det først ble opprettet. Denne utviklingen illustrerer en stiavhengig og samutviklende prosess rundt Internett og aktørene og prosessene rundt (Nelson 1994), slik som IK og de ikke-kriminelle organisasjonene og deres innovasjoner. Dette ved at endringer er basert på tidligere teknologi og kunnskap, og er kommet som følge av endringer som andre aktører har medført, og som har påvirket omgivelsene og andre aktører igjen. I den forstand er det en evolusjonær prosess, hvor endringer påvirker andre endringer og utvikler seg i en dynamisk prosess.

6.1.1 Internettkriminalitetsutviklingen de senere årene

Tidligere var det klassiske virus- og gutteromshackere som dominerte. Disse ønsket å vise hvor dyktige de var teknologisk og ønsket i stor grad å være synlige. Rundt år 2003 begynte man å se en endring i denne trenden, ved at det kom mere direkte kriminelle aktører på Internett. De kunne blant annet ha økonomiske og politiske militærstrategiske motiver for å stjele informasjon. Disse ønsket i motsetning til aktørene frem mot 2003, å være usynlige (Lilleeng, Norman, dybdeintervju).

Angrepsmønstrene i dag er i stor grad skreddersydd for å tjene penger, og i enda sterkere grad etter år 2006. Før var de utviklet til for eksempel å stjele kredittkortinformasjon eller e-postadresser. I dag utvikles det trojanere som gjør flere ting, blant annet stjeler de både kredittkortinformasjon, passord og e-poster, og sender dette til ulike steder, for at denne informasjonen videre skal kunne utnyttes til økonomisk vinning (Hardangen, UW, dybdeintervju).

Det som blir vanligere og vanligere, er det som kategoriseres som *Advanced Persistent Threats*[13] (Lilleeng, Norman, dybdeintervju; NSR 2012, 5). Dette beskrives som svært avanserte programmer, som blir resistent på maskinen, det vil si at det er vanskelig å fjerne, slik tilfellet var for Irans kjernefysiske utviklingsprograms datamaskiner i 2012 med viruset Flame (Dehghanpisheh 2012; Kaspersky 2012, 2). De som utvikler disse, innehar ekstremt mye ressurser (Lilleeng, Norman, dybdeintervju). Nasjoner som driver med spionasje er et eksempel på ressurssterke utviklere av slike systemer. I tillegg er kriminaliteten blitt mye mer organisert, og har dermed mange flere lag (Lilleeng, Norman, dybdeintervju). Det er noen som gjør selve programmeringsjobben og utvikler verktøy (Hardangen, UW, dybdeintervju). De vil ikke nødvendigvis noen gang anvende disse verktøyene selv, men blir betalt for en programmeringsjobb. Man har videre de som anvender verktøyet, og de som hvitvasker pengene (Hardangen, UW, dybdeintervju).

> *[…] det er noe med at det finnes nye, akkurat som vi driver og utvikler nye forretningsmodeller i vår lovlige verden, så er det noe med at de gjør det tilsvarende. Og Internett gir dem også muligheter til å utvikle nye forretningsmodeller, så vi ser jo også da at det er jo helt profesjonelle forretningsmodeller i den kriminelle verden som man egentlig nesten kunne lært litt av hvis man hadde sett det sånn da. Det er en slags innovasjon begge steder kan du si da.* (Grini, SB1, dybdeintervju)

I tillegg påpeker Grini (SB1, dybdeintervju) at de kriminelle ikke følger samme lover og regler og byråkrati som ikke-kriminelle organisasjoner, og dermed evner de å snu seg raskere. Hun sier seg enig i at det er en dynamikk mellom de kriminelles innovasjoner og de ikke-kriminelles innovasjoner. Hardangen (UW, dybdeintervju) beskriver også avanserte nettverk i undergrunnen, som ligner Facebook, hvor kriminelle kommer i kontakt med hverandre, kommuniserer og deler informasjon.

6.1.2 IKT-kunnskapsnivå blant kriminelle

Økning i antall individer med høy teknisk evne brukes som forklaring på fremveksten av lovløse brukere (Flowers 2007, 5). Det er også lovløse brukere som lager lovløse innovasjoner (ibid.). Kunnskapen blant brukere i dag er mye høyere enn tidligere, og de har evnen til å re-programmere og plukke fra hverandre svært komplekse og høyteknologiske

[13] **Advanced Persistent Threats** er et begrep anvendt om angrep hvor man anvender flere ulike metoder, både tekniske og sosiale, for å oppnå onde hensikter (Sterling 2010).

produkter og tjenester (ibid., 6). Dette har medført mindre kontroll for produsenter, noe som er utfordrende for produsenter og andre brukere (ibid., 6-7).

Moderne IK krever et høyt kompetanse- og kunnskapsnivå med hensyn til IKT. Dette gjelder særlig programmering, for å utvikle dagens svært avanserte ondsinnede programvarer. Samtidig har den kriminelle verden utviklet forretningsmodeller, hvor programmene selges som verktøy eller brukervennlige kriminelle programmeringsverktøy, ofte kalt exploit packs, slik at de som anvender disse, trenger minimalt med teknisk kunnskap for å dra nytte av det (Hardangen, UW, dybdeintervju).

6.2 Ikke-kriminelle innovasjoner og internettkriminalitet

«En *innovasjon* er en idé, praksis eller objekt som oppleves som ny av et individ eller andre enheter som adopterer den.» (egen oversettelse, Rogers 1983, 11). I følge Everett M. Rogers (1983, 363, 365) blir en innovasjon redefinert i implementeringsfasen når en innovasjon adopteres, og dette kalles *reinvention.* Reinvention defineres som endringer og modifikasjoner av brukere i adopsjons- og implementeringsprosessen (ibid., 16-17). Rogers (1983, 13) mener at teknologiske innovasjoner ofte blir adoptert for å minimere en form for usikkerhet, men at det også skaper andre usikkerheter, i forhold til potensielle konsekvenser ved adopsjon. En teknologisk løsning blir en innovasjon når den tas i bruk for å løse et følt behov eller et opplevd problem (ibid.). Når en ny idé, et nytt produkt eller en ny tjeneste blir tatt i bruk, blir den en innovasjon, og man vil fortsette å evaluere den, og bruke denne kunnskapen til å videre redusere usikkerheten rundt innovasjonens effekt og videreutvikle den (ibid.).

Fredrick Emery og Eric Trist (1965, 21) skriver at miljøet organisasjoner opererer i, i økende grad endrer seg mot å bli enda mer komplekse. Herbert A. Simon (1971) beskriver organisasjoners omgivelser i informasjonssamfunnet som på randen av informasjonsdrukning, og at uklok anvendelse av ny teknologi ikke er fordelaktig for organisasjoner. Han mener allikevel at ny teknologi gir løsningene på de fleste av samfunnets problemer, men at man aldri kan vite helt sikkert hva konsekvensen av ny teknologi medfører før den er blitt testet i virkelige omgivelser og har gitt erfaringer (Simon 1971, 49, 51). Han mener man i stedet for å henge ut dem man mener burde forutsett en uheldig konsekvens i etterpåklokskapen, heller burde fokusere på å håndtere det uforutsette (ibid., 49). Ny teknologi vil alltid medføre både negative og positive konsekvenser, og Simon setter sin lit til at mennesket kan løse kritiske problemer like fort som nye oppstår (ibid. 48, 51).

I takt med samfunnsutvikling og teknologisk utvikling går kriminalitetsutvikling, og dette medfører behov for tilpasning og videre utvikling for samfunn og teknologi. Organisasjoner generelt som ikke spesifikt jobber med Internett, som for eksempel bedrifter hvor forretningen ikke er tuftet på selve Internett, må i økende grad tilpasse seg de omgivelsene det å bare kommunisere gjennom Internett medfører. Og organisasjoner som for eksempel banker og nettaviser må i økende grad tilpasse seg de trusler som følger det å tilby deler av tjenestene over Internett. Internett byr på trusler for organisasjoner og for samfunnet, som man må tilpasse seg fordi den teknologiske utviklingen kun har gått fremover. Gjennom tilpasninger, som ikke nødvendigvis vil gi noen direkte finansiell gevinst, men snarere en nødvendig investering for fremtiden og retten til å overleve, skjer det endring i organisasjoner. Noen organisasjoner tilbyr ferdige løsninger for å dekke organisasjoners behov, slik som Norman gjør. Politimyndigheter har måttet innovere for å tilpasse metoder og verktøy til den nye formen for kriminalitet, som samfunnet i økende grad blir utsatt for.

6.2.1 Kriminalitet som skaper av behov

Ideen om kriminalitet og om institusjoner som definerer og straffer denne, har eksistert i tusener av år. Hva som oppfattes som kriminalitet, har endret seg med tiden. Etter hvert som samfunn har bygd seg opp, har de med makt forsøkt å holde ro og orden, men de har også sett seg nødt til å ta forholdsregler mot truslene og håndtere hendelser fra dem som ikke ønsker å underkaste seg de regler som er satt. Informantene har beskrevet en kritisk situasjon for mange ulike organisasjoner, hvor behovet for endring har vært nødvendig. Behovene for endring og mulighetene for endring er drevet frem av utbredt teknologisk bruk. Dette har igjen medført IK, blant annet på grunn av mulighetene ved at det økonomiske potensialet har økt på Internett. Men bare utbredt teknologisk bruk har ikke medført de store behovene og mulighetene for ikke-kriminelle organisasjoner. Det er IK som delvis har drevet frem disse.

> *[…], og det kan du si er drevet frem av omgivelsene, og der kan du si at behovet for å ha et mye sterkere fokus på sikkerhetsområdet, det er omgivelsesdrevet altså. Det er drevet av behovet for sikkerhetskompetanse, og det å ha et ordentlig fokus på det i organisasjonene, det er viktigere rett og slett.* (Grini, SB1, dybdeintervju)

6.2.2 Innovasjonsnytte

I caseanalysene forsøkte jeg å vise hvordan innovatørene er forskjellig i de ulike casene. Dette omhandler det funksjonelle forholdet til innovasjon, og gjelder det analytiske skillet mellom brukerinnovasjon og produsentinnovasjon (von Hippel 1988, 2005). Dette skillet kan være fruktbart fordi det åpner opp for at innovasjon ikke trenger å ha finansiell nytte, men at en

innovasjon allikevel må ha en form for nytte for at en idé, en tjeneste eller et produkt skal bli tatt i bruk og dermed bli en innovasjon. Richard Lipsey, Kenneth Carlaw og Clifford Bekar (2005, 68) antar at fordi innovasjon og oppfinnervirksomhet er risikofylt og dyrt, vil personer kun utvikle dette hvis de forventer en nytte som overgår antatt kostnad for individet. Annen innovasjon, og oppfinnelser som faller utenom dette, mener de er tilfeldig (ibid.). Dette kan trolig i mange tilfeller stemme, men som casene illustrerte, trenger ikke all innovasjon å være profittmotivert. Nytten kan komme gjennom en annen verdi enn finansiell profitt, noe som også kan gjøre det vanskelig å måle etter økonomisk måleenhet.

Eksempelet Underworld (UW) er en innovasjon i seg selv, basert på 100 prosent frivillighet. De har også innovasjon innenfor verktøy og metoder de anvender. De har heller personlige utgifter ved å gjøre det arbeidet de gjør (Hardangen, UW, dybdeintervju). De tar av egen privat tid og arbeider for et felles bedre nettsamfunn. Men dette kan om mulig være av det Lipsey, Carlaw og Bekar (2005, 68) beskriver som tilfeldig unntak. For SpareBank 1 (SB1) handler det kanskje om å få oppfylt organisasjonens filosofi om å gi tilbake til lokalsamfunnet av overskuddet. Og for IT-avdelingen er overskuddet sikkerhetsinformasjon, som kan gi den konsekvens at ved å nå ut til kundene raskt nok med denne informasjonen kan man minimere skadene IK har på nettbankkundene deres, og nettbankbrukere generelt også. I datainnsamlingen har jeg ikke tatt inn informasjon om hvor mye dette har kostet SB1 av ressurser, men de har tidligere også måttet håndtere informasjon om sikkerhet ut mot kunder, men kanskje ikke på en så direkte og aktiv måte. Hva som kostet mest med tanke på ressurser i forhold til denne prosessen før og etter paradigmeinnovasjonen, kan det ikke uttales noe om i denne oppgaven. Det eneste som kan nevnes, er det inntrykket jeg tydelig fikk fra samtlige av informantene til oppgaven: de tar sikkerhet og IK på alvor, og de vil jobbe for å minimere og håndtere IK.

> *Dette kan ses på som et våpenkappløp. På den ene siden har du de kriminelle som stadig utvikler ny angrepskode, mens på den andre siden har vi oss myndigheter og andre som jobber med å møte angrepene. Dette kappløpet krever en rask teknologisk utvikling innenfor fagfeltene utvikling, oppdagelse og analyse.* (Lillevik, seksjonssjef ved Norwegian Computer Emergency Response Team (NorCERT), dybdeintervju)

Dette kan kanskje antyde en annen interesse i å innovere mot IK, selv om kostandene ikke skal overgå den verdi organisasjonene har gitt innovasjonsnytten. I følge Marshall S. Poole (2004, 27) innebærer innovasjon og endringer lidenskap, fordi slike prosesser krever engasjement og forpliktelse for at de skal lykkes. Endringer i omgivelser kan for eksempel

tvinge organisasjoner til å endre ting de har lagt ned mye energi og ressurser i, og kan påvirke følelser (ibid.).

Samtidig har man Kripos, som må beregne om det er en nytte som kan rettferdiggjøre ressursbruken. Og Norman utvikler sikkerhetsløsninger for kommersielt salg, og krever at det er en finansiell nytte for Norman selv.

Innovasjon må ha en opplevd nytte for at det skal bli tatt i bruk og dermed bli en innovasjon. Alle caseinnovasjonene har vist en nytte. De har alle kommet som følge av en form for behovstrekk skapt av IK, og ved hjelp av kunnskap de har, har det blitt skapt løsninger, innovasjoner, som har fylt behovet helt eller delvis med kunnskapsdytt (Tidd og Bessant 2009, 229-233).

6.2.3 Nødvendighet og mulighet – bruker og produsent

Innenfor entreprenørskap snakker man om nødvendighetsdrevne entreprenører og mulighetsdrevne entreprenører (Reynolds m.fl. 2001). Dette er en enkel distinksjon som kan anvendes om oppgavens innovasjoner. Det vil være snakk om *opplevd* nødvendighet, som i likhet med nytte er et tøyelig begrep. Tre av innovasjonene var nødvendighetsdrevne for innovatørene, men for én av dem var det en mulighetsdreven innovasjon. Dette sammenfaller med at det var tre brukerinnovasjoner og én produsentinnovasjon blant casene (von Hippel 2005, 3). Den mulighetsdrevne innovasjonen var NSP fra Norman, hvor behovet og nødvendigheten lå hos en potensiell kunde, en ledebruker (von Hippel 2005, 4), mens innovasjonen for Norman ble en mulighet i å løse problemet eller dekke behovet til denne kunden og samtidig selv å få en finansiell profitt, en bedriftsøkonomisk gevinst (Godø 2008, 23).

Innovasjonsmuligheter beskrives som utfordringer ved negative endringer i omgivelsene, som dermed åpner for muligheten til å løse disse (Lipsey, Carlaw og Bekar 2005, 69). Også positive endringer i omgivelser kan utnyttes som innovasjonsmuligheter (ibid.). Ut fra denne forståelsen vil alle caseinnovasjonene være resultat av innovasjonsmuligheter som har vært i omgivelsene. Dette fordi endringen i omgivelsen som følge av IK har skapt behov som igjen har gitt innovasjonsmuligheter, og blitt møtt med innovasjon fra caseorganisasjonene.

6.2.4 Endring, tilpasning og organisasjonsutvikling

Ifølge organisasjonsteori er organisasjoner i kontinuerlig endring grunnet endringer i eksterne forhold, og endringer i miljøet organisasjoner befinner seg i (Child og Kieser 1981, 28). Disse endringene i det eksterne kommer blant annet av innovasjoner i omverdenen, konkurranse og offentlig etterspørsel og statlig politikk (ibid.). Dette medfører krav til organisasjoner om endrede prosesser, produkter og strategier for at organisasjoner skal kunne klare å opprettholde sitt nåværende operasjonsnivå (ibid.). Dermed støtter dette antagelsen om at organisasjoner er i samutvikling med sine omgivelser (Nelson 1994). Organisasjoner kan utvikle seg til både det bedre og det verre, det vil si med hensyn til organisasjoners evne til å utføre sine oppgaver (Child og Kieser 1981, 28, 30).

Lovløs innovasjon og lovløse brukere medfører endringer i de eksterne forholdene til blant annet ikke-kriminelle organisasjoner (Flowers 2008, 180; 2007, 5), som vil si at det er en aktører som påvirker omgivelsene til andre aktører. For Kripos for eksempel, handlet det om at pedofile begynte å anvende mer moderne teknologi og utvikle avanserte løsninger i deling av barnepornografi seg i mellom. Dette er en slags lovløs innovasjon som medførte at Kripos måtte finne en ny metode for å få avslørt de pedofile og samtidig få sanket bevis. De kriminelle endret omgivelsene til organisasjonene i casene, ved å endre miljøet på Internett og anvendelsen av Internett og ulike tjenester som tilbys her.

Flowers (2007, 2008) har sett på hvordan lovløse innovasjoner og lovløse brukere har medført tilpasning i ikke-kriminelle organisasjoner, og hvordan de gjennom sin aktivitet har supplert kommersielle innovasjonsprosjekter og innovasjonsprosesser. Lovløshet kan medføre nye og bedre produkter og nye markeder i den ikke-kriminelle verdenen (Flowers 2007, 3). Han illustrerer hvordan lovløs bruk og lovløs innovasjon både kan medføre motstand og tilpasning fra firmaer. Dette gjøres ved at lovløse modifiserer og anvender produkter og systemer for å gjøre ting utenom det de originalt var skapt for, og er dermed brukere som fungerer som aktører for teknologisk utvikling (Flowers 2007, 2008; Kline og Pinch 1996).

Innovasjon handler som nevnt ikke bare om å øke konkurransefortrinn, vekst og finansiell nytte, men handler i like stor grad om å holde seg på samme nivå (Child og Kieser 1981, 28, 30). Det handler blant annet om hvordan organisasjonen klarer å løse sine oppgaver (Child og Kieser 1981, 30), håndtere usikkerhet og uventede hendelser (Cyert og March 1963, 99), økende turbulens (Terreberry 1968, 606), og økende kompleksitet (Emery og Trist 1965, 21) i

omgivelsene. Endring og turbulens i samfunn, økonomi og teknologi kan skape kriser og trusler for organisasjoner. For å minimere disse, må organisasjoner tilpasse seg, noe som vil medføre endring. Disse endringene vil i mange tilfeller kunne være innovasjoner. Endringer et sted vil ofte føre til en kjedereaksjon, ved at den tvinger andre til å tilpasse seg og dermed endre seg (Lipsey, Carlaw og Bekar 2005, 4; Normann 1971, 1; Zaltman, Duncan og Holbek 1973, 6, 110). Det er en kjede av årsak-virkning (Lipsey, Carlaw og Bekar 2005, 4). Det handler altså om overlevelse, og om eksistensberettigelsen for en organisasjon. Det handler om tilpasning og endring som medfører organisasjonsutvikling og innovasjon. Innovasjon medfører alltid endring i rutiner, men endring trenger ikke nødvendigvis medføre innovasjon (Nelson og Winter 1982, 128; Zaltman, Duncan og Holbek 1973, 158). Casene illustrerer at innovasjoner som er drevet frem av IK, både kan ha blitt utviklet for å øke markedsandeler eller for å klare holde seg på samme nivå, det vil si å kunne fortsette med noe av det man allerede gjør.

6.2.5 Innovasjonsnytte og gevinst for organisasjoner

Organisasjoner vil ha ulik opplevd nytte av å innovere på grunn av IK, på bakgrunn av blant annet hva slags organisasjon det er og hvordan den rammes. Nedenfor nevnes kort noe av den mest synlige nytten noen ulike organisasjoner kan ha.

Nytten av å innovere som reaksjon hvis man kan rammes av IK og informasjonssikkerhetshendelser for de fleste norske virksomheter, er å minimere de økonomiske tapene. Økonomiske tap kan være direkte eller indirekte tap som følge av en hendelse. Mange virksomheter er i følge Kristine Beitland (direktør i Næringslivets Sikkerhetsråd (NSR), dybdeintervju) utsatt for IK eller informasjonssikkerhetshendelser uten å være klar over det. Årsaken er ofte manglende monitorering og logging av hendelser som er helt sentralt for å avdekke og forebygge sikkerhetshendelser. Ofte er det uskyldige e-poster skreddersydd for å infisere datasystemer. At en ansatt klikker på et ondsinnet e-postvedlegg, kan være nok til at datasystemer blir infisert. Videre forteller Beitland at det til Nasjonal sikkerhetsmyndighet ble rapporterte at en virksomhet hadde tapt posisjon i kontraktsforhandlinger verdt flere hundre millioner kroner som følge av informasjonsspionasje fra en konkurrent. En annen virksomhet rapporterer om stadig angrep via e-post, og har regnet ut at et vellykket angrep kan koste flere titalls millioner i direkte tap. Det kan dreie seg om informasjon som er vesentlig for kjernevirksomheten, deres konkurransefortrinn eller de planer virksomheten er tuftet på i fremtiden. I verste fall kan for

eksempel en konkurrent skaffe seg tilstrekkelig informasjon til å søke patent på en annen virksomhets forretningsidé. Dette kan også svekke omdømme og tillitt hos kunder, brukere og samarbeidspartnere forteller Beitland (NSR, dybdeintervju).

Nytten for disse organisasjonene er at man ved å innovere, for eksempel gjennom implementering av teknologi eller nye tankesett, kan øke inntjening og minimere sjansen for tap. I tillegg vil tillitten til organisasjonen trolig være høyere. Den økonomiske nytten kan være vanskelig å identifisere konkret. Særlig hvis man ikke vet at man er blitt rammet, eller hvis man har innovert og dermed ikke nødvendigvis kan vite hva tapet ville ligget på hvis man ikke hadde innovert. Men etter estimerte tall fra NorCERT kan det vise seg å være veldig dyrt å ikke innovere (NorCERT 2011, 19; NorCERT 2012, 21; NSR 2012, 19). Samtidig har du nytten av innovasjoner i offentlig organisasjoner eller ikke-profitt organisasjoner, som kan være ulike ting avhengig av målet med organisasjonen. For politiorganisasjoner kan nytten av å utvikle nye og tilpassede etterforskningsmetoder medvirke til høyere oppklaringstall og et tryggere samfunn, og ellers være med på å effektivisere måloppnåelsen Stortinget har satt for dem. Man har også nytten av å innovere som følge av IK ved å utnytte markedsmuligheten det gir. Fordi det oppstår et sikkerhetsbehov som følge av IK, kan man fylle dette behovet ved å lage sikkerhetsløsninger som dekker det. Nytten disse kan ha, er blant annet forretningsutvikling, økte inntekter og økte markedsandeler.

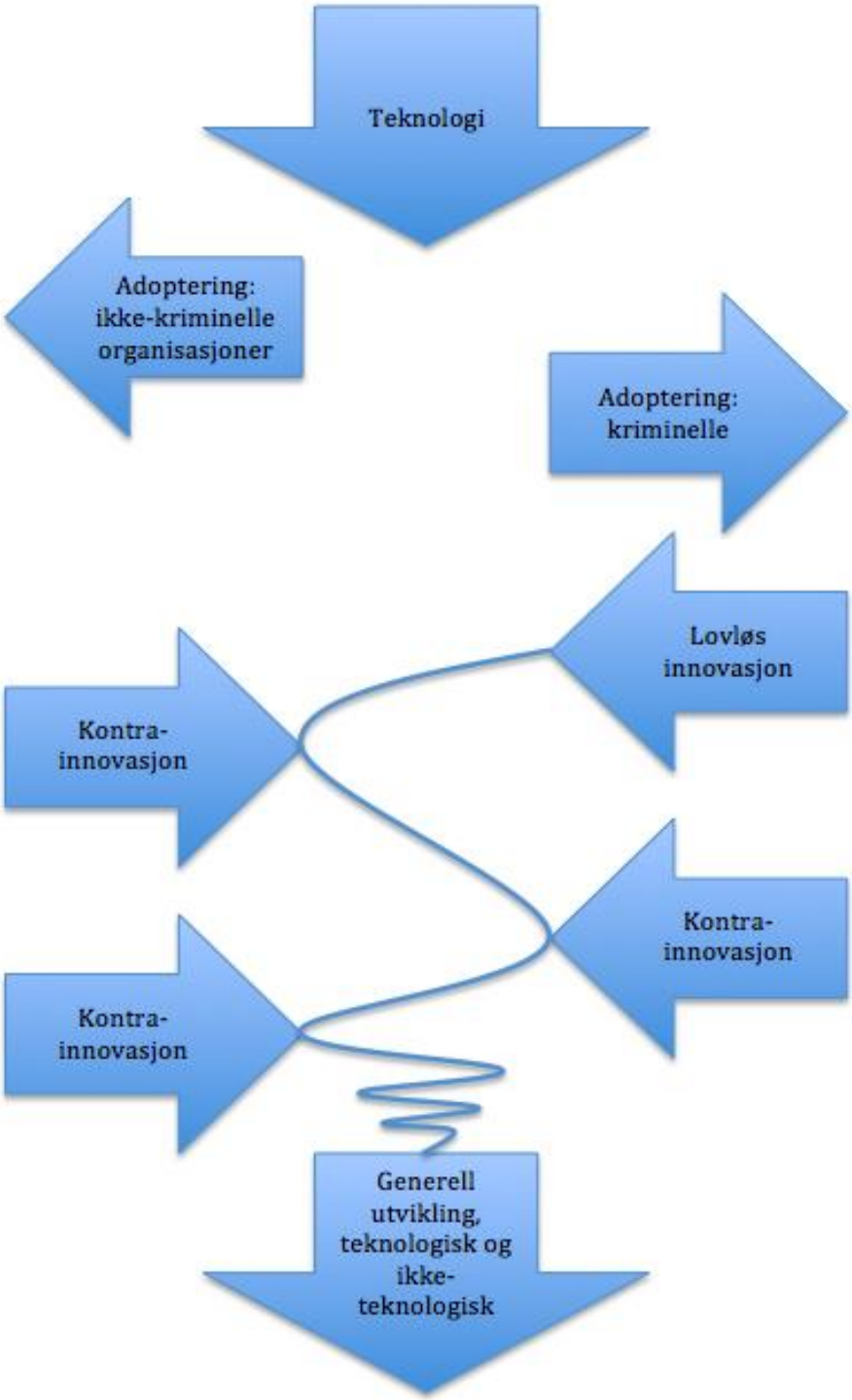
Mye av denne nytten er koblet opp mot bedriftsøkonomiske- og privatøkonomiske gevinster for organisasjoner (Godø 2008, 23-24). Men det kan også være tilfeller hvor det i større grad dreier seg om en velferdsgevinst og en samfunnsøkonomisk gevinst enn direkte nytte for organisasjoner (ibid.), noe flere av casene i denne oppgaven antyder.

6.3 Kontrainnovasjon

«We live today in a world of rapid economic change and social change. Any one change typically causes other changes, which in turn cause others, and so on in a concatenation of linked causes and effects.» (Lipsey, Carlaw og Bekar 2005, 4)

Enkeltendringer vil vanligvis medføre andre endringer, og slik går det videre i et slags nettverk av årsak og effekt (Lipsey, Carlaw og Bekar 2005, 4). På den måten kan en aktørs endringer og utvikling påvirke andre aktører gjennom at omgivelsene de deler, blir påvirket og krever tilpasning eller at en aktør direkte påvirker en annen aktør. Dette beskriver også den

dynamikken man ser i forhold til lovløse innovasjoner og innovasjoner i ikke-kriminelle organisasjoner. De kriminelle ser muligheter til å utnytte at flere og flere velger å anvende Internett. Disse mulighetene utnytter de, og dette rammer på mange samfunnsnivåer, enkeltindivider og private og offentlige organisasjoner. Etter hvert som trusselen eller hendelser oppleves som så truende eller alvorlige at organisasjoner ikke lenger kan gjøre som de pleier, vil dette medføre et behov for å gjøre endringer, for å tilpasse seg denne nye trusselen som er i miljøet. Dette kan gjøres på ulike måter, som casene har illustrert. von Hippel (2005, 1) skriver at det skjer en demokratisering av innovasjon når flere og flere får tilgang til informasjonsteknologi, og antall brukerinnovasjoner øker. Dette vil trolig medføre økning i antall kriminelle innovasjoner, som dermed trolig vil tvinge frem innovasjon fra ikke-kriminelle (Flowers 2007, 7, 14; 2008). Som et mulig resultat av dette vil teknologien utvikle seg enda raskere enn det vi har sett tidligere.



Figur 6.1. *Kontrainnovasjonsmodell for IK-drevet innovasjonskappløp*

Figuren illustrer det dynamiske forholdet hvor IK er en pådriver for innovasjon i ikke-kriminelle organisasjoner. Fordi den ene siden innoverer for å håndtere mulighetene eller behovet den andre siden skaper, må den motsatte siden videreinnovere. Slik driver de hverandre fremover i en spiral eller kjede av årsak-virkning, som igjen former og driver den teknologiske utviklingen samt prosessene rundt.

Jeg har valgt å kalle denne dynamikken *kontrainnovasjon*. Kshetri (2010, 21) skriver at man kan sammenligne IK med krig, derfor synes kontrainnovasjon å være et passende begrep. Det vil trolig alltid være flere faktorer som spiller inn i innovasjoner, som for eksempel mennesker, organisasjonskultur og lovverk. Men i innovasjonene jeg har illustrert gjennom de fire casene i denne oppgaven, har fellesnevneren i samtlige vært IK. IK har ikke alene drevet frem disse innovasjonene, det er teknologi og samfunnsstrukturer blant annet, og sikkert også tilfeldigheter. Men kanskje har IK vært en pådriver, som er et fenomen som påskynder eller tvinger frem noe (Bokmålsordboka 2010).

Som nevnt innledningsvis i denne oppgaven kan man kanskje delvis tolke IK som en pådriver - en *endringsagent* (Rogers 1983, 28, 312). Fordi de påvirker diffusjonen av sine egne ønskede innovasjoner, og gjennom dette påvirker ikke-kriminelle organisasjoner til å kontrainnovere. Gjennom disse kontrainnovasjonene i ikke-kriminelle organisasjoner, kan man samtidig tolke disse som endringsagenter. Dette fordi disse innovasjonene er drevet frem for å minimere eller sinke diffusjonen av den kriminelle innovasjonen og den kriminelle bruken, som er uønsket av disse organisasjonene (Rogers 1983, 28, 312). Modellen viser et system med aktører som påvirker hverandre og er i samutvikling på grunn av hverandre, og det er en dynamisk prosess uten sluttpunkt.

6.4 Kappløpet i kyberrommet

«Now, *here,* you see, it takes all the running *you* can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!»
(Carroll [1896] 2009, 145)

Kriminalitet er et samfunnsfenomen som, i likhet med den teknologiske utviklingen, har eksistert i tusener av år. I denne oppgaven har jeg forsøkt å illustrere hvordan IK har drevet frem innovasjoner i ikke-kriminelle organisasjoner. Disse er kommet som en del av samhandlingen mellom mennesker og teknologi, og denne samhandlingen driver frem en videre utvikling både teknologisk og ikke-teknologisk, hvor ikke kunnskapsdytt men behovstrekk er hovedgrunnen. Internett ble skap av det amerikanske forsvaret og det var kunnskapen som hovedsakelig drev frem internetteknologien i dens første tiår. Men etter hvert har utbredelsen av Internett i samfunnet medført at kriminelle har sett muligheter på Internett de også, og at dette har medført en trussel og risiko for de som er tilknyttet Internett.

Dette har igjen medført tilpasninger fra samfunnet, og noen av disse kan betraktes som innovasjoner, eller mer presist, som kontrainnovasjoner. Denne oppgaven har presentert og analysert fire caser representert gjennom forskjellige ikke-kriminelle organisasjoner i Norge som har skapt ulike typer innovasjoner på grunn av ulike behov eller muligheter som IK har gitt dem. Disse innovasjonene er et forsøk på, på en eller annen måte, å forsvare de ikke-kriminelle på Internett mot trusselen IK utgjør. Etter hvert som noen hull blir tettet igjen for de kriminelle, finner de seg andre hull og måter å skade mennesker og organisasjoner på. Disse kriminelle innovasjonene er også kontrainnovasjoner. Det vil si at de er i samutvikling i en dynamisk prosess uten sluttpunkt, som minner om et kappløp. Jeg definerer kontrainnovasjoner til å være innovasjoner som kommer som en følge av annen innovasjon som prøver å bryte ned den andre sidens interesser. Det er ikke her snakk om markedskonkurranseinteresser, og jeg forbeholder begrepet til å gjelde kriminalitets- og militærforhold. Her har det lenge manglet et passende begrep, som skiller denne type innovasjoner fra den der man hovedsakelig snakker om finansiell nytte, kommersielle interesser og markedskonkurranse.

IK er i stor grad utenfor de fleste ikke-kriminelles kontroll, men man kan håndtere det ved å beskytte seg midlertidig med en kontrainnovasjon. Slike kontrainnovasjoner skaper en egen dynamikk fordi det er en selvforsterkende prosess uten sluttpunkt - kontrainnovasjon vil skape nye former for IK. Det er en stiavhengig og evolusjonær prosess, fordi det bygger videre på tidligere innovasjoner, kunnskap og teknologier samt kommer som følge av konsekvensene andre aktørers endringer har på omgivelsene og andre aktører igjen (Freeman 1991; Nelson 1994; Perez 1983, 2010). Innovasjonene jeg har illustrert gjennom casene har alle til felles at de er forsøk på å få tilbake litt kontroll og makt eller i hvert fall utligne.

Sitatet over fra Alice i eventyrland, kan anvendes til å beskrive situasjonen som skapes av de to sidene som driver hverandre. Man må holde samme tempo, altså kontre hver kriminelle innovasjon med en egen innovasjon for å håndtere den kriminelle innovasjonen, hvis ikke vil man ikke klare seg i det lange løp i omgivelsene. Og hvis man skal klare å komme mye lenger frem enn de kriminelle, må man være dobbelt så rask i utviklingen og innovere oftere og bedre.

«*[…] her ligger, for å si det litt brutalt, kjeltringen et hakk foran.*» (Beitland, NSR, dybdeintervju)

6.5 Oppsummering

I dette kapittelet har jeg forsøkt å drøfte og komme med teorier og litteratur som kan forklare hvordan IK kan forstås som pådriver for innovasjon i ikke-kriminelle organisasjoner. Ved å gjøre dette har jeg forsøkt å sette caseanalysene i en større og mer generell kontekst, og drøfte problemstillingen. Det er brukt litteratur fra ulike disipliner, men hovedsakelig innovasjons- og organisasjonslitteratur, med en overordnet evolusjonær tilnærming.

I tillegg la jeg frem kontrainnovasjonsmodellen, hvor jeg gjennom denne og begrepet *kontrainnovasjon* forsøker å sette et navn på det oppgaven har hatt til hensikt å illustrere, når det hittil er et understudert fenomen og som ikke er blitt gitt et eget begrep.

7.0 Konklusjon

Formålet med denne oppgaven har vært å vise hvordan internettkriminalitet (IK) kan forstås som en pådriver for innovasjon i ulike ikke-kriminelle organisasjoner på ulike måter, ved å drøfte problemstillingen: *Hvordan kan internettkriminalitet være en pådriver for innovasjon i ikke-kriminelle organisasjoner?* Dette er blitt gjort ved først å svare på forskningsspørsmålet: *Hva slags innovasjoner kan komme som følge av internettkriminalitet i ikke-kriminelle organisasjoner?* gjennom å presentere og analysere fire caser som alle er fire ulike innovasjoner, og kategorisere og typologisere disse ut fra innovasjon- og kyberkriminalitetslitteratur.

Alle casene viser helt ulike typer organisasjoner med ulike forhold til IK. Videre har jeg drøftet hvordan IK overordnet kan være en pådriver for innovasjon hos ikke-kriminelle organisasjoner, og forklart denne innovasjonsdynamikken med en modell og et nytt begrep: *kontrainnovasjon*.

Hensikten har vært å vise hvordan kriminalitet generelt og IK spesifikt er med å drive innovasjon og utvikling, både av teknologisk og ikke-teknologiske karakter. Internettkriminalitet kan føre til ulike innovasjoner, og kan fungere som hva jeg kaller en *pådriver* for disse. Type innovasjon er avhengig av hva slags IK som berører organisasjonen, på hvilken måte organisasjonen påvirkes og hva slags organisasjon det er.

Kripos' infiltreringsprogramvare er en metodeinnovasjon hvor hovedgevinsten av innovasjonen er velferdsmessig. Det er en brukerinnovasjon, da hensikten med innovasjonen for Kripos var å bruke den som et verktøy for å sanke bevis i en større sak. Denne innovasjonen er en kontrainnovasjon mot annengenerasjons datainnholdskriminalitet. Norman SCADA Protection viser at man kan være produsent og innovere for å imøtekomme en etterspørsel i markedet ved å anse IK som en markedsmulighet. Norman har gjennom denne produktinnovasjonen fått en bedriftsøkonomisk gevinst, som er en kontrainnovasjon mot tredjegenerasjons kyberkriminalitet, som kan karakteriseres som dataintegritetskriminalitet. Dette er en produsentinnovasjon, da de har til hensikt å selge produktet til andre brukere. SpareBank 1 har paradigmeinnovert, noe som ut fra de to hovedkategoriene til von Hippel (1988, 2005) må karakteriseres som brukerinnovasjon, da innovasjonen ikke skal selges, men er integrert internt i IT-avdelingen. Dette er en innovasjon som er rettet mot behovet for informasjon til kunder for at de best skal kunne beskytte seg mot IK-trusselen, som er rettet

mot dem som nettbankkunder. Denne innovasjonen gir hovedsakelig en velferdsgevinst, og er først og fremst rettet mot annen- og tredjegenerasjons dataassistert kyberkriminalitet. Til slutt er det Underworld, som er en 100 prosent ikke-profitt organisasjoninnovasjon. Med dette mener jeg at organisasjonstypen og modellen som Underworld i seg selv er, er en innovasjon. Denne innovasjonen er vanskelig å klassifisere, i forhold til hvilken rolle den har i det funksjonelle innovasjonsforholdet. Men ut ifra hovedkategoriene må det bli en brukerinnovasjon, men en annen type rolle hadde kanskje også vært hensiktsmessig. Denne innovasjonen gir hovedsakelig en velferdsmessig gevinst, men også en utpreget samfunnsøkonomisk gevinst, når denne innovasjonen jobber 100 prosent ikke-profitt på arbeid som metodeinnovasjoner og med å begrense og avverge skader som ville gitt store utgifter, som ellers trolig ville belastet samfunnet. Underworld er i dag i stor grad en kontrainnovasjon mot tredjegenerasjons dataassistert- og dataintegritets kyberkriminalitet.

Alle casene viser at de er en respons på et behov (behovstrekk) som er oppstått som følge av ulike former for IK. Ulike former for IK, medfører ulike behov, som blir løst på ulike måter ut ifra hvem som skal imøtekomme behovene med kunnskap (kunnskapsdytt).

Samtlige av casene er et resultat av de endringer IK delvis har skapt i organisasjonenes omgivelser, enten de har løst det ut fra en mulighetstilnærming eller ut fra opplevd nødvendighetstilnærming.

Casene kan derfor tyde på at IK, ut ifra miljø- og omgivelsestilpasninger, medfører endrings- og tilpasningsbehov for organisasjoner som i casetilfellene medførte endringer som kvalifiserer som innovasjoner. Dermed antyder denne komparative caseundersøkelsen at internettkriminalitet kan være en pådriver for innovasjon i ulike ikke-kriminelle organisasjoner. Allikevel er denne undersøkelsen for liten til å kunne trekke konklusjoner utover denne oppgaven, samt at den er den første som ser på denne problemstillingen. Det trengs derfor mer forskning og større undersøkelser på dette feltet for at man skal kunne konstatere at IK kan være en pådriver for innovasjon i ikke-kriminelle organisasjoner, og at det er en innovasjonsdynamikk som antydet i begrepet og modellen om kontrainnovasjon.

7.1 Implikasjoner og forslag til videre forskning

Forhåpentligvis har mitt bidrag i form av denne oppgaven gitt innsikt og vekket nysgjerrighet, slik at andre forskere vil gå videre med studier som går enda mer i dybden på dette feltet. Et felt som er veldig aktuelt for det transnasjonale verdenssamfunnet vi i dag lever på Internett.

Denne oppgaven har handlet om et system hvor ulike aktører påvirker hverandre. Ikke-kriminelle organisasjoner, internettkriminelle, teknologi og kontrainnovasjoner. Innovasjon handler ofte om å håndtere negative konsekvenser og nød. Sult, energikriser og drivhuseffekten er eksempler på fenomener mennesker forsøker å løse ved hjelp av innovasjon. Dette er fenomener som trolig kan løses permanent gjennom innovasjon. Men kriminalitet virker som å være et sosialt fenomen som ikke kan løses permanent med innovasjon, og et fenomen som utvikles og tilpasses den teknologiske utvikling slik store deler av det sosiale miljøet gjør. Det kan virke som om kriminalitet er en integrert og permanent del av det sosiale miljø, og lar seg påvirke av teknologi, innovasjon, økonomi og mye mer. Forbindelsen med kriminalitet er kanskje «forbudt», men ikke mindre relevant og realistisk. Nytten av denne oppgaven er en erkjennelse av en faktor man i stor grad ikke har anerkjent innenfor innovasjonsforskningen: kriminalitet. Å forstå fenomenet internettkriminalitet som en del av det sosiale miljø og en aktør i prosessen for samutviklingen av teknologi og innovasjon, samt alt som igjen lar seg påvirke av dette. Kriminalitet er en del av innovasjonssystemet og samfunnet på godt og vondt.

Implikasjoner for praksis

Gjennom mine intervjuer kom det frem noen poenger i forhold til implikasjoner som IK og innovasjon har for praksis. Det ble nevnt behov for økt kunnskapsdeling mellom ulike miljøer og organisasjoner og institusjoner som jobber mot IK. I tillegg ble det nevnt at det måtte settes mer fokus på forskningssiden av dette. Særlig mot å bygge opp forskningsmiljøer og klustere innen ulike felt innenfor informasjonsteknologi (IT) og IT-sikkerhet. Dette vil trolig være helt nødvendig hvis det skal være mulig å håndtere den økte mengden av IK og dens nye former.

Et aspekt rundt dette ved mer kunnskapsdeling og forskning er at det må være en balanse mellom åpenhet og hemmeligholdelse. Forskning skal typisk publiseres og være offentlig tilgjengelig. Her bør det kanskje vurderes om noen forskningsprosjekter i større grad skal ha mulighet til å være unntatt fra offentligheten, når funnene kan være kritiske i kampen mot

internettkriminalitet, og når misbruk av funn fra kriminelle kan gi de kriminelle fortrinn i kappløpet i kyberrommet.

Implikasjoner og forslag for forskning

Denne oppgaven er blant de helt første på sitt felt, og har tatt utgangspunkt i de ikke-kriminelles innovasjoner og deres forståelse av hvordan IK er en medvirkende årsak og kan anses som pådriver for disse innovasjonene gjennom kvalitativ komparativ caseundersøkelse. Det er derfor nødvendig med mer forskning på området. Forskning på dette feltet innenfor innovasjonsstudier, men også innen science and technology studies (STS), kan gi en dypere forståelse av hvorfor noen innovasjoner blir til, hva som er grunnen til innovasjonen, både ved å forstå behovet den forsøker å dekke, og hvilken nytte innovatøren og andre kan ha av den. Det vil allikevel være svært hensiktsmessig å studere det jeg i denne oppgaven omtaler som kontrainnovasjoner fra de kriminelles perspektiv. Hovedutfordringen med dette vil trolig være å komme i kontakt og få innpass i disse miljøene. I tillegg vil anonymisering være nødvendig for å beskytte disse informantene. Mulige måter å komme i kontakt med de internettkriminelle på i starten kan være på de store konferansene som Black Hat og Defcon, eller man kan komme i kontakt med dem over Internett, hvor man allerede er anonymisert. Men kun å være i kontakt med anonyme informanter gjennom Internett kan være problematisk i forhold til en undersøkelses validitet og reliabilitet. Interessant vil det også være å se på samme teknologi, og hvordan den gjennom spiralen eller kjeden av kontrainnovasjoner, gjennom årsak og effekt, former teknologien gjennom innovasjonene og de påvirkende faktorene. For STS vil det trolig også være interessant å løfte blikket, og se på de større konsekvensene dette har for samfunnet.

I denne oppgaven har jeg forholdt meg til et innovasjonsrammeverk som på noen måter kanskje er for begrensende. Kanskje eksisterer det foreløpig ikke noen bedre innovasjonsrammeverk, men jeg oppfordrer andre til å se etter annen litteratur og teori ved videre forskning på emnet. Allikevel synes jeg oppgaven er et viktig bidrag i den forstand at den kanskje nettopp illustrerer denne begrensningen i innovasjonslitteraturen.

7.2 Avslutning

Jeg håper at denne oppgaven har vekket nysgjerrighet og gitt innsikt i en spennende verden av innovasjon, i hvordan man kan se på internettkriminalitet som en pådriver for innovasjon. En bredere forståelse av hvordan innovasjoner blir drevet frem kan kanskje også vekke ny innsikt

i pådrivere for innovasjon innenfor andre felt enn internettkriminalitet, og generelt gi en dypere forståelse av fenomenet innovasjon.

Innovasjon er ikke forbeholdt de lovlydige, de kriminelles innovasjonsevner er kanskje desto bedre, fordi deres kreative evner kanskje ikke i like stor grad blir styrt av organisasjoners faste modeller og retningslinjer, av byråkrati og formell utdannelse. Man verken oppmuntrer til kriminalitet eller hedrer kriminelle ved å se på slike temaer. Det man bidrar til, er å gi kunnskap og bevissthet om den faktiske verden vi lever i. Brukere, både lovlydige og lovløse er med på å forme og drive frem innovasjon og teknologisk utvikling. Dette er viktige aspekter hvis man ønsker å få en bedre forståelse av hvorfor verden og teknologien etter hvert tar de former de gjør, men også for å få en mer farget forståelse av hvorfor man innoverer og hva slags innovasjoner det kan være.

> *Det er en fullstendig uforutsigbar verden. Vi vil alltid ligge etter. Det er helt klart. […] Det eneste vi vet, er at kriminelle aktører vil investere enda mer i avansert, ondsinnet kode, og at vi må gjøre vårt for å henge med. Men å forutse nøyaktig hvilken vei det går, det er helt umulig, […]*. (Lilleeng, Norman, dybdeintervju)

8.0 Litteraturliste

Aas-Hansen, Astri. 2004. *Barn som møter overgriper på internett: Fokus på rettspraksis.* Redd Barna rapport, 02/04. Lesedato 19. februar 2013: http://jmadmin.barlind.com/kunder/smi/filer/Barn_som_moter_overgriper_pa_nettet_-_Redd_barna.pdf

Adner, Ron og Daniel Levinthal. 2001. «Demand Heterogeneity and Technology Evolution: Implications for Product and Process Innovation.» *Management Science*, 47(5):611-628. Lesedato 7. januar 2013: doi:10.1287/mnsc.47.5.611.10482

Asheim, Bjørn og Meric S. Gertler. 2005. «The Geography of Innovation: Regional Innovation Systems.» I Fagerberg, Mowery og Nelson (red.) *The Oxford Handbook of Innovation,* 291-317. Oxford: Oxford University Press.

Barlow, John Perry. 1994. «The Economy of Ideas: A framework for rethinking patents and copyrights in the Digital Age. (Everything you know about intellectual property is wrong).» *Wired.* Lesedato 19. mars 2013: http://www.wired.com/wired/archive/2.03/economy.ideas_pr.html

Benz, Matthias. 2006. «Entrepreneurship as a non-profit-seeking activity. » *International Entrepreneurship and Management Journal*, 5(1):23-44. Lesedato 22. februar 2013: doi:10.1007/s11365-006-0031-y

Bergek, Anna, Marko Hekkert og Staffan Jacobsson. 2007. «Functions in innovation systems: A framework for analysing energy system dynamics and identifying goals for system-building activities by entrepreneurs and policy makers.» *R&D and Innovation*' *and 'Dynamics of Economies* og *Institute for Management of Innovation and Technology,* Working Paper No. 84426-008. Lesedato 25. april 2013: http://imit.se/pdf/reports/2007_153.pdf

Bokmålsordboka. 2010. «Pådriver.» Lesedato 18. februar 2013: http://www.nob-ordbok.uio.no/perl/ordbok.cgi?OPP=p%E5driver&bokmaal=+&ordbok=bokmaal

Brodeur, Jean-Paul. 1983. «High Policing and Low Policing: Remarks about the Policing and Political Activities.» *Social problems*, 30(5):507-520. Lesedato 7. januar 2013: doi:10.2307/800268

Carroll, Lewis. (1896) 2009. «Through the Looking-Glass, and What Alice Found There.» Ny fremstilling i samleverk med introduksjon og redigering av Peter Hunt i *Alice's Adventures in Wonderland* and *Through the Looking-Glass*, 113-245. New York: Oxford University Press.

Castells, Manuel. 2000. *The Information Age: Economy, Society, and Culture, Volume 1: The Rise of the Network Society.* 2. utg. Oxford: Blackwell.

Chesbrough, Henry W. 2003. «The Era of Open Innovation.» *MIT Sloan Management Review*, 44(3):35-41.

Chesbrough, Henry W. 2006. «Open Innovation: A New Paradigm for Understanding Industrial Innovation.» I Chesbrough, Vanhaverbeke og West (red.) *Open Innovation: Researching a New Paradigm*, 1-12. Oxford: Oxford University Press.

Child, John og Alfred Kieser. 1981. «Development of organizations over time.» I Nystrom og Starbuck (red.) *Handbook of Organizational Design, Volume 1: Adapting organizations to their environments*, 28-64. New York: Oxford University Press.

Cope, Meghan. 2010. «`Interpreting and Communicating´ Qualitative Research.» I Hay (red.) *Qualitative Research Methods in Human Geography*, 279-294. 3.utg. Ontario: Oxford University Press.

Cyert, Richard M., James G. March. 1963. *A behavioral theory of the firm.* Englewood Cliffs, New Jersey: Prentice-Hall.

Dehghanpisheh, Babak. 2012. «Attacked by "Flame": Will Iran Retaliate the Latest Cyberassult?» *Time*. 29.mai. Lesedato 21. mars 2013: http://www.time.com/time/world/article/0,8599,2115970,00.html

Dowling, Robyn. 2010. «Power, Subjectivity, and Ethics in Qualitative Research.» I Hay (red.) *Qualitative Research Methods in Human Geography*, 26-39. 3.utg. Ontario: Oxford University Press.

Dunn, Kevin. 2010. «`Doing´ Qualitative Research in Human Geography.» I Hay (red.) *Qualitative Research Methods in Human Geography*, 99-138. 3.utg. Ontario: Oxford University Press.

Edquist, Charles. 2005. «Systems of Innovation: Perspectives and Challenges.» I Fagerberg, Mowery og Nelson (red.) *The Oxford Handbook of Innovation*, 181-208. Oxford: Oxford University Press.

Emery, Fredrick E. og Eric L. Trist. 1965. «The Causal Texture of Organizational Environments.» *Human Relations*, 18:21-32. Lesedato 11. februar 2013: doi:10.1177/001872676501800103

Flowers, Stephen. 2007. «From Outlaws to Trusted Partners: Challenges in mobilising User-Centric Innovation in R&D projects » IRNOP VIII Project Research Conference, 19-21. september 2007, Brighton, UK. Lesedato 22. februar 2013: http://ebookbrowse.com/gdoc.php?id=34793656&url=44dd02729dd26f5c1da39d595387c5e6

———. 2008. «Harnessing the hackers: The emergence and exploitation of Outlaw Innovation.» *Research Policy*, 37(2):177-193. Lesedato 26. mars 2012: doi:10.1016/j.respol.2007.10.006

Freeman, Christopher. 1991. «Innovation, Changes of Techno-Economic Paradigm and Biological Analogies in Economics.» *Revue économique*, 42(2):211-231. Lesedato 8. april 2013: http://www.jstor.org/stable/pdfplus/3502005.pdf?acceptTC=true

Freeman, Chris og Luc Soete. 1997. *The Economics of Industrial Innovation.* 3 utg. London: Pinter.

Godø, Helge. 2002. «Rethinking computer hacking.» *VEST*, 15(2-3):7-34.

———. 2008. *Innovasjonsledelse: Teknologiutvikling fra idé til forretningsplanlegging.* Trondheim: Tapir Akademiske Forlag.

Hafner, Katie og Matthew Lyon. 1996. *Where Wizards Stay Up Late: The Origins of the Internet.* New York: Simon & Schuster.

Hirshleifer, Jack. 1998. «The Bioeconomic cause of war.» *Department of Economics*, Working Paper No. 777. Lesedato: 10. mai 2013: http://www.econ.ucla.edu/workingpapers/wp777.pdf

Johannessen, Asbjørn, Line Kristoffersen og Per Arne Tufte. 2004. *Forskningsmetode for økonomisk-administrative fag.* 2. utg. Oslo: Abstrakt forlag.

Kaspersky. 2012. *Advanced persistent threats: not your average malware.* Lesedato 21. mars 2013: http://media.kaspersky.com/documents/business/brfwn/en/Advanced-persistent-threats-not-your-average-malware_Kaspersky-Endpoint-Control-white-paper.pdf

Kripos. Lesedato 27.november 2012: https://www.politi.no/kripos/om_kripos/Tema_71.xhtml

Kripos' strategi 2011-2015. Lesedato 18.februar 2013: https://www.politi.no/vedlegg/lokale_vedlegg/kripos/Vedlegg_1466.pdf

Kline, Ronald og Trevor Pinch. 1996. «Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States.» *Technology and Culture*, 37(4):763-795. Lesedato 28. februar 2013: http://www.jstor.org/stable/pdfplus/3107097.pdf

Kshetri, Nir. 2010. The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. Berlin: Springer.

Kvale, Steinar. 2007. *Doing Interviews.* Red. Uwe Flick. En del av serien The SAGE Qualitative Research Kit. London: SAGE Publications Ltd.

Lipsey, Richard G. Kenneth I. Carlaw og Clifford T. Bekar. 2005. *Economic Transformations: General Purpose Technologies and Long-Term Economic Growth*. Oxford: Oxford University Press.

Malerba, Franco. 2005. «Sectoral Systems: How and Why Innovation Differs across Sectors.» I Fagerberg, Mowery og Nelson (red.) *The Oxford Handbook of Innovation*, 380-406. Oxford: Oxford University Press.

Mansfield, Edwin, John Rapoport, Anthony Romeo, Edmond Villani, Samuel Wagner og Frank Husic. 1977. *The Production and Application of New Industrial Technology*. New York: W. W. Norton & Company, Inc.

McCusker, Rob. 2006. «Transnational organised cyber crime: distinguishing threat from reality.» *Crime, Law and Social Change*, 46(4-5):257-273. Lesedato 28. februar 2013: doi:10.1007/s10611-007-9059-3

Nelson, Richard R., Sidney G. Winter. 1982. *An Evolutionary Theory of Economic Change.* Cambridge, Massachusetts: Belknap Press.

Nelson, Richard R. 1994. «The Co-evolution of Technology, Industrial Structure, and Supporting Institutions.» *Industrial and Corporate Change*, 3(1):47-63. Lesedato 6. april 2013: doi:10.1093/icc/3.1.47

NorCERT (Norwegian Computer Emergency Response Team). 2011. *NorCERT kvartalsrapport for 4. kvartal 2011*. Oslo: NorCERT. Lesedato 29. oktober 2012: https://www.nsm.stat.no/Documents/NorCERT/2012/Q4_web_lav.pdf

———. 2012. *NorCERT kvartalsrapport for 1. kvartal 2012*. Oslo: NorCERT. Lesedato 2. oktober 2012: https://www.nsm.stat.no/Documents/NorCERT/2012/Q1_2012_WEB.pdf

NorCERT 1. Lesedato 29. mars 2013: https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/

NorCERT 2. Lesedato 29. mars 2013. https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/Om-NorCERT/

Norman. About. Lesedato 9. november 2012: http://www.norman.com/about_norman/no

Normann, Richard. 1971. «Organizational Innovativeness: Product Variation and Reorientation.» *Administrative Science Quarterly*, 16(2):203-215. Lesedato 12. november 2012: http://www.jstor.org/stable/pdfplus/2391830.pdf

NorSIS (Norsk senter for informasjonssikkerhet). 2012. Fidus. Lesedato 8. januar 2013: http://www.norsis.no/Fidus/index.html

NSR (Næringslivets Sikkerhetsråd). 2012. *Mørketallsundersøkelsen™ 2012.* Oslo: NSR. Lesedato 18. september 2012: http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/moerketall_2012.pdf

O'Neill, Michael Edmund. 2000. «Old crimes in new bottles: sanctioning cybercrime.» *George Mason Law Review*, 9:237-288. Lesedato 26. mars 2012: http://heinonline.org/HOL/Page?handle=hein.journals/gmlr9&div=16&g_sent=1&collection=journals

Oudshoorn, Nelly og Trevor Pinch. 2003. «Introduction: How Users and Non-Users Matter.» I Oudshoorn og Pinch (red.) *How users matter: the co-construction of users and technology*, 1-25. Cambridge, Massachusetts: MIT Press.

Perez, Carlota. 1983. «Structural change and assimilation of new technologies in the economic and social systems.» *Futures,* 15(5):357-375. Lesedato 8. april 2013: doi:10.1016/0016-3287(83)90050-2

———. 2010. «Technological revolutions and techno-economic paradigms.» *Cambridge Journal of Economics,* 34:185-202. Lesedato 8. april 2013: doi:10.1093/cje/bep051

Poole, Marshall Scott. 2004. «Central Issues in the Study of Change and Innovation.» I Poole og van de Ven (red.) *Handbook of Organizational Change and Innovation,* 3-31. Oxford: Oxford University Press.

Ragin, Charles C. og Lisa M. Amoroso. 2011. *Constructing Social Research: The Unity and Diversity of Method.* 2.utg. Thousand Oaks, California: Pine Forge Press.

Rasch, Mark D. 1996. «Criminal Law and The Internet.» I Ruh (red.) *The Internet and Business: A Lawyer`s Guide to the emerging legal issues.* Computer Law Association. Lesedato 10.februar 2013: http://groups.csail.mit.edu/mac/classes/6.805/articles/computer-crime/rasch-criminal-law.html

Reynolds, Paul D., S. Michael Camp, William D. Bygrave, Errko Autio og Michael Hay. 2001. *Global Entrepreneurship Monitor; 2001 Executive Report.* United Nations Association of the Unites States of America og Business Council for the United Nations. Lesedato 21.februar 2013: http://unpan1.un.org/intradoc/groups/public/documents/un/unpan002481.pdf

Rogers, M. Everett. 1983. *Diffusion of Innovations*. 3. utg. New York: The Free Press.

Rose-Ackerman, Susan. 1996. «Altruism, Nonprofits, and Economic Theory.» *Journal of Economic Literature,* 34(2):701-728. Lesedato 13.mars 2013: http://www.altruists.org/static/files/Altruism,%20non-Profits%20and%20Economic%20Theory%20%28Rose-Ackerman,%201996%29.pdf

Rush, Howard, Chris Smith, Erika Kraemer-Mbula og Puay Tang. 2009. *Crime online; Cybercrime and illegal innovation.* NESTA rapport, juli/09. Lesedato 19.februar 2013: http://eprints.brighton.ac.uk/5800/1/Crime_Online.pdf

Schulz, Celine og Stefan Wagner. 2010. «Outlaw Community Innovations.» I Flowers og Henwood (red.) *Perspectives on user innovation*, 191-210. London: Imperial College Press.

Schulze, Michael. 2007. «Types of Innovation.» *BLOG.DATAORANGE.DE,* 7.juni. Lesedato 15.januar 2013: http://blog.dataorange.de/?p=48

Schumpeter, Joseph A. (1934) 1983. *The Theory of Economic Development: An Inquiry into Profits, Capital, Credit, Interest, and the Business Cycle.* Ny fremstilling av første utgave med en introduksjon av John E. Elliott. New Brunswick, New Jersey: Transaction Publishers.

Shadowserver. Lesedato 13.mars 2013: http://www.shadowserver.org/wiki/

Simon, Herbert A. 1971. «Designing organizations for an information-rich world.» I Greenberger (red.) *Computers, communications, and the public interest*, 37-72. Baltimore: Johns Hopkins Press.

Stacey, Ralph D. 1992. *Managing the Unknowable: strategic boundaries between order and chaos in organizations.* San Francisco: Jossey-Bass.

Stefoff, Rebecca. 2009. *Cybercrime*. New York: Benchmark Books.

Sterling, Bruce. 2010. «The Advanced Persistent Threat Attack.» *Wired*, 30. januar 2010. Lesedato 14.februar 2013: http://www.wired.com/beyond_the_beyond/2010/01/the-advanced-persistent-threat-attack/

Teece, David J. 1986. «Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy.» *Research Policy,* 15(16):285-305. Lesedato 19. mars 2012: doi:10.1016/0048-7333(86)90027-2

———, David J. 2006. «Reflections on "Profiting from Innovation".» *Research Policy,* 35 (8): 1131-1146. Lesedato 19. mars 2012: doi:10.1016/j.respol.2006.09.009

Terreberry, Shirley. 1968. «The Evolution of Organizational Environments.» *Administrative Science Quarterly*, 12(4):590-613. Lesedato 11.februar 2013: http://www.jstor.org/stable/pdfplus/2391535.pdf?acceptTC=true

Tidd, Joe og John Bessant. 2009. *Managing Innovation: Integrating Technological, Market, and Organizational Change*. 4. utg. Chichester: John Wiley & Sons, Ltd.

van de Ven, Andrew H. og Harold L. Angle. 2000. «An Introduction to the Minnesota Innovation Research Program.» I van de Ven, Angle og Poole (red.) *Research on the Management of Innovation: The Minnesota Studies*, 3-30. (Opprinnelig utgitt av Ballinger Publishing Company, Cambridge Massachusetts, 1989.) Oxford: Oxford University Press.

von Hippel, Eric. 1988. *The Sources of Innovation.* New York: Oxford University Press.

———. 2001. «Innovation by User Communities: Learning from Open-Source Software.» *MIT Sloan Management Review*, 42(4):82-86. Lesedato 29. mars 2013: http://ocs.kpcl.co.in:7778/content/dav/kpcl/workspaces/SHASHWAT/HR/Middle%20Management%20Development%20Program%20-%202012/Marketing%20Management/Innovation/ContentServer.pdf

———. 2005. *Democratizing Innovation*. Cambridge, Massachusetts: MIT Press.

———. 2007. «Horizontal innovation networks— by and for users.» *Industrial and Corporate Change*, 16(2):293-315. Lesedato 26. mars 2012: doi:10.1093/icc/dtm005

von Krogh, Georg og Eric von Hippel. 2003. «Special issue on open source software development.» *Research Policy*, 32(7):1149-1157. Lesedato 29. mars 2013: doi:10.1016/S0048-7333(03)00054-4

Wall, David S. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Webopedia™. «SCADA». Lesedato: 13. februar .2013 http://www.webopedia.com/TERM/S/SCADA.html

Yin, Robert K. 2009. *Case Study Research: Design and Methods.* 4. utg. Thousands Oaks, California: SAGE Publications, Inc.

Zaltman, Gerald, Robert Duncan og Jonny Holbek. 1973. *Innovations and organizations.* New York: John Wiley & Sons.

Vedlegg 1

Informanter og intervjudatoer

Organisasjon	Navn	Stilling	Dato
Norman ASA	Bjørn Lilleeng	Technology Integration Manager	05.09.2012
Næringslivets Sikkerhetsråd	Kristine Beitland	Direktør	19.09.2012
SpareBank 1	Mari Grini	Leder IT	19.09.2012
Underworld	Anders Hardangen	Grunnlegger	26.09.2012
Kripos	Rune Fløisbonn	Avdelingsdirektør for Datakrim	08.10.2012
NorCERT	Eldar Lillevik	Seksjonssjef	19.10.2012

Vedlegg 2

Intervjuguide (Caseintervju)

Om organisasjonene og konteksten

-Hva slags organisasjon er dette?

-Hva er det dere hovedsakelig driver med?

-Hvordan er det dere blir påvirket av internettkriminalitet?

-Hvilke trusler/risikoer utgjør det?

-Hva er behovet for å håndtere det (er det direkte hos dere, eller hos kunder, samfunnet)?

Samarbeider dere med noen?

Innovasjon og problemløsning

-Hvordan håndterer dere trusselen fortløpende?

-Hvordan jobber dere med metodeutvikling/etterforskningsstrategier/produktutvikling/organisasjon-utvikling for å forberede dere på hva som kan komme? Er det noen form for etterretningsarbeid?

-Har dere gjort konkrete tiltak internt i organisasjonen ettersom dere har merket at trusselen for internettkriminalitet har økt?

-Har dere kommet med noen konkrete løsninger/produkter/metoder/prosesser som er kommet som en direkte eller indirekte konsekvens av internettkriminalitet?

- Hva er dette?
- Prosessen rundt innovasjonen?
- Tjener dere penger, sparer dere utgifter, øker dere tillitten hos brukere eller annet positivt, som følge av innovasjonen?

-Bruker dere mest tid på reelle eller potensielle internettkriminelle innovasjoner/trusler?

-Prøver dere å være forut for trusselbilde, eller fortløpende håndtering?

(-konkrete innovasjoner på fortløpende, eller forut innovasjoner/løsninger)?

Kunnskapsmiljø

-Hvordan innhenter dere informasjon om internettkriminalitet?

-Deler dere deres egen kunnskap og erfaring? Evt. med hvem?

-Hvem samarbeider dere med for å håndtere IK? Er dere et miljø vil du si?

-Konkret trussel/angrep og konkret konsekvens for dere, hvordan håndterte dere det, hva ble løsningen?

Vedlegg 3

Avtale om informert samtykke

Under møtet/intervjuet har informanten rett til å avbryte, og ikke svare på spørsmål den ikke ønsker å svare på.

Hvis informant ønsker å være anonym i oppgaven har den rett til dette.

Hvis informant skulle ønske at noe som blir sagt under møtet/intervjuet ikke skal bli nevnt i masteroppgaven har den rett til å kreve at dette ikke forekommer. Man kan kreve at noe blir "slettet" fra møtet/intervjuet. Informanten har krav på å få se transkribering og analysen som omhandler eget intervju, hvis den ber om dette.

Eventuelle opptak og transkriberinger skal kun brukes av forskeren selv i selve arbeidet med oppgaven og særlig i dataanalysearbeidet, og skal ikke være tilgjengelig for andre. Transkriberinger og opptak destrueres når oppgaven er ferdigstilt.

Alt som blir sagt av informant under datainnsamling skal fremstilles riktig, og skal ikke misbrukes.

Kontaktinformasjon:

Student ved Senter for teknologi, innovasjon og kunnskap ved det samfunnsvitenskapelig fakultet ved universitetet i Oslo.

Student: Roxanne Colle

Tlf.: 46 85 97 07

E-post: ercolle@student.sv.uio.no

Dato:……..

Sted:……...

Sign. Informant Sign. Forsker/student

…… ……