POLITIET I MØTE MED CYBERKRIMINALITET

June Nerlien

Masteroppgave i kriminologi

Institutt for kriminologi og rettssosiologi

Juridisk fakultet

UNIVERSITETET I OSLO

22. Mai 2018

© June Nerlien

2018

POLITIET I MØTE MED CYBERKRIMINALITET

June Nerlien

https://www.duo.uio.no/

Trykk: Reprosentralen, Universitetet i Oslo

POLITIET I MØTE MED CYBERKRIMINALITET

Sammendrag

Tittel: POLITIET I MØTE MED CYBERKRIMINALITET

Forfatter: June Nerlien

Veileder: Katja Franko

Levert ved: Institutt for kriminologi og rettssosiologi

Våren 2018

Den globale bruken av Internett har ført med seg store forandringer i samfunnet. Norge er i dag et av mest digitaliserte land i verden. Denne utviklingen har også hatt sin innvirkning på kriminalitetsbildet. I risikorapporterter utsendt av PST (2018) og NSM (2016) kan man lese at nettverksteknologien åpner opp for store sårbarheter som utnyttes av de med kriminelle hensikter og at det et press på offentlige og private virksomheter til å respondere. Denne masteravhandlingen har som sitt formål å studere politiets møte med cyberkriminalitet i Norge. Sådan er ikke dette et studiet av cyberkriminalitet, men et studiet av hvordan cyberkriminalitet påvirker politiets kultur og arbeidspraksis. Avhandlingen er basert på dokumentanalyse og intervjuer med politiets spesialister på cyberkriminalitet. Informantene som har bidratt til oppgaven kommer fra ulike seksjoner, avdelinger og særorganer i politietaten, og har både sivilt og politibakgrunn. Gjennom det fenomenologiske perspektivet gir avhandlingen en beskrivelse av spesialistenes syn på verden og deres arbeidshverdag, og hvordan cyberkriminaliteten utfordrer tradisjonelle politikulturer.

Oppgaven viser at nettverksteknologien endrer strukturen på kriminalitetsutførelsen i så stor grad at politiet med sin tradisjonelle arbeidspraksis står ovenfor store utfordringer. Det å utøve makt på internett kan være vanskelig fordi politiets maktutøvelse hovedsakelig har belaget seg på en fysisk tilnærming. Informantene opplever at cyberkriminalitet er et ansvarsområde der politiet ikke strekker til og at det innenfor organisasjonen generelt er lite digitalt forståelse og lite vilje til å omstille seg. Fra historiene til informantene og fra rapporter utgitt av politidirektoratet (2015;2017), kommer det frem at det er et begrenset antall i politiet som besitter den kunnskapen som etaten er i behov av for å håndtere det økende omfanget av cyberkriminalitet.

Informantene opplever en politiorganisasjon som styres av en ledelse som defineres som «ikke-digitalinnfødte» og av en byråkratisk modell som prioriterer å holde fast på det stabile og innøvde. Dette skaper en frustrasjon for spesialistene som utvikler seg hurtig og i takt med samfunnsendringene. At spesialistene ser nye utviklingsbehov og ledelsen ikke gjør det kan skape en sterk solidaritetsfølelse mellom spesialistene, hvor solidariteten reflekteres i holdningene de har mot nåværende styresett. Avhandlinger viser at cyberkriminaliteten utfordrer generalistrollen og åpner nye behov for spesialistkompetanse og større rolle for sivile i politiet.

Avhandlingen viser også at politiets manglende tilstedeværelse på internett og deres begrensede effektivitet i møtet med cyberkriminalitet har resultert i at private aktører har i stor grad tatt over cyberkriminalitetsbekjempelsen. Avhandlingen analyserer potensielle konsekvenser av en slik utvikling, særlig for politiets fremtidige legitimitet.

TAKK!

Først og fremst ønsker jeg å ytre en stor takk til informantene mine som har stilt opp, vært åpne og gitt meg god innsikt i deres verden. Uten dere hadde ikke denne oppgaven blitt til. Samtalene med dere har lært meg utrolig mye og gitt meg god erfaring til å ta med meg videre. Tusen takk!

Jeg ønsker å takke min veileder Katja for gode tilbakemeldinger, for at du holdt meg på stø kurs og for at du har gitt meg verdifulle tips. Tusen takk for alt du har lært meg.

Takk til venninnene min Anne, for hjelp til korrekturlesing og oppmuntrende ord. Du er god.

Takk til lunsjklubben for gøyale samtaler, filmtips, boktips, støtte, felleskap og for å ha diskutert tematikker med meg høyt når jeg har trengt å sortere. Satser på fast podcast «lørdagsrådet-style» med dere i fremtiden.

Sist, men ikke minst ønsker jeg å takke mamma, pappa og min kjære bror. Takk for at dere alltid har tro på meg, ler med meg, oppmuntrer meg og alltid stiller opp. Spesielt takk til broen min som har gitt meg utrolig god og nyttig innsikt i nettverksteknologi. Uten deg hadde jeg vært litt lost.

Oslo, mai 2018

June Nerlien

Innholdsfortegnelse

1. Innledning

Den globale bruken av internett har ført med seg store forandringer i samfunnet. I dag kommuniserer, lagrer og deler vi informasjon på helt andre måter enn det vi har gjort tidligere. Norge ligger på fjerde plass i verden over de mest digitaliserte landene, og 96 prosent av den norske befolkning er på nett (NorSIS, 2016). Det har sin innvirkning på politiet. I 2016 skrev den daværende avdelingsdirektøren i Politidirektoratet (POD), Fred Hermansen, dette i en artikkel:

> *«Digitalisering av politiet vil bli avgjørende for å løse samfunnsoppdraget effektivt i årene som kommer. Når kriminaliteten endrer seg, må politiet også endre sin kompetanse, sine arbeidsmetoder og sin strategiske tenkning. Og vi trenger nye og bedre arbeidsverktøy for å jobbe smartere og mer effektivt enn i dag. Den teknologiske utviklingen gir helt nye muligheter for å være i forkant av kriminaliteten gjennom digitale tjenester og kunnskapsbasert, mobil og effektiv oppgaveløsing. Norsk politiet må gjennom et digitalt skifte innen 2025».*

Ut ifra utsagnet ovenfor kan man lese at politiet har satt et strategisk mål om at de innen 2025 skal ha gjennomført et digitalt skifte. Samtidig er politiet med jevne mellomrom utsatt for kritikk for deres håndtering av det digitale skiftet.

Kriminalitets som foregår ved bruk av nettverksteknologi sies å være i økning. Spesielt har det vært fokus på at det er ressurssterke, organiserte miljøer som står bak de mest alvorlige sakene. Cyberkriminalitet utgjør nå en stor del av internettsfæren, som igjen har store innvirkninger på borgere og samfunn. Cyberkriminalitet påvirker alt fra internasjonal økonomi, til sikkerhet, og sosiale, og politiske relasjoner (Thomas and Loader, 2000). Politiet som skal opprettholde lov og orden, må ta innover seg hva dette betyr. For oppgaven blir det derfor viktig å identifisere hvordan cyberkriminaliteten blir møtt i politiet. Oppgaven skal se på korrelasjonen mellom ytrestyringsprosesser, politiets kultur og politiets arbeidspraksis i møte med nye endringer. Historisk sett, er det ikke nytt at teknologi er med på å endre politipraksis. Det har den gjort siden det offentlige politi sin opprinnelse. Det er heller ikke uvanlig at politiet som offentlig, statlig instans stadig går igjennom omorganiseringer. Likevel, ser det ut til at nettverksteknologien endrer strukturen på kriminalitetsutførelsen i så stor grad, at politiets tradisjonelle arbeidspraksis står overfor utfordringer. Der hvor politiet tidligere kunne gjøre lokale og nasjonale beslutninger, har internett åpnet opp for

global rekkevidde og trender. Kriminalitetsforholdet har blitt asymmetrisk, ved at et individ kan utføre en kriminell handling som hurtig påvirker mange, - samtidig, i mange forskjellige land. Kriminelle muligheter har blitt panoptisk og samtidig synoptisk ved at få kan utføre handlinger mot mange, men mange kan også utføre handlinger mot få (Mathiesen, 1997).

Eriksen (2007) skriver at det moderne samfunnet har endret tid og avstand betraktelig: *«datamaskinnettverkene og den satellittbaserte kommunikasjonen knytter verden sammen tettere enn noen telegraf eller noen dampskipsselskap kunne drømme om å gjøre» (2007:82).* På en annen side skaper også hastigheten i samfunnet vårt avstand. Der hvor politiet tidligere kunne tilegne seg informasjon om kriminelle hendelser og mistenkelig adferd fra «nabokona», er samfunnet nå mindre tilstede ute i gatene og mer tilstede på nettet. Borgernes gatenære forhold har endre seg. For politiet betyr det at de må tilegne seg informasjon på en annen måte, i tillegg til å vurdere hva det vil si å være politi på nett.

Cyberkriminaliteten sin uforutsigbarhet, hurtighet og distribusjon presenterer en rekke utfordringer for lov håndhevende organer som prøver å kontroller kriminaliteten. På nåværende tidspunkt i Norge, finner man et økt fokus på å kartlegge og styrke politiets kunnskap om cyberkriminalitet. Det ser ut til at det har blitt større medieoppmerksomhet og politisktrykk rundt trusselnivået. Til sammenligning, i akademia ser det ut til at det har vært gjort lite empirisk forskning på politiet i møte med digitalisering i Norge og i nordisk sammenheng. Her er det betydelige hull i litteraturen. Holt og Bossler (2016:106) påpeker at dette er kanskje er et av de minst studerte feltene, men hvor det er størst behov for akademiskforskning fremover.

1.1 Oppgavens problemstilling og avgrensning

Oppgaven består av mange store temaer blant annet: politikultur, nettverksteknologi og cyberkriminalitet. Av den grunn har ikke oppgaven dekket temaene i sin helhet. Oppgaven tar utgangpunkt i ni kvalitative intervjuer med politiets cyberkriminalitetsspesialister. Utvalget av informanter ble gjort på bakgrunn av at det er lite kunnskapen å hente om denne gruppen. Det er en gruppe et fåtall forskere har snakket med. Det har, fra politilitteraturen, vært en gjennomgående trend å studere polititjenestemenn på operativt nivå (Finstad, 2003; Bossler og Holt, 2012; Wall og Williams, 2013). Det viser seg at det er få studier, som studerer andre ledd i politiorganisasjonen. På tross av at det eksiterer ulike perspektiver på og nyanserte tolkninger av «gatepolitiet», oppleves studiene homogene. I en hierarkisk organisasjon som politiet eksisterer det mange ulike avdelinger, fagprofesjoner og seksjoner som er med på å forme politiet og politiets kulturer.

I avhandlingen har jeg valgt å ta utgangspunkt i spesialister i politiet, som hovedsakelig jobber med etterretning og etterforskning av cyberkriminalitet. Jeg var interessert i å få innsikt i hva de som jobbet med cyberkriminalitet daglig tenker om møtet med cyberkriminalitet. Spesialistene er de som er nærmest, føler det nærmest på kroppen, endringene som skjer i politiet på nåværende tidspunkt. En kvantitativ tilnærming ville gitt et bredere utvalg, annet fokus og perspektiv. Sådan ville oppgaven antageligvis hatt andre funn. Til tross for denne vissheten, var det samspillet mellom etatens overordnede bestemmelser og oppfattelsen spesialistene har om arbeidet med cyberkriminalitet, som var interessant å forfølge. Jeg har valgt å avgrense avhandlingen til følgende problemstilling:

- Hva er politispesialistenes opplevelse av politiet i møte med cyberkriminalitet i Norge?

Som en forlengelse av hovedproblemstillingen vil jeg også se på:

Hvordan utfordrer cyberkriminaliteten politikulturen, eller mer presist, politiets kulturer?

1.2 Utviklingen av internett

Internetteknologien er direkte knyttet til cyberkriminalitet. Cyberkriminalitet karakteriseres ved at kriminaliteten foregår gjennom nettverksteknologi, hvilket (så og si) gir momentan informasjonsoverføring og informasjonsinnhenting (Jewkes og Yar, 2010). Internett har en global rekkevidde, hvilket tilsier at cyberkriminelle ikke har restriksjon eller er avhengig av geografiskplassering (Jewkes og Yar, 2010). Hensikten med denne delen er å gi en kort presentasjon av utviklingsforløpet til internett og trekke frem aspekter som kan ha en innvirkning på politiets tilnærming til cyberkriminalitet.

Internett sitt inntog kom for fullt for bare litt over tjuefem år siden. Før den tid hadde man nesten ikke hørt om internett. Internett var noe som tilhørte militæret og vitenskapeligspesialistgrupper (Curran, 2010). Teknologi og digitalisering er en naturlig del av moderne samfunn, og er integrert i alle aspekter ved våre hverdagslige liv. Av den grunnen kan det være vanskelig å se hvor dyp innvirkning internett har hatt og hvor normalisert det har blitt. Internett er definert av store norske leksikon (2018) som:

> *«Nettverk av datamaskiner som kommuniserer med hverandre i henhold til protokollen Internet Protocol (IP). I årenes løp har mange slike nettverk blitt bygget opp og knyttet sammen til et stort, verdensomspennende nettverk som etter hvert har fått egennavnet Internett».*

IP adresser kan grovt sammenlignes med telefonnumre. Alle enhetene som er koblet til nett må ha en IP adresse for å kunne kommunisere med de andre enhetene (Dvergsdal, 2018). Det gjør IP adressen til en unik identifikator (Dvergsdal, 2018). I et kortfattet historisk perspektiv, ble internett originalt utviklet til militært bruk for kontroll, kommandosystemer og opprettholdelse av kanaler for kommunikasjon i tilfelle Sovjetunionen skulle utføre et atomangrep mot USA (Curran, 2010:17). Dette var sent på 50-tallet. Amerikanernes forskning førte til utviklingen av det vi i dag kjenner som det moderne internettet. Selv om den første datamaskinen kom på 40-tallet, var det ikke før i 1968 at man klarte å få til en suksessfull protokoll, hvor sammenkobling av datamaskiner over lengre avstander kunne sende ut datastrømmer samtidig. Dette pakkesvitsjede nettverket fikk navnet ARPANET (Castells, 2001). Norge hadde her en viktig rolle. Norwegian Seismic Array (NORSAR) på Kjeller i Lillestrøm mottok den første meldingen fra California og sendte meldingen videre til London (Schølberg, 2017:33). Videre utvikling gjorde at ARPANET ble nedlagt og world wide

web ble introdusert som et hypertekstsystem av Tim Berners- Lee på starten av 90-tallet (Schølberg, 2017). Hypertekstsystemet gjør tekstdokumenter, bilder og multimedia tilgjengelig på internett. Plutselig åpnet det opp et offentlig rom som ble en investering og av interesse for både bedrifter og privatpersoner. Rommet var desentralisert, stort sett ukontrollert og anonymt (Curran, 20110:22). Da Google kom på slutten av 90-tallet ble internett et sted for hurtig informasjonsdeling, opplysning og læring. I 2004 forandret internettilværelsen seg igjen, til å bli et sted hvor man både kunne tilegne seg informasjon, men også finne den. Facebook åpnet opp for en helt ny verden som i dag refereres som sosiale medier. Sosiale medier er ulike plattformer som åpner opp for sosiale nettverk hvor brukerne skaper, deler innhold, og kommunisere med hverandre på sekunder (Gunn og Aalen, 2017). Til en viss grad forsvant anonymiteten med inntoget av sosiale medier. Inspirert av Mathiesen (1997) kan det forståes at sosiale medier åpner opp for at mange plutselig kan se få, men få kan også se mange.

Parallelt med internettutviklingen kom også nye former for kontroll. På 90-tallet dukket overvåking av bruksmønstre opp som et resultat av entreprenørers ønske om å gjøre størst mulig profitt (Curran, 2010:28). «Cookies» ble brukt til å innhente og overvåke brukere på hjemmesider slik at de kunne utvikle produkter, men også for å forhindre piratkopiering (Curran, 2010:28). Fra å gå fra frihet og anonymitet, utviklet internett seg til å bli et sted hvor teknologien ble og blir utnyttet til å drive konstant overvåking. Frembruddet av regjeringsmakter som kontrollerer adferd for å «beskytte» borgerne mot avvikende adferd sies å bidra til å gjøre internett gjennomsiktig og kontrollert. Internett er i disse sammenhenger beskrevet som et glasshus (Curran, 2010:28). På den andre siden, som en dynamisk reaksjon, har den globaliserte rekkevidden til internett og hurtige utviklingen åpnet opp for muligheter som undergraver lov håndhevende organer og truer samfunnssikkerheten (Thomas and Loader, 2000:1). Internetteknologien går jevnsides der hvor cyberkriminalitet finner sted og betraktes som en styringsform som regulerer cyberkriminalitet ut fra handlingsforløp (Castells, 2000). Internett er ikke lenger noe du har på en datamaskin hjemme, det er noe du bærer rundt med deg, og er i konstant bruk av. Dette åpner opp for mange muligheter.

1.2.1 Internett og atferdsendring

I dag gir et estimert tall overslag på over to billioner internettbrukere verden over (Bossler og Holt, 2016) Ifølge (POD, 2015 og NSM, 2016) så gir et grovt overslag et tall på ca. 20 milliarder ulike dataenheter hvorav ti milliarder er data, syv milliarder smarttelefon og tre milliarder andre enheter som er koblet opp mot internett. For politiet innebærer det at de må gjøre endringer i henhold til et mangfold av nye bruksmønstre. For eksempel, politiet står overfor utfordringer fra: sosiale medier (ulovlig bildedeling, netthets, forfølgelse, utpressing, grooming, og så videre), ondsinnede programvarer slik som maleware, det mørke nettet, krypteringsteknologi, 3D printere som enkelt kan produsere skytevåpen, VR teknologi, skyløsninger, kritisk infrastruktur som blir styrt ved hjelp av datateknologi, biologiske sensorer som kontrollerer vitale funksjoner i kroppen og kunstig intelligens (POD, 2015). Ikke minst samles massive mengder av digitalinformasjon inn, ofte referert til som *«big data»,* som må prosesseres (POD, 2015). Enorme mengder med stordata gjør at politiet benytter redskaper til å utnytte og sortere ut relevant og viktig informasjon. En negativeffekt er at flere havner i systemet fordi informasjonsinnhentingen inkluderer også personer som ikke har kriminelle hensikter eller har begått lovbrudd. Samtidig, når så mye data skal prosesseres kan politiet ende opp med å gå glipp av viktig informasjon fordi de ikke alltid vet hva de leter etter..

Den enorme økningen i bruk av teknologi og internett gjør at vi forandrer måter å tenke på, tilpasse oss og oppføre oss på, og forventninger vi setter. På den ene siden, finner man de unge som vokser opp i dag som har hatt tilgang til internett hele sitt liv og kun kjenner til en verden med internett. De har fått tildelt betegnelsen «digital natives» eller digitaltinnfødte (Ablon og Libicki, 2015). Teknologien har ikke endret deres adferd over tid, den er noe som helt fra starten har vært innplantet og vært med på å forme deres syn på verden. Mesteparten av deres interaksjoner har foregått over i den virtuelle verden og deres daglige behov og ønsker har blitt tilfredsstilt av teknologiskenheter (Holt and Bossler, 2016). På den andre siden finner man «digital immigrants» eller såkalte ikke-digitaltinnfødte. Dette uttrykket sikter til individer som ikke har vokst opp med internett, som må tilpasse sin adferd og lære nye måter å forholde seg til verden på (Ablon og Libicki, 2015). I noen tilfeller gjør teknologien at ikke-digitaltinnfødte må tilpasse seg ting mye hurtigere enn det de er klare for. Et motsvar fra denne gruppen er å motsette seg ressurser, tid og penger på å lære seg

alt det nye (Holt and Bossler, 2016). Et digitalt generasjonsskille kan være utfordrende for en organisasjon som politiet, hvor fleste parten av lederne faller inn under gruppen ikke-digitaltinnfødte. At nye generasjoner kommer inn og utfordrer det gamle, er likevel ikke noe nytt. Oppgaven vil blant annet undersøke om skillet mellom generasjoner ikke er så relevant som man kanskje tror.

1.3 Begrepsavklaring

I prosessen for innsamling av data møtte jeg på hindringer knyttet til ulik begrepsbruk. Ulik tolkning og bruk av flere begrep var begrensende og til tider forvirrende både for informantene og meg selv.

Uklarhet i definisjon har lenge vært problematisk for politi, rettsvesen og forskning, nettopp fordi det påvirker forebygging, samhold, og utbedring (Gordon og Ford, 2006). På lik linje med tradisjonell og gatenær kriminalitet, forekommer kriminalitet som er begått ved hjelp av teknologi i mange ulike miljøer og scenarioer. I et forsøk på å definere og lage et rammeverk for lovbrudd begått ved hjelp av teknologi ser man at betegnelser som: Internettkriminalitet (Sunde, 2005; Jewkes and Yar, 2010; Jewkes, 2007), Datakriminalitet (POD, 2015,2017; KRIPOS, 2017; Sunde, 2016a; Gottschalk, 2011), IKT og internettkriminalitet (NSM, 2016) Teknologi basert kriminalitet (McQuade, 2006), Cyberkriminalitet (Schølberg, 2017; Interpol, 2017,Wall, 2003,2007; Williams og Wall, 2013; Leukfeldt,Veenstra, Stol, 2013; Loveday, 2017; Gordon og Ford, 2006) og Digitalpolitiarbeid (POD, 2017), som noen av flere eksempler på ulik begrepsbruk av teknologibasert kriminalitet. Mye av grunnen til at det foreligger så mange ulike begrep er fordi det ikke foreligger en allmentakseptert rettslig definisjon (Schølberg, 2017). Nåtidens definisjoner defineres ut fra oppfatninger som både observatører og offeret sitter med (Gordon og Ford, 2006). På grunn av ordbegrensninger vil jeg ikke ta for meg alle begrepene. Jeg har valgt å avgrense til betegnelsen «cyberkriminalitet».

1.3.1. Betegnelsen Cyberkriminalitet

I litteraturen blir William Gibson sitt verk *«Neuromancer»* fra 1982, referert til som startpunktet for betegnelsen cyberspace, som videre har utviklet begrepet «cybercrime» (referert i Schølberg, 2017:17;Wall, 2007:10). I Gibsons novelle beskrives cyberspace som en mentalbasert, virtuell verden hvor datanettverksaktivitet finner sted (referert i Schølberg, 2017:17; Wall, 2007:10). «Cybercrime» er da kriminaliteten som forekommer i denne verden og som i dag brukes som en betegnelse på risiko og fare på nett (referert i Schølberg, 2017:17; Wall, 2007:10). David Wall begynte å bruke betegnelsen «cybercrime» i akademisk forskning i 1998, da han refererte til kriminalitet utført på nett (referert i Holt and Bossler 2015). På midten av 2000-tallet ble det en gjennomgående trend for forskere å benytte seg av begrepet «cybercrime» i referanser til nettverkbasert kriminalitet (Holt and Bossler,

2015). Selv om terminlogien «cyberkriminalitet» har oppnådd en aksept og er nå et anerkjent og ofte brukt begrep, eksisterer det likevel store forskjeller i tolkninger om hva cyberkriminalitet er (Gordon and Ford, 2006). Videre skal jeg trekke frem fem eksempler på ulik tolkning i et forsøk på å demonstrere kompleksiteten knyttet til dette begrepet. Thomas og Loader (2000:3) definerer «cybercrime» som følgende:

> *A computer-mediated activities, which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Its distinctiveness is derived from the versatile capabilities provided by the new internet and web-based information and communication technologies.*

Thomas og Loader sin definisjon påpeker at cyberkriminalitet defineres og er særegen nettopp på grunn av nettverkteknologiens muligheter, men hvor aktiviteten blir definert som «cyberkriminalitet» hvis den blir vurdert som ulovlig. I og med at internettmulighetene skifter fortløpende, og har en global rekkevidde, kan det å definere begrepet ut ifra aktivitet som er lovlig/ulovlig møte på begrensninger. For eksempel ved at en handling defineres ulovlig i et land, men lovlig i et annet. Å vurdere betegnelsen på den overnevnte måten skaper store utfordringer ved at cyberkriminaliteten kan påvirke mange, på samme tid, i mange forskjellige land. Aktøren kan i tillegg befinne seg i et annet land enn det landet aktøren utfører kriminalitet mot. Tilnærming kan dermed skape begrensninger for internasjonalt samarbeid og etterforskning. The Council of Europe Convention on Cybercrime (kjent som Budapest konvensjonen), har prøvd å utligne problemet gjennom å skape et internasjonalt lovverk og styrke lands samarbeid (Schjølberg, 2017). I tillegg har Europol samlet europeiske land under deres «Joint Cybercrime Action Task force», hvor Norge nå nylig fikk offisielt medlemskap[1]. Likevel eksisterer det forskjell i tilnærming og tolkning. En annen, mer vanlig tilnærmingsmetode til dette fenomenet er å skille mellom to typer cyberkriminalitet, men også her finnes det variasjon i tolkning.

På Interpol sine hjemmesider[2] står det skrevet at Interpol tar utgangspunkt i skillet mellom lovbrudd begått ved hjelp av og lovbrudd begått med og mot datamaskiner når de bruker betegnelsen «cybercrime». Førstnevnte refererer til kriminalitet som eksisterte før internett sin opprinnelse, men som har utviklet seg og endret seg ved hjelp av mulighetene internett

[1] https://www.europol.europa.eu/newsroom/news/europol-and-norway-join-forces-in-combating-cybercrime
[2] https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

og teknologien tilbyr. Interpol refererer til dette som *«cyber enabled crime».* Kategoriene innenfor denne typen kriminalitet er som følgende: bedrageri, tyveri, narkotikahandel, organisert kriminalitet, utpressing, terrorisme, vinningskriminalitet, innbrudd og seksuell utnyttelse. Den andre sikter til lovbrudd som ikke kunne eksistert uten internett, som angriper globale elektroniske nettverk og datamaskiners software og hardware – kalt *«High-tech crime».* Her sikter Interpol til malware, ondsinnet programvare som har til hensikt å ta kontroll over datamaskiner for å skade og/eller få tak i viktig informasjon. På KRIPOS sine hjemmesider[3] står det skrevet en lignende tolkning, men KRIPOS skiller seg ut ved å legge til internett som sporsted. I tillegg bruker KRIPOS betegnelsen «datakriminalitet», noe som for eksempel Schjølberg (2017) er skeptisk til fordi han mener at det er en gammel betegnelse som burde opphøre. Skillet som politiorganene benytter seg av kan være hjelpsomt i sortering av lovbrudd, men til hindring ved at de isolerer måten å begå lovbrudd på. Hvilket som regel ikke stemmer med virkeligheten. Cyberkriminalitet kan inneholde alle de tre formene for kriminalitet og være sterkt knyttet sammen. Eksempelvis kan en med kriminelle hensikter bruke ondsinnet programvare for å gjennomføre et datainnbrudd mot en datamaskin for å hente ut informasjon som skal benyttes senere til å begå bedrageri. Dermed vil også stedet for hendelsen (internett) være sporsted.

Det tredje eksempelet finnes i norsk akademia hvor Inger Marie Sunde (2016a) og Stein Schjølberg (2017) gir en juridisk, strafferettslig tilnærming til begrepsbruken. Begge med hver sin tolkning og hvert sitt begrep. Schjølberg (2017) tar utgangspunkt i begrepet «cyberkriminalitet». Han forklarer at begrepsbruken burde være et ledd som passer inn med internasjonalutvikling. Leddet burde forstås i dag i overensstemmelse med den kriminaliteten som omhandler vern av data i straffeloven av 2005. Det vil si

> *«Lovovertredelser som omfatter innbrudd i datasystemer, uberettiget befatning med tilgangsdata, identitetskrenkelser, krenkelser av rett til skadeverk, elektroniske dokumentforfalskning, databedrageri og fremstilling av seksuelle overgrep mot barn»* (2017:18).

Inger Marie Sunde (2016a) forholder seg til betegnelsen «datakriminalitet». Her skiller hun mellom digitalytring og digitalhandling for å tolke straffebud. Ytring utpekes som

[3] https://www.politiet.no/rad/datakriminalitet/

«meningsutveksling mellom to mennesker» (2016:13). Eksempler på dette kan være hatefulle ytringer, bedrageri, narkotika på nett og så videre. Det er mottakerens kognitive oppfattelse som kriminaliteten retter seg mot, ikke handling mot datamaskin eller programvare. En handling på den andre siden, sier noe om et lovbrudd som påvirker eller retter seg mot datasystemer, og ikke mennesket i seg selv.

Et fjerde eksempel på ulik tolkning er av Gordon og Ford (2006). De deler inn i kategoriene Cybercrime I og Cybercrime II. Cybercrime I er kriminalitet, men mest teknologisk av natur. Det vil si at kriminaliteten baserer seg på offerets uvitenhet og datamaskiner/programvaresårbarheter. Denne formen for kriminalitet blir typisk utført ved at enkeltindivider eller organiserte grupper sender ut mail med ondsinnet programvare til et offer, med den hensikt å drive utpressing eller tyveri. Cybercrime II er derimot kriminalitet som er begått ved hjelp av datamaskiner eller nettverk, men som inneholder flere menneskelige elementer enn det førnevnte. Her baserer handlingen seg på å kartlegge og overvåke brukeren sin adferd. Gjerne ved å bygge opp et tillittsbånd med offeret. Hensikten er utpressing, utnyttelse, manipulasjon, spionasje, planlegging av terroristangrep og så videre. De foregående eksemplene bærer likhetstrekk og har lignende tolkninger, men som vist her er de likevel forskjellige. Betegnelsen cyberkriminalitet mangler enstemmighet, og det er stor uklarhet i hvordan skillet mellom kriminaliteten klassifiseres. Det er kanskje ikke så unaturlig når nettverksteknologien forandrer kriminalitetsutførelsen i så stor grad som den gjør.

Som siste eksempel vil jeg trekke frem Wall sin transformeringstest (2007). Ut fra bredlesning vil jeg si at han presenterer en klar tolkning og definisjon. Transformeringstest er lett forståelig og anvendelig. Transformeringstesten går ut på å fjerne internett fra ligningen for å se hva det gjør med kriminaliteten og adferden. Dersom fravær av internett gjør at det ikke eksisterer noe lovbrudd, vil det være snakk om cyberkriminalitet. Om man står igjen med lovbrudd som vil og har eksisterer uten internett tilhører kriminaliteten kategoriene som faller under tradisjonell kriminalitet.

I min avhandling tar jeg utgangspunkt i begrepet «cyberkriminalitet» nettopp av den grunn at det har blitt et etablert begrep innenfor akademia og i internasjonal sammenheng. Ut fra Wall (2007) sin transformeringstest og med inspirasjon fra Gordon og Ford (2006), vil jeg

skille mellom det jeg vil kalle cyberkriminalitet 1 (CK1) hvilket refererer til kriminalitet som ikke ville eksitert uten nettverksteknologi, og cyberkriminalitet 2 (CK2) som referer til tradisjonell kriminalitet utviklet og tilpasset nettverksteknologien (CK2). Selv om jeg ser ulempene ved å opprettholde et skille, ser jeg også fordelene. Jeg har valgt en slik tilnærming for å gjøre det klart for leseren hva jeg henviser til.

1.3.2 CK1 og CK2

Her skal jeg presisere og konkretisere min tolkning av forskjellene mellom CK1 og CK2.

CK1

Ut fra Wall (2007) sin transformeringstest er CK1 kriminalitet som ikke ville eksistert uten internett. CK1 er straffbare handlinger rettet mot data og datasystemer også definert som dataangrep, hacking (Gottschalk, 2011; Wall, 2017) og high-tech crime (Interpol 2017). En økende trend er individer eller grupper som tar over kontrollen av en eller flere datamaskiner ved å sende ut eksempelvis, e-post med ondsinnet programvare (malware). Når eieren trykker på linken i e-posten vil viruset spre seg, låse datasystemer eller bli brukt for å innhente informasjon. Dataangrep har som regel til hensikt å svindle til seg penger, terrorisme, industrispionasje, politisk maktspill eller å utrette skade (Gottschalk, 2011). Det finnes flere ulike typer malware og de kan bygge på hverandre eller jobbe sammen. Videre har jeg hentet informasjon fra Interpol (2017) og Gottschalk (2011) for å beskrive noen: *Botnet,* er flere datamaskiner som samarbeider om å ta ned servere. Her sender man massive mengder med informasjon og spam til en eller flere servere slik at de kollapser. Angrepet er også kjent som *Denial of Service (DDoS)* angrep. *Rootkit* er en samling av programmer som gjør at at innbryteren får privilegert tilgang til maskinen og i noen tilfeller andre maskiner i samme nettverk. *En orm,* er ondsinnet program som bruker eksisterende kommunikasjonsmetode for å sende kopier av seg selv til andre datamaskiner. *Trojaner,* er ondsinnet program som utgir seg for å være noe annet enn det er, slik som lovlige programmer eller spill. Hvis man prøver å kjøre/installere programmet vil det infisere datamaskinen med ondsinnet kode, fot eksempel: spyware eller virus. *Spyware* har til hensikt å hente ut informasjon fra datamaskiner/nettverk og gjør det ved hjelp av skadelige koder. *Adware,* er programvare med skadelige koder som bruker reklame, pop-ups og virus til å spre den ondsinnet programkode som kopierer seg selv inn i filer eller

oppstartssektorer. *Ransomware*, låser datamaskiner og hindrer brukerne fra å ha tilgang. Hensikten er utpressing, vinning, spionasje eller propaganda til politisk agenda eller oppfordring til sosiale forandringer. Ut fra overnevnt beskrivelse, kan man se at CK1 bærer sterke likhetstrekk med økonomiskkriminalitet og krigsforbrytelser.

Flere politiorganer har ytret sterk bekymring over CK1[4]. De som utfører handlingene bryter med det stereotypiske bildet på en kriminell - at de kommer fra fattigdom og lavstatusgrupper eller er sosiale avvikere (Aas, 2013). Interpol beskriver blant annet at det er en sterk økning i cyberkriminelle nettverk, som besitter avansert teknologisk kompetanse. De organiserte, cyberkriminelle gruppene består som oftest av høyt utdannede individider eller fremmede statlige aktører med avansert trening i utførelse av store, globalt ødeleggende dataangrep. Blant annet, sommeren 2017 var det to store angrep som fikk høy medieoppmerksomhet. Et stort krypto-utpressingsangrep, kalt «NotPetya» rammet en rekke bedrifter i Europa og kostet selskaper så mye som 1,5-2,4 milliarder norske kr (Digi, 2017). Ransomware viruset «Wannacry» er et annet eksempel. I løpet av et døgn hadde viruset spredd seg til 150 land verden over, og 230.000 datamaskiner hadde fått all informasjonen kryptert (Trædal, 2017a). Det gikk hardt utover samfunnsinstitusjoner blant annet flere britiske sykehus (Trædal, 2017a). PST skrev i sin trusselvurderingsrapport fra 2018 at de er bekymret for fremmede etterretningsvirksomheter som bruker avanserte datanettverksoperasjoner rettet mot norsk beredskapssektor, politiske beslutningsprosesser og infrastruktur. CK1 kan innvirke på sosiale, økonomiske og politiske forhold.

CK2

Ut fra Wall (2007) sin transformeringstest er CK2 kriminalitet som eksisterte før internett, men som ved hjelp av internett har utviklet seg. Eksempler på dette er: kjøp og salg av narkotika, smugling, kjøp og salg av illegale produkter, trusler, rasistiske og hatefulle ytringer, utpressing, id-tyveri, netthets, ulovlig bildedeling, seksuelle overgrep, utnyttelse og overgrep mot mindreårige, terrorisme, tyveri, bedrageri og menneskehandel. Utviklingen av CK2 har medført at store deler av denne typen kriminalitet er transnasjonal og foregår på det man kaller «The darkweb», eller det mørkenettet. Her benytter lovovertredere nettleseren Tor til å skjule sin identitet fra myndigheter og politiorganer (Bolt og Hossler,

[4] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime

2016:175). Tor opererer på den måten at den bruker avanserte krypteringsprogram og nettlesere som skjuler stedsplassering og brukere, i tillegg til at brukerne kan opprette skjulte, krypterte internettsider (Holt og Bossler, 2016:175). Det er viktig å presisere at Tor ikke bare brukes av de med kriminelle hensikter, men kan også benyttes som en nettleser for de som ønsker å beskytte sitt personvern eller i land hvor ytringsfriheten er begrenset og internett er sensurert. Jeg har ikke til hensikt å gå dypt inn i diskusjon om det mørke nettet i denne avhandlingen. Dette fenomenet er såpass omfattende at det ville vært en avhandling i seg selv. Hensikten her er å informere leseren om og å vise til nok et aspekt ved internett som kompliserer politiets arbeid.

1.3.3 «Cyber» kriminalitet- et nytt fenomen?

En siste diskusjon jeg ønsker å trekke frem er funnet i flere forskningsartikler. Diskusjonen omhandler bruken av uttrykket «cyber». Her mener forskere at «cyber» er veldig misvisende fordi kriminelle som utnytter teknologi til å begå lovbrudd ikke er noe nytt (Gordon og Ford, 2006; Sunde, 2016a og 2016b). Fenomenet beskrives som «old wine in new bottles» (Jewkes and Yar, 2010). Sunde (2016b) skriver at terminologien «cyber» vil opphøre i fremtiden, det vil ikke være behov for terminologien for å skjønne hva vi referer til. Terminologien vil eksistere i en transformeringsfase. Gordon og Ford (2006) mener det at terminologien er misvisende fordi det lager en vertikal representasjon av problemet, som egentlig er horisontal av natur. Med andre ord, man kan ikke kan isolere cyberkriminalitet som noe eget, for i dagens samfunn er så og si all kriminalitet overført til nett. Schjølberg (2017) trekker på den andre siden frem styrken i begrepsbruken, ved å peke på at det å holde seg til betegnelsen «cyberkriminalitet» korrelerer med internasjonalutvikling (2017:17). Betegnelsen har han adoptert fra Europarådets konvensjon om cyberkriminalitet fra 2001, nettopp av den grunn at det skal øke det internasjonale samholdet rundt begrepet. I lik tråd, skriver Jewkes og Yar (2010) at terminologien og skillet mellom ulik type cyberkriminalitet nå er så utberedt og det som er hyppigst brukt blant akademikere og politimyndigheter, at det vil være mest fornuftig og holde seg til det. Likevel, når beskrivelser og tolkning varierer i den graden den gjør, er det her litt uklart hvilket skille Jewkes og Yar (2010) sikter til.

1.3.4 Oppsummering

Ut fra min tolkning av CK1 og CK2 gjenkjenner jeg at de går over i hverandre, men at det ikke er et nytt fenomen. Det som er annerledes er at det foregår ved hjelp av nettverksteknologi, på en annen type arena, som krever annen type kompetanse og forståelse. På den andre siden er det ikke nytt at kriminaliteten utvikler seg i takt med samfunnets utvikling. Kriminalitet kan forstås som et sosialt konstruert fenomen, og vil derfor bli til gjennom de sosiale, økonomiske og kulturelle prosesser (Christie, 2000). Cyberkriminalitet vil kunne tolkes som en naturlig tilpassing og utvikling til disse prosessene.

1.4 Kompleksitet og utfordring

På grunn av sin grenseløshet og store muligheter for anonymitet, vil det være umulig å kvantifisere cyberkriminalitet. Dette gjør cyberkriminaliteten vanskelig å forske på (Jewkes and Yar, 2010). Lignende ble skrevet i rapporten fra POD (2015). Her skrives det at politiet har kort erfaring med cyberkriminalitet, de har vanskeligheter med å vurdere trussel og risikonivået på grunn av at teknologiens høye uforutsigbarhet og raske utvikling. Kriminalitetsutviklingen av cyberkriminalitet er noe man likevel er oppmerksom på og som er bekymringsfullt fordi Norge er nå et gjennomdigitalisert samfunn, hvilket gjør landet veldig sårbart ovenfor cyberkriminalitet (Gottschalk, 2011). Oppgavens fokus er på spesialistenestanker om det å møte kriminalitet på en ny arena. Av den grunn kommer jeg ikke til å spisse meg mot en type cyberkriminalitet. Oppgaven vil heller ta for seg et bredere perspektiv, - hvordan informantene opplever møtet med all cyberkriminalitet. Derimot, på noen områder vil oppgaven dele inn kriminaliteten etter referansen CK1 og CK2. Jeg ønsker videre å presentere leserne med ulike problemstillinger politiet står ovenfor. Jeg mener det er viktig for leseren å ha kjennskap i dette for å kunne forstå de ulike intrikate aspektene som influerer politiets møte med cyberkriminalitet.

Det er syv området som utpeker seg: uavhengig geografisk plassering, lagring av elektroniskspor, hurtig utvikling, mørketall, anonymisering og kryptering, utvisking av offentlige og private ansvarsområdet og nye kontrollformer. Videre skal jeg gi en kort forklaring av alle, som senere blir utdypet i analysen.

Den kanskje største utfordringen ved at forbrytelser begås via eller over nett er at forbryteren/e ikke er avhengige av geografiskplassering (Gottschalk, 2011). Uavhengig geografisk plassering visker ut nivået på planlegging, identitet, forberedelser og flukt. Tradisjonell operativ politipraksis baserer seg på disse elementene. Ved at disse, i stor grad, blir fraværende på internett, må politiet tenke annerledes. I tillegg er cyberspace den eneste arenaen hvor det å gjennomføre globale straffbare handlinger kan skje uten stor risiko for å bli straffet, fordi det ikke foreligger en sterkt internasjonal lovgiving eller domstol (Schølberg, 2017). Det er noe politiet jobber aktivt med å løse. Den andre utfordringen er at det forekommer store vanskeligheter ved å finne og lagre elektroniske spor. Å sikre spor er en en vesentlig del av etterforskningsarbeidet. Å sikre elektroniskspor krever god

tekniskkunnskap, og oppdatert og godt utarbeidet verktøy som det ofte er mangel på. I tillegg forsvinner elektroniskspor hurtig. I Norge for eksempel har IP-adresser en lagringstid på maks 21 dager. Det krever at etterforskerne sikrer seg IP adressen hurtig, noe som ikke alltid er mulig. En tredje utfordringer relaterer seg til lovverket. Fordi teknologien endrer seg i den hastigheten den gjør, kan det være vanskelig å følge opp med oppdatert lovverk. Det skaper huller i lovverket som igjen gjør rettsforfølgelse vanskelig. Den fjerde utfordringen politiet møter på er at de ikke har et klart bilde på hvor stort omfang cyberkriminaliteten har. Det finnes ikke nøyaktige cyberkriminalitetsstatistikker som politiet kan jobbe ut ifra (Jewkes, 2007). I en undersøkelse foretatt av Datakrimutvalget i Næringslivets sikkerhetsråd i 2006, *«Mørketall»,* avdekket de funn som peker på at cyberkriminalitet er langt mer utbredt enn det som kommer frem i statistikkrapporter (NSR, 2016). Grunnen til det store spriket har blitt diskutert i lys av manglende anmeldelser fra norske virksomheter. Siden 2006 har det vært årlig publikasjon av mørketallundersøkelsen som viser samme gjennomgående trend (NSR, 2016). Den femte utfordringen er knyttet til anonymisering og kryptering som øker i omfang, hvilket hindrer politiet i å få tilgang til bevis og identitet (POD, 2015). Jewkes and Yar (2010) tilføyer at det objektivt sett er det den sosiale og politiske responsen til det overnevnte problemet som skaper utfordringer. Et økt politisk fokus på å utrede såkalte risikovurderinger har økt redsel og bekymring. Det skaper cybersikkerhet til en salgsvare for private, kommersielle aktører. Ved å styrke personvern på tjenester private aktører tilbyr (for eksempel ved å kode informasjon slik at innholdet ikke kan leses av andre) beskytter det individer mot kriminelle hendelser, men vanskeliggjør politiets tilgang til elektroniskspor (POD, 2015). I tillegg har det blitt snakket om at private aktører tar over ansvarsområder som egentlig tilhører politiet. Å skillet mellom offentlig og private ansvarsområder blir til tider vanskelig. En siste utfordring settes i sammenheng med nye former for kontroll. I litteraturen har det blitt diskutert om økt overvåking av borgerne kan fremprovosere en såkalt «chilling effekt» (Richards, 2013). Her trekkes det frem at ytringsfriheten og personvernet til borgerne blir begrenset ved at statsmakter i høyere grad benytter seg av instrumentell kontroll slikt som overvåking som et verktøy for å forebygge risiko. Det kan tvinge frem nye bruksmønster hvor flere går over til å bruke det mørkenettet, og hurtigere benytter seg av krypteringsteknologi.

Som man kan se ut fra de overnevnte punktene, står politiet overfor utfordringer vedrørende karlegging, avdekking og forebygging av cyberkriminalitet. Wall (2007) mener det at vi kan forstå påvirkningen cyberkriminalitet har på samfunnet ved å dele inn i tre hovedmåter. Den første er at teknologien har utvidet, opprettholder og tilrettelagt for nye forhold for lovovertredelser. Det andre er at det har åpnet opp for nye, hurtige transnasjonale muligheter, og det tredje er å se på det virtuelle miljøet som har skapt nye former for lovovertredelser, hvilket ikke bærer preg av begrensninger slik som tidligere «tradisjonell» kriminalitet. Ved å separere disse tre og se på innvirkningen hver og en av dem har, kan politiet klare å tilrettelegge beslutningstaking og forstå fenomenet på en slik måte at de klarer å utøvde sine arbeidsoppdrag i tråd med samfunnsutviklingen.

1.5 Oppgavens oppbygging

Gjennom oppgavens seks kapitler vil jeg presentere og analysere informantenes historier om møtet med cyberkriminalitet. Fra spesialistenes oppfattelser har jeg analysert ulike aspekter som potensielt sett har en innflytelse på politietatens arbeid med cyberkriminalitet. Teorien og de ulike perspektivene som skal bli benyttet gjennomgående vil bli presentert i et kapittel. Hvordan jeg gikk frem for å tilegne meg empiriskmateriale og analysen av selve datamaterialet er fordelt på tre kapitler. Det siste kapittelet er et avslutningskapittel.

I kapittel 2 fremlegger jeg en kort bakgrunn, diskuterer valg av teori og presenterer relevant, tidligere forskning som legger grunnlaget for analysen og diskusjonen i de neste kapitlene som legger frem oppgavens empiriske materialet.

I kapittel 3 diskuterer jeg valg av metode og hvordan jeg tilnærmet meg feltet. Her gjør jeg rede for hvordan forskningsarbeidet er gjennomført, refleksjon rundt eget arbeid, og en presentasjon av de etiske vurderingene som ble tatt underveis.

Kapittel 4 vil være første analysekapittel. Her vil politikultur være i fokus. Fra historiene som er fortalt av informantene skal jeg undersøke hva det vil si å være politi på nett i dag. Analysen vil se på i hvilken grad cyberkriminaliteten utfordrer politiets interne tradisjoner, verdier og normer. Avslutningsvis trekkes frem informantenes ønsker om endring.

I kapittel 5 er vil jeg ta for meg informantenes tanker om ledelse og styring. Her vil jeg se på ytre kontrollprosesser og hvilken innvirkning kontrollprosessene har på informantens arbeid med cyberkriminalitet. Her vil ledelse, kultur og styringsstrategier være i fokus.

I kapittel 6 vil jeg kort oppsummer, sammenfatte diskusjoner, trekke frem oppgavens hovedfunn og konkludere med noen tanker for veien videre.

2 Teoretiske perspektiver og tidligere forskning

Prosjektets fenomenologiske og induktive tilnærming legger føring for valget av hovedteori. Den bygger først og fremst på teorier om politiets kulturer. Politikulturteorien er basert på antagelsen om at holdninger og verdiene til politiet styrer og former hvordan de ser og opplever verden. Politikulturen vil kunne bidra til en bedre forståelse av historiene slik de er fortalt av informantene. Temaene som fremstod som viktig for informantene har styrt de understøttende teoriene og perspektivene. Møtet mellom cyberkriminalitet og politiorganisasjonen er komplekst og en teori alene kan ikke forklare prosessene som dukker opp når to store felt møter hverandre. Underveis i diskusjonene vil jeg introdusere andre teorier for å skape en nyansert drøfting. Jeg vil starte dette kapittelet med å gi en kort bakgrunn. Deretter beveger kapittelet seg over til å presentere politikultur som teori og tidligere forskning.

2.1 Bakgrunn

2.1.1 Utviklingstrekk

Politietaten i Norge er en del av offentligsektor, hvilket vil si at organisasjonen er politiskstyrt (Johannessen og Glomseth, 2015:44). Reiner (2010) skriver at politiet er hjertet av statens funksjon og den preges også av statsdefinerte metoder for politiskstyring. Politiske prioriteringer, media, økonomiske og teknologiske faktorer spiller inn og påvirker politiets kurs. Ikke minst kriminalitet og utvikling. Justis og beredskapsdepartementet har det overordnede ansvaret for den politiske styringen av politietaten (Johannessen og Glomseth, 2015:101). De skal etablere og definere mål og overordnede strategiske planer i tråd med politiske ambisjoner innenfor samfunnssikkerhet, straffesak og beredskapskjeden (Johannesen og Glomseth, 2015:101). Politidirektoratet (POD) utgjør den andre delen av den sentralpolitiske ledelsen vi har i Norge. POD skal iverksette og operasjonalisere de tiltakene som er satt på politisknivå, gjennom fag og metodeutvikling, koordinering og styring av politidistriktene (Johannessen og Glomseth, 2015:102).

Politidirektoratet (POD) fikk 1. November 2013, tilsendt et brev i form av et mandat fra Justis og Beredskapsdepartementet (POD, 2015). Her stod det nedskrevet at POD skulle gjøre en

utredning av overordnet nasjonal strategisk bekjempelse om «datakriminalitet», og gjøre en kartlegging av hvordan «datakriminalitet» bekjempelsen foregikk. I 2015 kom rapporten *«Datakrimstrategien»* og i mellomrommet 2015-2018 ble en gruppe opprettet som fikk ansvar for å gjøre en omfattende kartlegging av den interne kunnskapen politiet i Norge har, med forslag til tiltak videre. I tillegg ble det nylig publisert på politiforum, at politiet skal opprette et nasjonalt cyberkriminalitetssenter (NC3) (Trædal, 2017b). Det er tydelig at politiorganisasjonen er i en endringsfase og driver selv med kartlegging av etatens fremtidige behov i møte med cyberkriminaliteten. Videre ønsker jeg å presenterer tre ulike tilnærminger i litteraturen som har innvirkning på politiets væremåte, deres arbeidshverdag og på den organisatoriske prosessen som er i gang.

Den byråkratiske modellen

Granér og Kronkvist (2015:61) beskriver politiorganisasjonen som: *«et tydelig definert hierarki av beslutningstakere på ulike nivå med ulike oppgaver og kompetanse*». Beslutninger tas fra overordnet nivå og forplantes nedover i organisasjonen (Granér og Kronkvist 2015). Oppdrag skal ledes og gjennomføres i henhold til lover, regler visjonen og intensjonen satt på overordnet nivå (Johanessen og Glomseth, 2015). I likhet så skal håndtering av ethvert politioppdrag og alle oppgaver dokumenteres og rapporteres oppover i organisasjonen (Johanessen og Glomseth, 2015). Politiorganisasjonen verdsetter stabile, innøvde og repetitive utførelser av arbeidsoppgaver som må tjenestilpasse budsjetter og regelverk (Johanessen og Glomseth, 2015). Styringen bærer flere likhetstrekk med det som defineres som den byråkratimodellen. En definisjon av byråkrati er at det er *«en regelstyrt virksomhet»* (Weber 1990, I: Granér og Kronkvist 2015:61). Fra overnevnte beskrivelser kan det trekkes slutninger om at politiorganisasjonen er en byråkratisk styrt organisasjon.

At politiorganisasjonen styres ut fra et byråkratiske tankesett kan medføre at det oppstå indre maktkamper mellom beslutningstakere på ulike nivå. Spesielt mellom operativt «gatepoliti», og ledelse på overordnet nivå (Johannessen og Glomseth, 2015). Fordi operativt jobber tett på arbeidsoppdraget tilsier situasjonen at de må gjøre ulike prioriteringer ut fra egne profesjonelle valg og erfaringer, noe som ikke alltid samsvarer med de abstrakte strategiene som er utarbeidet av overordnet nivå (Johanessen og Glomseth, 2015). Kritikk av den byråkratiske modellen er at målet som blir satt fra overordnet nivå blir viktigere enn selve arbeidsutførelsen, og man tar i lite grad hensyn til situasjoner som krever

hurtige, tilpassede beslutninger (Granér og Kronkvist 2015). I tillegg kritiseres modellen for å ha en funksjon kun tilpasset forutsigbare og stabile miljøer, men fremstår som uegnet når det skal gjennomføres forandringer av egen praksis (Johanessen og Glomseth, 2015). Som det kommer frem i oppgaven kan det å holde fast på en byråkratisk arbeidspraksis være en utfordring i møte med nettverkteknologien. Internett bringer frem hurtighet, komplekse samfunnsproblemer og et endret kriminalitetsbildet som utfordrer politiets styringsform.

Risikosamfunnet og sikkerhet

I litteraturen om risiko samfunn, beskrives moderne samfunn som risikostyrt gjennom samfunnets sentrerte fokus på frykt og sikkerhet (Aas, 2013). En risikobasert styringsmodell har fokus på å forhindre fare og redusere kriminalitet gjennom bruken av instrumentelleteknikker (Gundhus, 2007). Ny risikoforståelser produseres i en samtidig prosess med samfunnsutvikling, teknologi og vitenskapens fremgang. Eksempelvis, årlig kommer det ut risikorapporter fra politi og sikkerhetsorganer som benytter risikovurderingene som utgangspunkt for sine strategier (PST, 2018; NSM, 2018).

Sosiologen Ulrich Beck (1986) sitt arbeid og boken *«The Risk Society»* var utgangspunktet for debatten om risikosamfunnet. Risikosamfunnet beskrives som et moderne samfunnet hvor det å forhindre og håndtere fremtidsrettet risiko som samfunnet selv produserer blir et hovedfokus (Aas, 2013). I Ulrich Becks arbeid beskrives nye moderne risikoforståelsen som at risiko er noe menneskeskapt og ikke knyttet til naturen. Risikoen er noe som er globalt og potensielt verdensutslettende (Aakvaag, 2008). Til motsettning definerer Ericson og Haggerty risiko som: *«risk refers to external danger, such as a natural disaster, technological catastrophe, or threatening behavior by human beings»* (1997:3). I deres tolkning tillegger de at risiko kan forbindes med naturlige og teknologiske katastrofer. Jeg velger å benytte med av Ulrich Bech sin forståelse av risiko, da det kan virke som menneskeskaptrisiko er sentralt knyttet til cyberkriminaliteten.

De dominerende diskursene i risikosamfunnet sentrerer rundt frykt, trygghet og sikkerhet (Aas, 2013). Risikosamfunn vil være på konstant utkikk etter farer og adferd som vil true samfunnsfreden. I stedet for å kontrollere avvikende adferd som allerede har oppstått, vil man da heller prøve å styre den menneskeskapte risikoen. Her står «jeg-et» i sentrum. Gjennom indirektestyring oppfordres individer, bedrifter, organisasjoner og kommuner til å aktivt ta del og ansvar for å unngå risiko (Aas, 2013). Ved at samfunnet styres på den

overnevnte måten, så diskuteres det om rettssystem, politiet og politikere utformer strategiske tiltak på bakgrunn av risikokategorier. Hva som klassifiseres som farlig og hvem som havner i risikokategorien er noe mer vagt og til tider veldig skiftende (Jones, 2012). At risikokategoriene er foranderlig tilsier at målgruppen vil skifte etter overordnet fokus. Til tross for dette, hevder Jones (2012) at risikogruppene fremdeles inkluderer de klassiske gruppene; fattige, arbeidsløse, rusmisbrukere, etnisk og religiøse minoritetsgrupper. Risikosamfunnet har i tillegg et endret strafferettslig tankesett. Der hvor tidligere tankegang var «uskyldig til motsatte bevist», er tankegangen i risikosamfunnet «skyldig til bevist motsatt» (Jones, 2012). En fremtredende konsekvens av en slik tankegang er at fler og fler havner under overvåking og i systemet.

Som en naturlig mekanisme til et samfunn som fokuserer på risiko, vil det være en økende etterspørsel etter sikkerhet. Sikkerhet kan forståes på mange måter, men Zedner (2003:158) definerer sikkerhet som: *«objective state of being protected from threats or danger a subjective feeling of safety or the means of pursuit of either of these».* Ideen om objektiv og subjektiv sikkerhet baserer seg på en fremtidsrettet, proaktiv logikk (Jones, 2012). Paradoksalt nok promoterer sikkerhetsmarkedet at sikkerhet er en gode for alle, men som har vist seg å øke sosial ekskludering (Jones, 2012).

Kunnskapsbasert politiarbeid

I takt med at det har vokst frem nye risikobaserte styringsformer, har det i nyere tid blitt diskutert om at det har vokst frem et nytt paradigme i utførelse av politiarbeidet (Gundhus, Vrist og Fyfe, 2017). Paradigmet baserer seg på ideen om at politiets strategier, responser og arbeidsmetodikk burde vektlegge kunnskapsbasert tilnærming til politiarbeidet (Gundhus, Vrist og Fyfe, 2017). Kunnskapsbasert arbeid vektlegger den enkeltes kompetanse, samarbeid med andre fagprofesjoner og ansvarliggjøring av problemeiere i stedet for problembærere (Gundhus, 2007:164). Utviklingen av teknologi kan være en fremtreden årsak til hvorfor overordnede planer setter mål om at politiet skal jobbe mer analytisk og ut ifra annen kunnskap en sin egen. Det strider mot den operative, tradisjonelt arbeidspraksisen som verdsetter erfaring og reaktiv respons til problemer som allerede har oppstått (Gundhus, 2007). Tradisjonelt setter politiet inn tiltak etter at kriminaliteten har inntruffet (Gundhus, Vrist og Fyfe, 2017). Kunnskapsbasert praksis oppfordrer til å analysere årsaken til kriminaliteten, og verdsetter ideer om virkningen av forebyggende tiltak. Å

vektlegge forebyggende tiltak og kunnskapsbasert tilnærming kommer da i konflikt med det som klassifiseres som det «ekte» politiarbeidet (Se kapittel fire). At proaktivt arbeid dukker opp som en ny modell kan knyttes sterkt til teorien om risikosamfunn, hvor da utøvelsen av instrumentell kontroll i form av for eksempel, overvåking, blir en vesentlig del av den sosiale kontrollformen (Gundhus, 2007). Fra de tre overnevnte perspektivene kan det forståes at en av de store utfordringene for politiet blir å tilpasse sin tradisjonelle byråkratiske arbeidspraksis til nye kontrollformer som utvikler nye arbeidsmetodikker. Wall (2017a) skriver blant annet at, en del av ansvar til politiet i det moderne samfunnet blir å holde tritt med det sikkerhetsnivået borgerne ønsker, men det må samsvar med hva som faktisk er realistisk for politi og rettsvesen å levere.

2.1.2 Tidlige forskning på politi i møte med digitalisering

Få studier ser på nettverksteknologien i møte med politipraksiser, og veldig få har forsket på dette i Skandinavia. I perioden 2001-2009 var det generelt få studier som tok for seg cyberkriminalitet grunnet manglende statistiske tall og anmeldelser (Wall og Williams, 2013; Jewkes og Yar, 2010). De siste årene har det likevel vært en stødig vekst og et økende fokus både for forskere og for politi (Wall and Williams, 2013). Et studie i Nederland så på hvordan politiet taklet bekjempelsen av avansert cyberkriminalitet, og avdekket at det er såpass store kunnskapsmangler i det nederlandske politiet at de ikke klarer å registrere anmeldelsene tilstrekkelig. Studien viste til at det er en signifikant del av cyberkriminalitet som aldri entrer rettssystemet (Leukfelt, Veenstra & Stole, 2013). Et negativt utfall kan være at rettssystemet stagnerer ved at få saker hindrer oppdateringen av lovverket. Det vil videre gjøre det vanskelig for politiet å rettsforfølge saker. Lignende funn har også blitt gjort i amerikanske studier. Senjo (2004) fant ut at amerikanske politibetjenter sin kunnskap kom for det meste fra mediebildet og av stereotypier, hvilket ikke samsvarte med empiriskdata. At teoretisk og praktiskkunnskap ikke samsvarer kan lede til en politiorganisasjon med ulik arbeidspraksis. Organisasjonen blir lite enhetlig ved at ulike politidistrikt håndterer sakene forskjellig. Eksempelvis, at borgerne får god hjelp til en sak i et distrikt, mens saken blir henlagt i et annet. Det kan føre til minkende tillitt mellom politiet og borgerne, hvilke kan sette spørsmålstegn ved politiets legitimitet. Bossler og Holt (2012) gjorde et makent studie i USA med noe lignende resultat. I likhet med Senjo (2004), studerte Bossler og Holt operativt nivå. Politibetjentene ble spurt spørsmål om lokale politidistrikt skal håndtere cyberkriminalitetshendelser som utspiller seg i lokalmiljøet. Funnene viser at majoriteten av politibetjentene ikke ønsket ha et primæransvar for å takle cyberkriminalitet. Begrunnelsen til politibetjentene var at spesialistavdelinger har bedre verktøy og kunnskap til å respondere på cyberkriminalitet. Politibetjentene anerkjente at endring var nødvendig, men var selv ikke interessert i å gjøre endringer som gikk utover deres daglig tjeneste. Operative politibetjenter er som oftest de borgerne er i kontakt med i sine dagligdagse liv. At politibetjenter fraskriver seg cyberkriminalitet som ansvarsområdet kan føre til minkende samarbeid fra lokalsamfunnet. Det strider da mot for eksempel nærpolitireformen, som vektlegges nærhet til lokalsamfunn som en viktig prioritering (Prop. 61 LS, 2014-2015). Fra studiene ovenfor kan man lese en gjennomgående trend som peker på politiorganisasjoner som generelt har lav erfaring, liten kunnskap og lite innsikt i cyberkriminalitet feltet.

I Storbritannia ytrer Loveday (2017b) at for at politiet skal klare å håndtere nye krav og kriminalitetsutfordringer så kreves det fleksibilitet i rekruteringen. Aller helst rekruttere og hente inn folk fra privatsektoren. Det går ikke å møte digitale utfordringer uten digitalt kompetent personell, argumenterer han. Å utføre store endringer i rekruteringskriteriene til politiet, kan føles utrygt. Manning (1992) hevder at teknologien truer maktbalansen innad i organisasjonen gjennom å undergrave byråkratiet og trolig endre kulturen. Til sammenligning, finner tidligere studier som har sett på teknologiske endringer, at teknologien får innpass, men gjennom en gradvis modningsprosess. Studiet av Chan (2001) viste at teknologiendringer forandrer politipraksiser langsomt, men de store påvirkningene digitaliseringen har på politiet kommer an på hvordan digitaliseringen harmonerer med de eksisterende kulturelle verdiene, ledelsen, styring, nåværende arbeidspraksis og teknologiskevne. En gradvis endring er noe som passer inn med den byråkratiske tankegangen, men som strider mot hurtigheten til nettverkteknologien. Internetteknologien utfordrer de tradisjonelle prinsippene og lager en rekke nye utfordringer for politiet (Castells, 2001).

Wall og Williams (2013) trekker frem to bekymringsfulle måter cyberkriminalitet har utviklet seg på de siste årene. Den ene er at cyberkriminalitet utføres mer og mer av «spesialister» og grupper som utfører ekstremt komplekse og sofistikerte angrep mot datamaskiner.Det bærer likhetstrekk med bekymringen som kommer frem i risikorapportene fra PST (2018) og NSM (2018). Her virker det som det kan være fruktbart for politiet å tenke annerledes, hvis de skal ha en sjans til å bekjempe kriminaliteten. Det kan virke som det ikke bare gjelder endringer i forhold til intern kompetanse, men også en endring i tankesett i henhold til hvem som utøver kriminaliteten og hvordan politiet kan bruke teknologien til sin fordel. En annen bekymring som Wall og Williams (2013) peker på, er «ikke-spesialister» som får større muligheter og rekkevidde til å utføre CK1 og CK2 på grunn av organisering og kommunikasjonsmulighetene sosiale medier åpner opp for. Internett er ikke bare et teknologiskverktøy, men et stort kommunikasjonsmedium (Castells, 2001). På den ene siden blir sosiale medier benyttet som kommunikasjonsplattformer hvor kriminelle mobiliserer seg, på den andre siden benyttes sosiale medier av majoriteten av befolkningen, og kan være et stort hjelpeverktøy for politiet. Politiet kan bruke plattformene til å samle inn informasjon. Viktigheten av informasjonsinnhenting ble tatt opp av Manning (1992). Han

trekker frem at borgerne er politiets hovedkilde til informasjon. Å motta informasjon fra publikum, er essensielt for at politiet skal kunne håndtere situasjoner og problemområder. Kort oppsummert, kunnskapsmangler i politiet viser seg som en trend i tidligere forskning. Det kan få utslag av ulike art. I tillegg ser det ut til at politiorganisasjoners begrenset fremgang kan bunne i overordnede styringsmodeller. Dette vil bli diskutert videre i analysen.

2.2 Teori

Teori gjør det mulig å se på hendelsesforløp, beskrive og forklare prosessen til fenomenet som skal studeres (Gottschalk, 2011:105). Avhandlingen er innsnevret til en forståelse av spesialistenes livsverden, hvilket vil bli diskutert og analysert opp mot politikulturteorien og overordnede kontrollprosesser. Politikulturen vil bli gjennomgående fordi den baserer seg på studier om politiets interne normer, verdier, tradisjoner, tankesett og praksiser. Spesialistenes fortellinger i møte med cyberkriminalitet er en god kilde til informasjon for å forstå samspillet mellom holdninger og opplevelsen informantene har om de intern og ekstern prosessene (Lofthus, 2009). Det faller det seg naturlig å diskutere det i lys av tidligere studier som belager seg på politiets kultur. En kritikk av politikulturen er at kulturen studeres separert fra sosiale, politiske og organisatoriske kontekster (Chan, 1997). Det har jeg tatt høyde for i oppgaven ved å analysere forholdene mellom politikultur, og overordnede styringsformer opp mot informantenes opplevelser.

2.2.1 Politikultur

Politikultur blir beskrevet av Johannessen (2013) som politiets måter å snakke, tenke, handle og utøve arbeidet på. Reiner (2010) skriver at politikultur handler om å tolke hvordan aktører i politiorganisasjonen referer til verden rundt seg og forstår sin rolle i den. Reiner (2010) og Johannessen (2013) er bare to av flere forskere som definerer hvordan man skal forstå politikultur.

Å forstå hva som gir mening internt i politiorganisasjonen er viktig først og fremst fordi politiet spiller en sentral rolle og har en sosial påvirkning på samfunnet vi lever i (Lofthus, 2009:4) Politiet symboliserer lovverket samfunnet er bygget opp på og har en betydningsfull innflytelse på hvem som entrer rettssystemet, hvem som defineres som kriminelle og i hvor stor eller liten grad kriminaliteten blir et bekjempelsesfokus (Lofthus, 2009). En oppfattelse av kulturen er at den motsetter seg forandringer gjennom antagelser om at interne holdninger og verdier står som det største hindret til endring (Newburn, 2013). I deler av politikulturteorien beskrives politikulturen som homogen og uforanderlig. Dette isolerer kulturen og gir et bilde på at det finnes kun én, monolittisk kultur i politiet (Finstad, 2003; Gundhus, 2009). Flere forskere har motsatt seg den overnevnte forståelse, og ved det verget seg for å referer til kulturen som «politikultur» (Finstad, 2003; Gundhus, 2009). Protestantene hevder at kultur eksisterer i varierende grad, og på alle nivå, i alle

interaksjoner (Crank, 2004:33). Det gjør at det ikke finnes én politikultur, for gjennom kunnskapsdeling, erfaring, og dagligaktivitet oppstår det et sett med delte oppfatninger om hvilke praktiske ferdigheter som behøves når man skal håndtere dagligdagse problemstillinger (Crank, 2004). Kulturen påvirkes og endres hele tiden, alt ettersom hvordan miljø og ytre påvirkninger endres og utviklinger skjer. For eksempel, kan endre lederskap innad på en avdeling være med på å endre den allerede eksisterende kulturen som finnes der. En ny leder kan komme inn med annen bakgrunn, erfaring, holdning og sett med praktiske ferdigheter. For å tilpasse seg nytt lederskap, kan avdelingen endre på de allerede aksepterte praktiske ferdigheten og normene som avdelingen besitter.

På en annen side selv om det er snakket om at kulturen er varierende, er det observert at det foreligger generaliserte trekk som går igjen på kryss av politiorganisasjoner. Reiner (2010:118) referer til disse som *«core characteristics».* Reiner sin fremstilling er i tråd med hvordan amerikanske og engelske politiforskere beskrev den klassiske politikulturen på 1960-tallet. Sentrale tematikkene i den klassiske angloamerikanske beskrivelsen er: makt, rase, kjønn, maskulinitet, mistenksomhet, fare, isolasjon og politimoral (Crank, 2004; Reiner, 2010; Chan, 2001; Lofthus, 2009). Trekkene sies å ha opphav fra tjenestemenn og kvinners tilnærming til arbeidsoppdragene de er satt til å gjøre (Granér og Kronkvist 2015). Politiarbeidet er ikke bare oppfattet som en jobb, men et «mission» (Reiner, 2010). Politiet beskrives som tjenestemenn som utgjør «the thin blue line» (Reiner, 2010:120). Beskrivelsen referer til politibetjenter som oppfatter at deres nærvær er det som utgjør en forskjell fra et samfunn i balanse eller et samfunn i total kaos. Reiners beskrivelse av felles yrkestrekk som går igjen på tvers av politiorganisasjoner, sies å være trekk som gjøre politiet motstandskraftige mot endringer innad i organisasjonen (Granér og Kronkvist 2015; Gundhus, 2009). Likevel ser det ut til at litteraturen i høy grad, belager seg observasjoner og studier av «gatepoliti». Sådan er det nødvendigvis ikke trekk som går igjen høyere opp i hierarkiet.

Selv om forskere gjenkjenner at det ikke finnes en kultur, belager litteraturen og teorien seg for det meste på observasjoner gjort av «gatepoliti». Dette gjør teorien i seg selv veldig begrenset dersom man skal tolke andre ledd i organisasjonen enn gatepolitiet. Et viktig bidrag her er boken til Reus-Ianni (1993), som presenterer empiriskforskning av det hun referer til som «street cops» og «management cops». Boken forsøker å vise til forskjeller i

kulturvariasjoner mellom og innenfor politiorganisasjonen. I tillegg til politikulturens begrensinger trekker Johannessen (2013) fram at det innenfor nordisk forskning (vedrørende temaet kultur og læring), bygges på tradisjonalisme. Det er typisk å henvise og bruke standard litteratur som går flere tiår tilbake. Det er lite fremgang på disse områdene. Jeg er til en viss grad enig med Johannessen (2013), hvor det i nordisk politiforskning eksempelvis er begrenset forskning på cyberkriminalitet i møte med politiets kulturer. Til tross for dette har litteraturen vist seg å være nyttig i tolkningsarbeidet. Sådan er jeg uenig i at tradisjonalisme er negativt. Jeg velger heller å se på tradisjonalisme som en grunnmur å jobbe ut ifra.

2.2.2 Tidligere forskning av politikultur

Som beskrevet ovenfor er tidlig forståelse av politikultur at det er en monolittisk, homogen og en maskulin kultur, hvor arbeidsutførelse bygger på tradisjoner og arv (Lofthus, 2009). Det vil, som tidligere nevnt, være veldig isolerende og begrensende å tolke kulturen på denne måten. De sentrale tankene om kultur er nettopp det at man gjenkjenner at kultur verken er bra, dårlig eller ensformig, men heller sentral organiserte prinsipper om sosialt liv (Waddington, 1999). Det er dette som gjør politiet likt som oss, ikke ulik fra oss (Waddington, 1999). Likevel ser man, siden politiforskningens begynnelse på 60-70-tallet, at politikultur har blitt et paraplyfenomen, men med en rekke negative tolkninger av verdier og praktiser utført mellom aktører i politiorganisasjonen (Crank, 2004). Fra tidlig av sentrerte politiforskning rundt misbruk av politimakt, rase, diskriminering og politikorrupsjon, hvilket kan gi en forklarende grunn til den negative tolkningen av politiets kulturer.

Amerikanske Jerome Skolnick (1966) var en av de første til å sette lupe på politiorganisasjonens interne kultur. Skolnick sin forskning blir i dag regnet som banebrytende på dette området (Lofthus, 2009). Skolnick (1966) studerer politiets bruk av makt og hvordan politiet har et ytre press på seg til å produsere, vise effektivitet og vise til resultater. Skolnick hevder at politiet fortere tyr til hardere metoder gjennom slik styring. Nettopp fordi politiet besitter maktutøvelse som verktøy, skiller de seg ut fra andre arbeidsplasser og oppdragsutførere. Politiet er et symbolsk uttrykk for statens myndighet, og en viktig begrunnelse for den moderne stats eksistens (Zedner, 2006). Ved at politiet representerer autoritet og har maktmonopol vil politiet i deres samfunnsoppdrag, ofte støte på fare og uro fra de som er i opposisjon til loven, politiets eksistens og politiets

arbeidsutførelse (Reiner, 2010). Enhver politibetjent må derav forholde seg til å kunne møte på fare i sin tjeneste. På bakgrunn av den tanken har kulturen blitt beskrevet som tøff, maskulin, actionfylt, utfordrende og ferdighetsbasert (Finstad, 2000). Reiner (2010) ytrer at dette er veldig misvisende fordi politiets oppdrag for det meste er trivielle og kjedelige, hvilket medfører at beskrivelse ikke samsvarer med realiteten. Lignende ytringer og funn ble også gjort av Finstad (2003) og Bittner (2005), som finner at svært mye av politiarbeidet handler om service og sosialarbeid. Politiet er sjeldent i farefylte situasjoner, og bruker generelt lite av tiden sin på kriminalitet (Ericson og Haggerty, 1997).

I Norge er det er det foretatt et fåtall studier av politiets kulturer. De studiene som er gjort har vært gjort gjennom fenomenologiske studier. Det er hvordan politiet opplever sin arbeidssituasjon, og hvilke dynamikker som finnes mellom politiets forståelse og utøvelsen av arbeidet som har vært viktig å fange. Det kanskje mest innflytelsesrike og et av de viktigste studiet om norsk politikultur, er studiet om ordenspolitiet utført på midten av 1990-tallet av Liv Finstad (2003). I boken *«Politiblikket»* studerer Finstad hvordan politifolk bruker sitt *«blikk»* som en grunnleggende og en felles måte å leser omgivelsene rundt seg. Boken er et viktig bidrag til nordisk forskning. Bokens gir et innblikk i hvordan operativt politi forstår og ser sin verden på. En annen viktig studie er gjort av Helene I. Gundhus. Boken *«For sikkerhets skyld»* (2009) tar for seg problematikk som er knyttet til innføring av akademisktenkning i operative miljøer og hvilken påvirkningskraft IKT-verktøy har på politiets arbeidsutførelse. Ved å se på hvordan politiets yrkeskulturer responderer på nye implementeringer og forandringer gir boken et innblikk og forståelse i hvordan politiet møter endring. Det har kommet til stor nytte i denne avhandlingen. I nyere tid er boken *«Politikultur: Identitet, makt og forandring i politiet»,* av Stig O. Johannessen (2013) blitt mye omdiskutert. Boken diskuterer hvordan politirollen vil forandre seg i et demokratisk samfunn i endring. Etter 22. juli-rapporten har det vokst frem ytre og indre press på at politiet skal vise til resultater og handlekraft, og at ulike praksiser opererer på ulike måter for å vise dette. Likevel har politiet hatt begrensede, interne forandringer i arbeidsmetodikk, skriver han. Johannessen velger å ta utgangspunkt og studere politikultur ut ifra fire ulike praksiser: den operative, akademiske, byråkratiske og fagforening praksisen. Disse perspektivene er nyttige ved å gi et innblikk i avgjørelsesprosesser fra flere hold.

At politiets kultur former måte politiet tenker, handler og utfører arbeidet sitt på har likhetstrekk med Pierre Bourdieus handlingsteori og habitusbegrep. Det er ikke intensjonen til denne oppgaven å gå videre inn på handlingsteorien, men kun gi denne kort beskrivelse av hvordan Bourdieus habitus begrep forståes og har blitt benyttet av akademikere.

Kort fortalt, Bourdieu beskriver habitus som det som formidler relasjonen mellom aktør og struktur. Habitus er: *«Et system av varige, men foranderlige disposisjoner gjennom hvilke aktørene oppfatter, vurderer og handler i den fysiske og sosiale verden»* (Aakvaag, 2008:160). Habitus kan forståes som en kroppsliggjøring og ikke en mentaltilstand. Habitus kan sammenlignes med beskrivelsen av kulturell kunnskap. Habitus er basert på tidligere opplevelser hvilket gir forrang til erfaringer gjort tidlig i livet (Bourdieu, 1998). Beskrevet som en kroppsliggjort, refleksiv handling tilsier at habitusen er varig og stabil for det om (Aakvaag, 2008). Habitusen i politistudier forståes som politiets kultur, men som hele tiden er i endring alt ettersom den trigges i møte med elementer i livssyklusen. Blant annet referer Gundhus (2009:30) til habitus begrepet i sin beskrivelse av yrkeskultur og hvordan politiarbeidet formes ut fra forståelsen om sin egen kultur. Politikulturen forståes som kulturen som styrer politiets oppfattelse, vurderinger og handlinger i samfunnet. Habitus er ikke bare formet gjennom politiets posisjon i samfunnet men i kontekst innenfor det sosiale feltet (Bourdieu, 1998). Chan (1997:73) har utformet en interaksjonsmodell inspirerer av Bourdieu, hvor hun bruker interaksjonsmodellen til å forståelse hva som spiller inn på politiets arbeidsutførelse. Gjennom politikultur, ytre politiske kontrollprosesser og organisasjonsstruktur blir arbeidspraksis til. Likevel motsetter hun seg tanken om politiet som passive aktører. De spiller aktivt inn i utvikling, motsettelser, forsterkninger og transformasjoner. Chan mener at svakheter i handlingsteorien til Bourdieu er at den ikke tar høyde for politifolks egen vurderings evne. Politiet kan ta avgjørelser som er situasjonsbestemt. Ved at Bourdieu vektlegge disposisjoner og posisjonering ekskludere handlingsteorien vesentlig elementer i politipraksisen. Likevel utfyller teorien på andre punkter. Chan (1997) beskriver at forskningen som er gjort av politikultur har separert kulturen fra de ytre sosiale, politiske og organisatorisk kontekst som omgir polisiær virksomhet. Gjennom Bourdieus handlingsteori mener hun at man kan komplementere forståelsen av politiets syn på verden. I denne oppgaven kommer jeg noen steder til benytte

meg av Bourdieus begreper, særlig for å forklare hvordan politiets habitus påvirkes av ny teknologi.

2.2.3 Konkluderende tanker

Ifølge Crank (2004) finnes det ingen objektiv måte å studere en kultur på, da forskere til en viss grad vil studere kulturer i interaksjon med kulturen de studerer (2004:31). Selv om jeg er klar over begrensningene og er kritisk til å referere til kulturen som politikultur, velger jeg å benytte meg av begrepet. Grunnen til dette er at begrepet er såpass godt etablert i litteraturen, men også fordi jeg mener at det gir en klar referanse til hvilken organisasjon som studeres. Til tross for dette, tilnærminger jeg meg studiet av den norske politikulturen ved at jeg bryter med tanken om at politikultur best forståes i entall. Jeg kommer til å ta høyde for at det finnes flere «subkulturer» innad i politiet, og gjenkjenner at dette er en mangfoldig kultur som stadig er i endring.

3. Metode

I første del av dette kapittelet vil jeg diskutere hvorfor valget falt på kvalitativmetode. Videre vil jeg beskrive utvalgsprosessen, før jeg avslutningsvis i kapittelet vil reflektere over gjennomføring av datainnsamlingen og analyse av datamaterialet.

3.1 Hvorfor kvalitativmetode?

Undersøkelsesformålet har vært å få et innblikk i spesialistenes forståelse av sin verden. I kvalitativforskning er forsøker man å fange historier som trekker frem subjektets følelser, meninger og oppfatninger (Matthew og Ross, 2010). Fra et tidlig stadium var jeg interessert i å forstå det sosiale fenomenet cyberkriminalitet gjennom øynene til aktører som jobber i politiet fordi dette er et felt det er lite forsket på. Ut ifra det fenomenologiske perspektivet ønsket jeg å observere og analysere hvilke holdninger og oppdagelser politiet selv satt med. Det var raskt klart at en kvantitativmetodetilnærming ikke ville kunne belyse og besvare problemstillingen på en slik måte jeg var ute etter. Kvantitativ metode jobber med store mengder strukturert data, eksempelvis: data fra spørreundersøkelser som presenteres numerisk (Matthew og Ross, 2010). Selv om en spørreundersøkelse kunne gitt meg større mengder data og jobbe med, fattet jeg større interesse for oppdagelsene som kunne komme frem fra den dagligdagse talen mellom mennesker. Jeg var ikke ute etter «overflate»-svar, jeg var ute etter en dypere forståelse av problemstillingen jeg skulle undersøke.

I kvalitativforskning kan forskere velge mellom ulike teknikker for å samle inn data, blant annet gjennom feltstudier, observasjon, analyse av tekst, dokumentanalyse og andre medier (Kvale og Brinkmann, 2015). Grunnet tidsbegrensninger valgte jeg bort feltstudier. Dokumentanalyse ble også valgt bort. Jeg hadde fra tidligere av lest rapporter og tidsskrifter som omtalte det temaet jeg var interessert i, men det gav meg ingen nyttig informasjon om hva menneskene bak dette egentlig opplevde. Valget falt dermed på intervju som metode, som også er den mest utbredte måten å fremskaffe data på i kvalitativforskning (Ryen, 2002). Gjennom kvalitativtintervju opplevde jeg å best kunne innhente mening og forståelse om temaet som jeg ønsket å belyse fra den vinkelen jeg ønsket å studere. Likevel, som understøttende materialet har jeg benyttet meg av rapporter fra politidirektoratet.

3.2 Dokumentanalyse

Gjennom hele forskningsprosessen har jeg benyttet meg av rapporter og analyser, utgitt av politidirektoratet, som omhandler cyberkriminalitet og digitaliseringen av politiet. For avhandlingen har det spesielt vært «*Pilotprosjektet 2015-2018*» og «*Datakrimstrategien, 2015*» som har vært relevant. Jeg har brukt rapportene fra POD som et støttemateriale for informasjon om forandringsprosesser som skjer i politiet på nåværende tidspunkt. I tillegg har jeg brukt undersøkelser og rapporter fra andre instanser som jobber med cyberkriminalitet, slik som: NorCert, PST, NorSiS, NUPI og Digi. Rapportene og dokumentene har opprinnelig har hatt et annet formål enn det jeg har benyttet dem til (Thagaards, 2013:59). Dokumentene som er brukt er en refleksjon av myndighetenes offisielle politikk, eller en refleksjon av offentlig diskurs om temaet på et gitt tidspunkt, likevel har rapportene vist seg å være verdifulle ved å gi meg bakgrunnskunnskap jeg har kunnet bygge videre på i avhandlingen og benytte meg av under intervjuprosessen. Rapportene har fylt inn informasjon der empirisklitterære tekster har vist seg å være mangelfulle.

3.3 Intervjuprosessen

3.3.1 Utvalg

Å velge ut et passende utvalg gjør at forskeren må ta flere valg enn kun hvor mange som skal intervjues (Ryen, 2002). Hvor mange som skulle intervjues og hvilke informanter som var av relevans for avhandlingen ble bestem ut fra hvor mange i politiet som jobbet med feltet, avhandlingens tema, tidsbegrensing, problemstillingen, spørsmålene jeg ønsket å stille, og funn i dataene jeg gjorde underveis.

Det er vanlig at antallet informanter varierer, men at det varier ut ifra hva formålet med undersøkelsen er (Kvale og Brinkmann, 2015:148). Å velge ut informanter og miljø gjorde jeg på bakgrunn av den tanken om at personene som kunne belyse min problemstilling måtte ha kunnskap om og være de som satt midt opp i det. Med andre ord var jeg på utkikk etter de som virkelig opplevde, følte på og var vitne til stemning, kultur og holdninger. Målet var å sikre ulike informanter, med ulik spesialistbakgrunn innenfor cyberkriminalitetsmiljøet i politiet. Et slikt mål ble satt for å sikre at jeg fikk informanter med ulike perspektiver, og en variasjon i utdannelsesbakgrunn. Mangfoldet i utvalget ble begrenset av det faktum at det kun er et fåtall som jobber med cyberkriminalitet i politiet, i Norge. Totalt endte jeg opp med å intervjue ni personer. Informantene var ansatte i politietaten, og hadde, som jeg ønsket, sivil- og politihøyskolebakgrunn. Informantene jobbet alle innenfor cyberkriminalitetsområdet, men hadde ulik spisskompetanse og ulike interessefelt. Primært jobbet de fleste med etterretning og etterforskning, i tillegg til utvikling av fag, metode og verktøy. Informantene falt inn under én av to kategorier; beslutningstakere og spesialister. Inndelingen fordelte seg slik: Fire beslutningstakere på ulike nivå i politiet, og fem spesialister. Tre av informantene hadde sivilutdanning, mens de resterende hadde politihøyskolen som grunnutdannelse. Det ble ikke stilt krav til alder, kjønn, bosted eller etnisitet. En trend viste seg likevel fort ved at alle informantene jobbet i Oslo og alle var etnisk norske. Flertallet av informantene var dessuten menn.

3.3.2 Rekruttering

Rekruttering av informanter til avhandlingen gikk overraskende lett. Jeg hadde forberedt meg på en lang og vanskelig prosess, men når ballen først begynte å rulle fikk jeg kontakt med mange som ønsket å delta. Det som viste seg å være tidkrevende var å få satt tid til intervju. Informantene jobbet på avdelinger med hektisk tempo og uforutsette hendelser, hvilket gjorde at tiden for intervjuet kunne bli flyttet eller satt flere uker frem i tid. Uforutsigbarheter gjorde at intervjuprosessen ble lengere enn forventet.

Selve innsamlingsstrategien startet ved at jeg sendte ut skriftliginformasjon på mail i mai 2017. En mail ble sendt ut generelt til politietaten, men også direkte til avdelinger og personer av interesse. Ved hjelp av kontaktpersoner i politiet fikk jeg videre kontakt med flere mulige informanter. Det viste seg å være noe mer vanskelig å få tak i yngre informanter og kvinner. En trend melde seg etter kort tid, hvor alle informantene var fra Oslo, og hvite menn i aldersgruppen 35-60 år ble overrepresentert. På alle arbeidsplassene jeg besøkte var kvinner godt representert, men likevel var det få kvinner som meldte sin interesse. Dette gjorde at jeg etter hvert gikk aktivt ut for å rekruttere kvinner, for å få begge kjønnsperspektiv. Hvorfor det var så få kvinner som ønsket å delta i studiet fikk jeg aldri helt svar på.

3.3.3 Intervjuguiden

Avhandlingens intervjuform var semistrukturert. Denne teknikken ligger nært opp til dagligdagssamtale, og er ikke begrenset som et lukket spørreskjema (Kvale og Brinkmann, 2015). Fordelen ved intervjuformen er at man lager spørsmål ut fra en intervjuguide og nøkkelspørsmål, men selve intervjuet er akseptert som en åpen og fri dialog mellom to parter. Å velge en slik tilnærming gjør at man kan erfare oppdagelser i samtalen som man kanskje ikke har vært bevisst på eller hatt kunnskap om. Ulempen ved denne tilnærmingen kan være at forskerens aktive deltakelse spiller inn på produksjonen av datamaterialet (Matthew og Ross, 2010). Jeg merket at intervjuene skapte en setting som forventer noe av informantene i samtalen (Kvale og Brunkmann, 2015). Det ble satt et tema og samtalen ble i stor grad styrt av intervjuguiden. Det gjorde noe med interaksjonen mellom meg og informantene ved at samtalen til tider ble litt stiv. Blant annet kan det settes i sammenheng

med at noen av informantene ikke hadde sett spørsmålene på forhånd. Ryen (2002) skriver at, informanter som ikke er forberedt på spørsmålene og som er bevisst på tidsbegrensningen i samtalen, kan hurtig prøve å komme opp med svar, selv om det er temaer de ikke har gjort seg opp en mening om.

Gjennom det kvalitative intervjuet ønsket jeg å få svar på utfordringer, arbeidsutførelse, tanker som informantene satt med om cyberkriminalitet, hva som påvirker deres arbeid og hva de selv så på som de største utfordringene og dilemmaene. Før jeg gikk i gang med intervjurundene gjorde jeg pilottest. En pilottest opplevde jeg som fordelaktig ved at jeg fikk testet meg selv i rollen som forsker, jeg fikk prøvd ut spørsmålene, formuleringen, og jeg kunne få tilbakemeldinger på hva jeg eventuelt burde endre på før start (Matthew og Ross, 2010). Da intervjurundene sto på opplevde jeg stor interesse for avhandlingens problemstilling. Det førte til at interaksjonen mellom meg og informantene ble veldig positiv. I tillegg kom informantene med god informasjon og tips i etterkant i henhold til personer jeg burde intervjue, litteratur jeg burde se på og områder jeg burde undersøke nærmere. Siden jeg selv var engasjert i temaet, ble samtalen mer avslappet etterhvert som samtalen utspant seg. Til tross for dette, gjenkjente jeg noen av de overnevnte dilemmaene. At samtalen hadde en tidsbegrensning gjorde at samtalen til tider måtte bli styrt i den retningen jeg som intervjuer ønsket. Ved sånne type inngripelser ble flyten i samtalen brutt opp, og interaksjonen mellom meg og informant forandret seg tilbake til rollene «informant»-«forsker». Det ble ikke den flyten som oppstår i dagligdagse samtaler.

3.4 Gjennomføring og refleksjon

Jeg vil her dra frem ulike elementer som jeg har reflektert på i etterkant av intervjuprosessen. Sted for intervjuet, kontakten mellom intervjuer og informant, og bruk av båndopptaker er tre ulike elementer jeg ønsker å bruke for å besvare om jeg som forsker klarte å lage et rom som åpnet opp for fri dialog og meningsutveksling. Her blir det viktig for meg å vise til en refleksjon rundt min rolle som forsker. Siste del vil ta for seg etikk.

3.4.1 Sted for intervju

Å utføre et intervju drar frem ulike problemstillinger. Som tidligere nevnt, vil det å fastslå et tema og sette av tid og sted for en samtale, automatisk gjøre noe med dynamikken i samtalen. Det var viktig for meg at informantene selv fikk bestemme sted slik at de kunne være mest mulig komfortable. Det viste seg raskt at alle informantene ønsket at jeg kom til deres arbeidsplass i deres arbeidstid. Unntaket var en informant som ønsket å komme til Instituttet for kriminologi og rettssosiologi. Jeg fikk inntrykk av at valg for sted ikke nødvendigvis handlet om trygghet, men heller tidsbegrensninger grunnet hektiske arbeidsdager. Jeg selv trivdes godt med å komme til informantene, fordi jeg på denne måten kunne bruke ventetiden før intervju til å forberede meg, og jeg var trygg på at informantene var i en komfortabel setting. Intervjuet på instituttet opplevde jeg som mer formell, jeg fikk en mer markant rolle som forsker og jeg ble selv mer bevisst på intervjusettingen.

3.4.2 Kontakt mellom intervjuer og informant

Et dilemma som ofte forekom under intervjuene var at personene som ble intervjuet prøvde å svare så korrekt som mulig og etter hva de trodde jeg som forsker ville høre **(**Ryen, 2002). Dette fant jeg ofte i korrespondansen før intervjuet hvor intervjuinformanten ønsket å få tilsendt spørsmålene på forhånd slik at de kunne være mest mulig forberedt, men også under intervjuet. Her ble det spurte flere ganger, - hva jeg var ute etter, hva oppgavens formål var og om de var på riktig spor. Thagaard (2013) skriver at det er en naturlig reaksjon som forekommer før, under og etter intervjuet, fordi intervjupersonene skal eller har kommet med informasjon om personlige og emosjonelle meninger, hvilket setter dem i en sårbar situasjon. Det ble det viktig for meg å gi positive reaksjoner til informantene når de fortalte noe, og jeg så stor nytte av debrifing etter intervju. Da båndopptakere ble slått av lot jeg samtalen flyte litt og jeg spurte informanten om deres opplevelser av intervjuet og om det var noe de hadde fortalt som de ønsket at jeg ikke skulle ta med.

Det andre dilemmaet som dukket opp var rollen som nøytral forsker. Som intervjuer var det vanskelig å forholde seg nøytral i ulike settinger hvor jeg selv hadde sterke meninger og synspunkter. I noen tilfeller førte dette til litt for ledende spørsmål hvor informantene svarte det jeg ønsket å høre. I andre tilfeller førte mitt engasjement til at informantene slappet mer av og tilførte mer informasjon og ny informasjon som jeg ikke visste om. Fra informantene merket jeg en viss avventende holdning i startfasen, samtalen fløt ikke med en gang og det var en mer tilbakeholdenhet i væremåte. Ved å vise mitt engasjement og tilføye min kunnskap, utspant samtalen seg, forholdet mellom meg og informanten ble etablert og de forstod min intensjon med intervjuet. Slik ble også samtalene mer uformelle. Det som vekket diskusjonene og senket garden, var engasjementet og de utfordrende spørsmålene. Ofte fikk jeg positive tilbakemeldinger i etterkant av intervjuet om at jeg hadde kommet med mange gode spørsmål, at temaet var veldig dagsaktuelt, og at intervjuet hadde gitt informantene fine samtaler de selv fikk noe igjen av.

En siste utfordring som dukket opp under intervjuene, var noe jeg ikke hadde forberedt meg på. Som tidligere nevnt påpeker Kvale og Brinkmann (2015) at forskningsintervju ikke er en maktfri og fullstendig fri dialog mellom to likestilte parter. Et vanlig fenomen, skriver de, er at forskeren skaper et asymmetrisk maktforhold, fordi forskeren har vitenskapeligbakgrunn og fører samtalen. Det samsvarte ikke med min opplevelse. De jeg intervjuet var personer i høyere stillinger og som hadde ekspertkompetanse på det temaet jeg ønsket å belyse. Den asymmetriske maktbalanse ble dermed skapt av informantene (Harvey, 2011). Jeg prøvde å være så belest jeg kunne før intervjuene, for at jeg skulle kunne produsere kvalitets materiale, jevne ut balansen, og sådan oppnå tillit fra intervjupersonene (Harvey, 2011). Det jeg likevel ikke kunne forberede meg på var erfaringen disse informantene satt med. Det at majoriteten av informantene hadde lang fartstid i politiet og ekstremt god kunnskap om sitt felt gjorde at deres erfaringer gikk langt forbi det jeg kunne innhente av informasjon fra bøker.

3.4.3 Båndopptaker

Under alle intervjuene ble en båndopptaker tatt i bruk. For meg var dette et nyttig verktøy slik at jeg var sikker på at jeg fikk med meg alt, hadde riktig gjengivelse og kunne lære av

egne feil ved å gå gjennom samtalen i etterkant. Alle samtykket til bruk av båndopptaker, og de fleste informantene fortalte at det var et verktøy de selv var godt kjent med. Selv om ingen hadde innvendinger mot at samtalen ble tatt opp, merket jeg at alle informantene var bevisste på at den var der. De fleste ønsket forsikring om anonymisering, men også uttalelser som «off the record» gjorde at jeg visste at båndopptakeren spilte en rolle i samtalen. Det var i tillegg flere av informantene som kom med god informasjon og hadde en mer frittalende samtale etter at båndopptakeren var slått av.

3.4.4 Refleksjon rundt rollen som forsker

Som diskutert tidligere har min posisjon som forsker og intervjuer påvirket samtalen i mer eller mindre grad. Jeg opplevde intervjuene ulikt fra person til person, men over det hele oppfattet jeg samtalene som gode. At jeg oppriktig var interessert i feltet, og de jeg snakket med følte jeg skinte igjennom, noe som skapt gjensidig engasjement fra begge sider. Det engasjementet oppfatter jeg at var det som skapte spennende og informasjonsrike samtaler. Jeg opplevde ingen ubehagelige intervjuer eller ukomfortable elementer. Det var hele tiden viktig for meg å ikke overskride personene sine grenser, og det var viktig for meg å vise at jeg ikke var ute etter å lure frem historier som ikke skulle frem. Jeg var mer interessert i hvilke oppdagelser som kunne komme frem ved å se ting fra informantenes side. Derfor la jeg også stort vekt på åpenhet rundt studie.

Det er ulike tinge jeg kommer til å ta med meg videre fra intervjusettingen. Det ene er at i henhold til begrensning av begrepsbruk styrte jeg nok samtalen mer enn nødvendig. Ettersom jeg ble trygg i intervjurollen benyttet jeg meg av intervjuguiden mindre og mindre, men jeg kunne gitt litt mer slipp. Det andre jeg tar med meg videre, er at i de settingen jeg selv var trygg og avslappet ble også informantene trygge og avslappet. Derfor vil jeg ta med meg tanken om at valg av sted for intervju har like mye å si for intervjuer som for informanten.

3.5 Etikk

I et forskningsprosjekt vil det forekomme moralske og etiske spørsmål som vil være pågående under hele prosessen (Kvale og Brinkmann, 2015). De etiske dilemmaene er særlig knyttet til hvordan jeg som forsker ivaretar personvern, hvor personlige spørsmål jeg kan stille og hvordan jeg presenterer informasjonen fra informantene i analysen (Thagaard, 2013).

3.5.1 Personvern

Det var viktig for meg å opprettholde informantenes personvern og handle i tråd med etiske retningslinjer. Alle opptak på båndopptakeren ble slettet forløpende etter transkribering og notatene jeg tok underveis har vært sikret på et sikkert sted (Matthew og Ross, 2010). Dokumentene som inneholdt transkriberinger har vært låst og sikret med passord. En presentasjon av studiet, formålet, informasjonsskriv og intervjuspørsmålene ble sendt inn til Norsk Senter for Forskningsdata (NSD). Prosjektet måtte godkjennes av NSD før intervjuprosessens kunne starte. For å sikre anonymisering og personvern av innhentet datamateriale, opprettet jeg en koblingsnøkkel som erstattet navn, personnummer, e-epostadresse eller andre personentydige kjennetegn i et datasett med et kode/nummer som viser til en atskilt liste der hver kode/nummer viser til navn. Koblingsnøkkelen ble oppbevart separat fra selve datamaterialet for å sikre at utenforstående ikke fikk tilgang til koblingen mellom navn og kode. I selve analysen har alle navn blitt anonymisert og erstattet med tall 1-9. Av hensyn til at det ikke skal være mulig å identifisere informantene på andre måter, har alle intervjuene blitt transkribert til bokmål og det har blitt tatt hensyn til geografiskplassering, kjønn og spesialistbakgrunn.

3.5.2 Informasjonsskriv og samtykke

Informasjonsskriv har til hensikt å informere aktuelle informanter om studiet, formålet, hvem som har tilgang til materialet, fordeler og risikoer ved deltakelse (Kvale og Brinkmann, 2015:104) I informasjonsskrivet ble formålet med undersøkelsen presisert, slik at informantene som ble spurte, kunne forbedre seg på og ta stilling til verdien av undersøkelsen. Kvale og Brinkmann (2015) skriver at informasjonsskrivet er viktig for den vitenskapelige verdien av kunnskapen som søkes. I tillegg informerte skrivet om at studiet var frivillig. Informantene fikk beskjed om at de hadde mulighet til å trekke seg fra studiet når de måtte ønske og at studiet var frivillig. Før deltakelse måtte alle informantene

undertegne et informertsamtykke som bekreftet at de var informerte om de overnevnte områdene.

3.6 Analyse av datamaterialet

Dataanalyse var et kontinuerlig arbeid som startet når jeg inntrådte i forskningsfeltet og ble avsluttet når avhandlingen var ferdigstilt (Matthews og Ross, 2010). Analysen og tolkningen av materialet startet allerede etter første intervju. Underveis i intervjuprosessen gjorde jeg meg opp tanker, ideer og refleksjoner rundt det som ble sagt og fremtidige teoretiske perspektiver. Jeg gjennomførte det første intervjuet i juli 2017 og det siste intervjuet i oktober 2017.

Alle intervjuene ble tatt opp på båndopptaker og transkribert fra tale til skriftlig tekst. Jeg valgte å transkribere hvert intervju fortløpende etter at de var gjennomført, med visshet om at dette var en tidkrevende prosess. Intervjuene ble transkribert ordrett og i sin helhet, men fordi cyberkriminalitetsmiljøet i Norge er såpass lite, valgte jeg å transkribere dialekter til bokmål av hensyn til personvern. I tillegg, i overføringen fra transkribering til sitat, ble visse muntlige preg fjernet. Slik som «eh», «ee» ble tatt ut, da jeg anså at disse omskrivelsene ikke hadde en betydning for analyseprosessen og historiene som ble fortalt. Halvorsen (2012:167) sier for eksempel at det å gjøre beslutninger vedrørende hvor detaljert transkriberingen skal være, vil måtte gjøres ut fra hvilket formål undersøkelsen har.

Koding av datamaterialet startet tidlig. Etter å ha transkribert tre intervju startet jeg allerede å se en trend i svarene, og jeg begynte på daværende tidspunkt å dele inn materialet i ulike kategorier. Kategoriene samlet materiale om gjentagende temaer som ble tatt opp og som kunne passe inn med teoretiske perspektiver. Kategoriene ble tildelt farger og utartet seg som følgende; ledelse og kultur, kompetanse, begrepsbruk, maktutøvelse, maskulinitet, tillit, politihøgskolen og risiko. Jeg leste gjennom transkriberte intervju i sin helhet flere ganger i tillegg til å se på korrelasjonen mellom hva de ulike informantene sa om de samme temaene. Det ble viktig for meg å presentere alle ni sine synspunkter slik at alle ble belyst, og for å unngå at noen ble presentert for mye på bekostning av andre.

Den analytiske teknikken jeg valgte å benytte meg av er diskursanalyse. Diskursanalyse jobber med språk (Matthews og Ross, 2010). Jeg som forsker ser på formuleringen av språket og hvilke underliggende ideer som kommer frem gjennom språket (Matthews og Ross, 2010). Jeg går ut ifra tanken om at virkeligheten er sosial konstruert gjennom

individers tanker, formuleringer og beskrivelser av sin opplevelse av verden (Matthews og Ross, 2010). Analysen i seg selv henter også frem etiske dilemmaer ut fra hvor dypt og kritisk jeg kunne gå i min analyse og hvordan jeg tolket uttalelsene fra intervjupersonene (Thagaard, 2013). Det ble i viktig for meg å gjøre vurdering på hvordan jeg presenterte historiene fra informantene i analysen. Som forsker har jeg en helt annen fagbakgrunn og annet perspektiv enn det informanten har, hvilket gjorde at jeg til tider var veldig oppmerksom på at min forståelse preget presentasjonen av funnene. Det ble utfordrende å formulere teoretiske perspektiv og i tillegg prøve å sikre informantenes interesser. Som Thagaard (2013) sier, håndtering av slike vurderinger er viktig for å beskytte informantene mot uheldige konsekvenser av sin deltakelse i forskningsprosjektet. På den andre siden, vil det å tolke materialet opp mot teori og annen empirisk forskning gjøre at funnene kan bli sett i lyset av en større sammenheng og kanskje trekke frem nye forståelser og mønstre i temaene som blir analysert (Thagaard, 2013).

4. Politimakt på nett: interne erfaringer og opplevelser

Første analyse kapitel vil ta utgangspunkt i politikulturen. Målet er å få en forståelse for og avdekke hvilke tanker spesialistene selv sitter med i møte med cyberkriminalitet og hvordan det kan ha en sammenheng med intern kultur i politiorganisasjonen. Første del vil presentere hovedfunn, deretter beveger oppgaven seg over i diskusjon om særtrekk som gjør politi til politi, og hva det vil si i henhold til cyberkriminalitet. Siste del vil ta for seg potensielle endringer og problematiske sider ved utviklinger.

Hvis man tar utgangspunkt i politiloven (1995) §2 nr. 1-4, står det lovfestet hvilke oppgaver politiet skal utføre og hvilken funksjon politiet skal ha i samfunnet (Myhrer, 2014:40). Politiet skal avsløre, etterforske, rettsforfølge og identifisere lovovertredelser. De skal også ha en rådgivende funksjon, være kilde til informasjon og holde ro og orden. De har en lang rekke arbeidsoppgaver og ansvarsområder. Som nevnt i kapittel to, det er få studier som har sett på hvordan politiet opplever, oppfatter og erfarer arbeidet med cyberkriminalitet. Et perspektiv har vært å se på hvordan politiet forholder seg til teknologi som støtteverktøy i arbeidet, et annet har vært å se på hvordan teknologi brukes som styringsverktøy for å kontrollere politiet og overvåke resultater (Chan, 2001; Gundhus, 2009). Det man har tatt mindre stilling til og sett lite på er hva som vil skje når teknologi og digitalisering ikke lenger kun fungerer som en støtte eller et styringsverktøy, men blir politiorganisasjonens nye DNA. Med dét mener jeg, for at politiet skal kunne utføre de lovfestede oppgavene de er satt til å utøve i dagens samfunn, må politiet ta stilling til å nye egenskaper som kan dirigerer oppbyggingen (nettverksteknologi) og se på hvordan det møter overførte egenskaper som ligger som arveanlegg (politikulturer). Her vil det naturlig nok dukke opp endringer som både kan skape indre konflikter, men også store omstillinger.

4.1 Sammendrag

Intervjuene med informantene var preget av sterke meninger om at internett ikke ble benyttet i den graden politiorganisasjonen burde. Det var generelt lite digitalt forståelse og lite vilje til omstilling, fortalte informantene. Cyberkriminalitet er et ansvarsområdet der politiet ikke strekker til. En av spesialistene med lang fartstid i politiet forteller:

> Informant 2: Etaten er litt i ferd med å gå ut på dato. For å sette det litt på spissen. Kompetansemessig så er vi det. Vi henger ikke med i det hele tatt.

En av beslutningstakerne sier noe tilsvarende:

> Informant 3: Vi er jo ingen nyttig aktør på nett. Vi tilbyr jo svært lite. Vi burde vært det. ÅPENBART burde vi vært det. Men vi er ikke godt rusta. Vi tilbyr ikke gode tjenester. Vi kan jo ikke en gang anmelde på nett! Det er svært få forhold du kan anmelde på nett. Det er jo et paradoks da. Du kan ikke en gang anmelde datakriminalitet på n e t t.

Fra det informantene forteller kan det tolkes at informantene mener at politiorganisasjonen ikke følger med. Politiet burde *«åpenbart»* være en nyttig aktør på nett, men det er de ikke. Deres kommentarer kan gjenspeile både frustrasjon og savn. Frustrasjon kan settes i sammenheng med at informantene kanskje ikke er der de føler på at de burde være. Savnet kan knyttes opp mot informantenes behov for at resten av politiorganisasjonen ser det de ser. Et samfunnsbehov som ikke blir fulgt opp og dekket. Informantene er godt informert og har selv god kunnskap om den digitale utviklingen som foregår i samfunnet. Fra beretningene kan det virksom informantene føler et sterkt ansvar for å opplyse resten av politiorganisasjonen. Som fortalt av denne informanten med sivil bakgrunn, vil flere og flere av politiets ansvarsområder flytter seg over til internett:

> Informant 6: Problemet vårt er jo det at større og større del av livene våre flytter seg over på en digitalplattform på et eller annet vis. Altså på et eller annet tidspunkt må vi på en måte slutte og.. Hva skal jeg si.. Tenke at kriminalitet som foregår på nett eller lovbrudd som foregår digitalt ikke er alvorlig nok til at vi skal gjøre noe med det. For det oppstår jo et problem i det gapet mellom kompetansen til de som begår lovbruddene og til de som skal etterforske blir for stor, tenker jeg da. Og det gapet er ganske stort akkurat nå.

Nettverksteknologien åpner opp for nye typer kommunikasjonsformer som organiserer samfunnet på en ny måte (Castells, 2001). I politiorganisasjonen er informantene noen av de få som besitter relevant nok kunnskap til å håndtere cyberkriminaliteten. Fra det

informanten forteller kan det virke som om de ikke får utført de arbeidsoppgavene de er pålagt å gjøre, på en tilstrekkelig måte, fordi de mangler nok ressurser til å ta hånd om den økende mengden med cyberkriminalitet saker. Hvilke konsekvenser det medfører kom blant annet frem i samtalene om hvilken rolle politiet har på nett i dag. To av informantene med politihøgskolebakgrunn forklarer:

> Informant 8: Nei, vi er ikke viktig nok på nett. Det har lenge vært, lenge oppfattet som et lov tomt rom tror jeg. På internett. Man har kunnet gjort som man vil også har det vært noen grad av indre justis på noen arenaer der man har vært på der man er gjenstand for sosialkontroll.

> Informant 5: På nett han man nok ikke. Tror jeg ikke man kan si at politiet som sådan har noen særlig rolle i det hele tatt.

Informantenes fortellinger kan tolkes dithen at anarkiet på nett vil fortsette hvis politiorganisasjonen ikke prioriterer å styrke politiets tilstedeværelse i dette rommet. Den tidlige optimismen som omkranset internett bygget på tanker om at teknologien skulle tilby frihet fra statelige involveringer og sensur, skape sterkere bånd mellom borgerne, og gi en viss kulturell kontroll (Jewkes og Yar, 2010). Ettersom internett har vokst, og flere milliarder mennesker nå benytter seg av internetteknologien i sine dagligdagse aktiviteter, har det ført til en oppblomstring av varierte problemer, trusler og farer (Jewkes og Yar, 2010). Internettbrukeren er sårbar og sårbarhet fører til ønske om sikkerhet. Fra det informant åtte og fem forteller ovenfor, er ikke politiet tilstede på internett i særlig grad. På den andre siden, kunne flere av spesialistene fortelle om en endring. Politiet skulle ha en klar rolle på internett, og den hadde de begynte å etablere, men den måtte videreutvikles.

> Informant 1: Helt klart. Politiets rolle er ikke endret selv om vi har fått en nye sfære å bevege oss i. Samfunnet har fått en ny svære å bevege seg i. Stiller nye krav tenker jeg. Nå vet jeg ikke helt hvordan dette her var. Men når bilen kom så måtte man gjøre ting på en annen måte.

Hva rollen innebærer i dag ble beskrevet at denne informanten:

> Informant 9: Jeg tenker politiet har en rolle for å være, lede arbeidet med ulykker og kriminalitet på nett. Altså på en måte styre, koordinere etaten, så lenge det ikke er en krigssituasjon og Forsvaret tar over. Tenker at politiet har en operativrolle på nett, være tilstede, synlig, uniformert, forebyggende. På en måte være tilstede i grupper der det skjer kriminalitet, forebygge kriminalitet og bruke politiloven på nett. Så man har en operativrolle på nett. Så er det det her med at politiet har en etterforskningsrolle på nett da. Innhente bevis og lage modeller av hva som har skjedd på nett. Også har politiet en rolle med

> kriminalitetsbekjempelse opp imot kriminalitet som blir begått på nett da. Det er jo kanskje forebyggende, men også ren kriminalitetsforebyggende slik som cybercrime da. Jobbe med det på nett da.

Her kan det leses at politiet skal ha de samme ansvarsområder som i den fysiske verden, i den virtuelle verden. Politiet skal ha en operativ, etterforskende og forebyggende rolle på nett. De skal være synlige, uniformerte, og tilstede. Likevel mangler politiet en tydeliggjøring og vurdering av ulike aspekter ved det å være politi på nett. Jewkes (2010), skriver det at mulighetene for de som har tilgang til internett er nesten ubegrenset, hvilket tilsier at cyberkriminaliteten vil bevege seg raskt og hele tiden vanskeliggjør og utfordre arbeidet for politiet. Politiets ansvar i dag er å forhindre og bekjempe all cyberkriminalitet som faller innenfor landets grenser og som ikke tilhører Politiets sikkerhetstjeneste (PST) eller Forsvaret (Piloten, 2017). Cyberspace kan forståes som et nytt domene som politiet må ha kontroll over, men som informanten forteller - det er et området som har fått lite oppmerksomhet i norsk politi. Videre vil jeg presentere ulike problemstillinger som dukket opp i samtalene med informantene. Dette er problemstillinger informantene mente politiet måtte ta innover seg i tiden fremover.

4.2 Maktutøvelse på nett

Politiet skiller seg fra andre instanser ved at de har hjemlet i politiloven at de kan utøve makt i situasjoner hvor det er nødvendig. Dette gir politiet en særegen og unik posisjon i samfunnet (Gundhus og Larsson, 2007:17). I politiloven § 6 er makt utøvd av politiet, definert som: «*et tvangsmessig, fysisk inngrep mot person eller eiendom».* Det står også i loven at maktutøvelse skal anvendes i situasjoner hvor svakere midler er prøvd og alt annet sees på som utilstrekkelig. Referert til som behov- og nødvendighetsprinsippet (Myhrer, 2015:90). At maktutøvelse har blitt et hovedverktøy og en kjernefunksjon i politipraksisen, var ikke tilfelle fra tidlig stadiet. Reiner (2010:207) skriver blant annet at britisk politiet i det 19 århundret ikke hadde mer maktmyndighet enn en vanlig borger. At politiet fikk legitim rett til å utøve makt kom litt senere, da det ble antatt at politiets bruk av makt kunne bli benyttet til å opprettholde lov og orden, og skape ro i samfunnet gjennom avskrekkelse og sikkerhet (Reiner, 2010). Denne tankegangen har fortsatt og i dag har politiet mye makt, men skal helst ikke bruke den (Finstad, 2003).

Skolnick (2005) skriver at, i et forsøk på å forstå politiets syn på verden er det hjelpsomt å prøve å forstå hvilke forhold som kan være med på true politiets autoritet og posisjon. Å ta stilling til vesentlige elementer som beskriver politiet som politi i dag, eksempelvis utøvelse av makt, fortoner seg annerledes på internett. Det kan virke som politiets fravær av kontroll på internett, truer politiets posisjon. På internett må politiet møte fullmakten på en annen måte, det å utøve makt her er ulikt maktutøvelsen på gatenivå. Det kommer frem i en beskrivelse til en beslutningstaker med fagbakgrunn fra politihøgskolen:

> Informant 4: Ja. Vi har ikke noe makt. Når du ikke vil gå hjem fra byen, men jeg sier at du skal gå hjem fra byen, så kan jeg ta tak i kragen din og si - Nå går du hjem fra byen eller så går du inn i den politibilen. Og da er du på måte. Da har du to valg. Makten er rask og reell. Du får føle det her på kroppen ganske raskt. På internett så er det ikke så enkelt. Du kan være anonym og jeg kan ikke ta tak i deg på samme måte. Og når jeg skal ta tak i deg så krever det mye energi, ikke sant. Mye, mye arbeidstid på å finne ut av hvem vedkommende er, hvor han bor og hvordan skal vi gjøre det. Også sitter han i Ukraina, ikke sant. Ja, da må vi innom rettsvesenet osv. Så makt på internett er veldig vanskelig.

Fra utsagnet, og politilovens definisjon av makt, kan det virke som om at det å utøve makt på internett vil være vanskelig fordi politiets maktutøvelse hovedsakelig har belaget seg på en fysisk tilnærming. I tillegg til anonymitet og grenseløs sfære som gjør det vanskelig og

tidkrevende å identifisere lov forbryteren/e. Maktprinsippet i seg selv kan forståes på mange ulike måter. En vanlig oppfatning er å forstå makt som en handling man tvinger på individer som aktiverer motstand. For eksempel, Bittner (2005:15) skriver at den unike eksistensen til politiet ene og alene er at politiet har myndighet til å tvinge frem og pålegge provisoriske løsninger på akutte problemer, uten å måtte forholde seg til og tolerere motstand i noe slags form. Granér og Kronkvist (2014) definerer den type makt som tvangsmakt. I litteraturen om politikultur er makt beskrevet som en utøvelse utført i akutte situasjoner (Crank, 2009). At samfunnet er innforstått med at politiet har lovlig mulighet til å bruke tvangsmakt skal fungere både som sikkerhet i akutte situasjoner, og avskrekkelse. Avskrekkelsesteorien dukket opp med Cesare Beccaria (Reisig og Kane, 2014). Beccaria mente at mennesker var rasjonelle, kalkulerende individer som motstod fra kriminalitet fordi de fryktet å bli tatt eller bli straffet for lov overtredelser (Reisig og Kane, 2014). Til tross for dette har avskrekkelsesteorien har vist seg å være noe mangelfull, da individers valg ikke alltid viser seg å være rasjonelle (Reisig og Kane, 2014).

I den formelle treningen til politiet blir maktutøvelse noe som alltid belager seg på motstand (Crank, 2009). Ved å følge politiloven definisjon og politiets opplæring skal jeg tilnærme meg makt på internettarenaen, hvor det å utøve tvangsmakt vil være begrenset. Spesialistinformanten med politihøgskolebakgrunn forteller:

> Informant 7: Nei, det er vel ingen som har spesiell utøvende makt som driver på nett som jeg vet om, hverken i Norge eller andre steder egentlig.

Yar (2013) skriver at, ved et fravær av et sentralt styre på nett, møter politiet på utfordringer med å håndheve loven, opprettholde orden og oppklare kriminalitet. Birkeland (2007:44) skriver det at hvis samfunnets krav til politiet ikke samsvarer med hva politiet klarer å levere, vil det oppstå det han kaller en *«legitimitetskrise»*. Birkeland (2007:44) deler mellom to hovedsider ved politiets legitimitet og funksjon. Den ene er politiets konkrete effektivitet i å håndheve loven. Den andre er politiets symbolske betydning. Politiet må oppfattes som et symbol på normative struktur og sosial orden. Hvis politiet svikter på en eller to av disse vil borgerne sette spørsmålstegn ved politiets legitimitet.

En institusjon defineres som legitim: *"if and only if it is morally justified in wielding political power, where to wield political power is to attempt to exercise a monopoly, within a*

jurisdiction, in the making, application, and enforcement of law" (Buchanan 2002:689–90 referert i Reisig og Kane, 2014:3). I litteraturen om politilegitimitet står det at, når borgerne opplever politiet som en legitim autoritet i samfunnet vil borgerne i høyere grad følge loven, samarbeide og henvende seg til politiet (Taylor, 2004). Fra definisjonen ovenfor forståes legitimiteten til en organisasjon utfra bruk av makt som er i tråd med lovverket. Makt blir moralsk rettferdiggjort hvis den utøves for å håndheve loven. Å forstå legitimitet bare på bakgrunn av makt og avskrekkelse blir veldig begrenset. Politiet må også vise til at de har evne til å oppnå effektive resultater (Bottoms og Tankebe, 2012). Som tidligere beskrevet i del 4.1, det norske politiet har ikke en symbolsk funksjon på internett enda. I tillegg mangler de nok ressurser til å håndtere cyberkriminaliteten på en effektiv måte. Ved å ta utgangspunktet i perspektivet til Birkeland, kan det se ut til at politiet er på vei mot en legitimitetskrise i møte med cyberkriminalitet. På en annen side, gjentagende empiriske funn i litteraturen om temaet, peker på at politiets legitimitet i bunn og grunn handler om hvor rettferdig politiet er i sin arbeidsutførelse (Reisig og Kane, 2014).

Tom Taylor sitt arbeid åpnet vei for den nåværende forståelsen kriminologien har om politi legitimitet (Reisig og Kane, 2014). Taylor mener det at politiets legitimitet kommer fra borgernes frivillig samarbeid og støtte (2004). Politiet er avhengige av at borgerne aksepterer og velger å følge loven (Taylor, 2004). Tradisjonelt har politiet belaget seg på en instrumentell tilnærming i form av makt som avskrekkelse, men Taylor hevder at det er en ustabil tilnærming fordi det kan variere ut fra situasjoner og omstendigheter. Et samarbeid som er frivillig og som baserer seg på individers egne verdier og motiver for å følge loven vil være mer stabilt, og adferden til individene vil bli selvregulerende (Taylor, 2004). Det kan virke som individer blir motivert til å følge loven, hvis autoriteten viser en stor rettferdighet i måten de utfører sitt arbeid på (Taylor, 2004).

I Norge har politiet relativ høy status og tillit i befolkningen (Larsson, Gundhus, og Granér, 2015). Fra beskrivelsene til Taylor (2004), kan det tilsi at politiet utøver sine oppdrag på en slik måte at det skaper støtte fra befolkningen. Borgerne oppfatter politiet som en legitim autoritet gjennom måten de utfører sitt arbeid på, ikke kun fordi de har maktmonopol. Ved at politiet har høye tillitten, kan politiet ha skapt et sterkt tillitsbånds som vil gi politiet rom og tid til å etablere, og tydeliggjøre sin autoritet og rolle på internett. Likevel krever det at politiet fortsetter å utføre sin arbeidspraksis på en slik måte at de oppnår tillit fra

befolkningen, også på nett. Det krever som Birkeland (2007:44) sier, at politiet viser til effektivitet gjennom evnen til å håndheve loven. Politiet må være rettferdig i arbeidsutøvelsen, men også vise respekt og rettferdighet i situasjoner hvor de må utøve makt.

4.2.1 Illusjonsmakt

Å utøve makt på internett er, som tidligere vist, noe politiet strever med på nett. Maktutøvelsen her strider bort fra fysisk tvangsmakt, over til panoptiskmakt. En av beslutningstakeren trakk frem en interessant vinkling:

> Informant 4: Hvis vi klarer å håndtere ting på nett, så gir vi en illusjon om at vi har makt og klarer å få tak i deg. La oss si at vi får tak i fem prosent av dem som holder på med ting. Det kommer til å være en ganske stor forskjell fra nå. For i det øyeblikket du logger deg på og vet du risikerer å være en av de tusen menneskene i Norge nå som blir tatt for noe på internett, da lar du fort være.

Illusjonsmakt som informant fire betegner det som, er noe politiet også utøver ute på gaten. For eksempel, patruljere synlig ute i trafikken hvor formålet er å få bilistene, som ser politibilen, til å justerer fartet til den lovlig grensen. Denne maktutøvelsen belager seg på en forebyggendeeffekt og individuell selvregulering. For at illusjonsmakt skal ha en funksjon, må borgerne også ha kjennskap til hvilke konsekvenser lovovertredelser kan få eller tidligere har fått. Bilistene vet at høy hastighet kan medføre bot, inndragelse av førerkort eller kort fengselsstraff dersom farten har vært uforsvarlig høy. Innledningsvis ble det trukket frem at risikoen for å bli tatt for noe på nett er relativ lav. Å utøve fysisk tvangsmakt kan være vanskelig når politiet ikke vet hvem de skal utøve makt mot fordi de ikke vet hvem som har utført lovbruddet eller hvor vedkommende befinner seg. Likevel ser det ut til at politiet har klart å få til en viss type illusjonsmakt.

Det man er vitne til i dag er myndigheter som ønsker å få større kontroll over internettadferd i form av overvåkning, i den hensikt å takle og identifisere lov forbrytelser på nett. Eksempelvis, Forsvaret har fått innvilget digitalt grenseforsvar som går ut på å innhente informasjon fra fiberoptiske kabler som går inn og ut av Norge (Lysne, Grytting, Jarbekk Lunde, og Reusch, 2016). Fiberoptiske kabler er der 99 prosent av internett kommunikasjonen foregår i dagens samfunn (Lysne, Grytting, Jarbekk Lunde, og Reusch, 2016). Parallelt har politiet ønsket å få utvidet fullmakter på internett. I 2016 ble det

fremmet et forslag om at politiet ønsket å få lovfestet en endring som sier at de kan bruke skjulte tvangsmidler på internett i forebygging og etterforskning av alvorlig kriminalitet, slik som cyberkriminalitet (Schølberg, 2017). Overvåking som en kontrollmekanisme kan forståes som en type illusjonsmakt som politiet kan utøvet på internett og som internettbrukerne er bevisst på at statens instanser benytter seg av. Spesielt etter avsløringene fra Snowden.

Overvåking av individers adferd på internett er ikke et nytt fenomen. Studier av overvåking har økt i en såpass stor grad at det nå er et eget tverrfaglig spesialistfelt (Yar, 2013:158). Ordbegrensningene i denne oppgaven gjør at jeg ikke vil gå i dybden på overvåkningslitteraturen, men kun trekker frem overvåkning som et eksempel på en type maktutøvelse politiet har på internett og hvorfor denne formen for makt er annerledes.

En måte å definere internettovervåkning på er gjort av Lyon (2015:3) som beskriver overvåking som: «*a general activity, which is to collect information in order to manage or control individuals or groups for a defined purpose*». Å kontrollerer individer og grupper gjennom overvåking kan forståes som en påtvunget handling og vil passe inn under tvangsmakt beskrivelsen, men vil ikke utarte seg fysisk. Illusjonen av makt i form av overvåking, er et fenomen som dukket opp med Jerry Benthams *«Panopticon»,* som var en ide` til å designe fengsel på slutten av 1700-tallet (Newburn, 2013). Pan-optikon betyr: *«Å se alt»* (Christie, 2000:107). Ideen til Bentham gikk ut på å designe et rundt fengsel, nesten som et kakestykke, hvor voktere plasseres i et tårn i midten. Her hadde vokterne full oversikt over alle fangene, og vokterne kunne overvåke fangene til enhver tid (Newburn, 2013). Fangene kunne ikke se vokterne og dermed visste de heller ikke når de ble iakttatt og når de ikke ble det (Newburn, 2013). At fangene følte på å bli overvåket til enhver tid, gjorde at fangene tilpasse sin adferd. På 1970-tallet ble denne ideen videreutviklet og diskutert av Michel Foucault (1977) i *«Panopticism».* Foucault beskriver hvordan overvåking benyttes som et redskap i moderne samfunn til å kontrollere og trene opp individer til hva som er «riktig» adferd. Slik som informanten fire sier; *«du lar fort være»* hvis du tror at du risikerer å bli tatt for noe. Ved å ta utgangspunkt i Foucault, kan overvåking forståes som makt, hvor individer som føler på det kognitive ubehag av maktutøvelsen, regulerer sin adferd slik at individet ikke opplever å bli fysisk straffet. Som beskrevet, utøver politiet også denne avskrekkelsesmetoden ute i det fysiske rom, gjennom tilstedeværelse og synlighet.

Hvis overvåking blir politiets primære maktmiddel på internett, vil det bli overflødig for politiet å anvende fysiske maktmidler fordi det ligger en automatikk bak denne maktutøvelse, hvilket tilsier at fysiskmakt nærmest blir overflødig. Ved at individer konstant føler på å bli iakttatt, kan individer bli selvregulerende ved å tilpasse adferd til de aksepterte normene, lovene og reglene. I tillegg vil politiet kunne ha mulighet til å gripe inn, regulere, irettesette og anbefale metoder som ansees for å være bedre tilpasset den «riktige» normen, når behovet dukket opp.

Til tross for at politiet argumenterer for at innhenting av informasjon gjennom overvåking ansees som viktig i etterforskning og i forebyggingsarbeid, mener Yar (2013) at potensialet for misbruk av makt gjennom overvåking, er altfor fremtredende og invaderende. Som en motstand til denne formen for maktutøvelse har krypteringsteknologien hatt en signifikant økning de siste årene. Castells (2007:171) beskriver krypteringsteknologi som en fundamental teknologi som beskytter det private innholdet i meldinger ved koding. Kryptering kan også skjule identitet og stedsplassering. Individers behov for å beskytte personvern og beholde konfidensiell informasjon gjør at teknologien blir brukt som et redskap for å forhindre at politiet får tak i personlig informasjon og for å forhindre overvåking av bruksmønstre (Yar, 2013:157). Det gjør at politiet får vanskeligheter med å vite hvem som gjorde hva, hvor og når, hvilket tilsier at politiet ikke kan gripe inn når adferden til individer strider mot normer og regler. En av informantspesialistene forteller om utviklingen:

> Informant 6: Fokuset på personvern blir jo større også har vi hatt en god del skandalesaker i media de siste årene. Særlig i USA. Der for eksempel, de store produsentene som Apple, Samsung og alle disse her ser det jo som et markedsføringsfortrinn å tilby kundene sine personvern. Ikke bare for kriminelle, men vern fra statelige aktører, ikke sant. Personvern selger om dagen, da, og det vanskeliggjør selvfølgelig vår hverdag. Det liker jo privatpersonen i meg, men fagpersonen i meg ser jo det som utfordrende.

Fra beretningen til informanten over kan man lese at krypteringsteknologi blir benyttet av de som utøver kriminelle handlinger, men også av individer som føler på et sårbart personvern og ønsker sikkerhet. En vekst i behovet for sikkerhetstjenester kan settes i sammenheng med perspektivet om risikosamfunnet.

I et risikosamfunn kan overvåking forståes som en måte å holde kontroll over de som gjør moralske feil, men overvåking benyttes også som et verktøy for å samle inn kunnskap om de som ikke gjør feil (Ericson og Haggerty, 1997). Basert på denne kunnskapen dannes det rammer for hva som er akseptabel risiko og hva som ikke er det (Ericson og Haggerty, 1997). En påtvunget handling rettferdiggjøres hvis den forhindrer skade (Zedner og Ashworth, 2014). En sånn type kalkulering kan da veie nivået av skadet mot begrensing av frihet (personvern) i den forebyggende fasen til politiet. Et eksempel: Hvis politiet får inn tips om at det kommer til å skje et alvorlig angrep mot Oslo sentrum i nærmeste fremtid, kan politiet velge å benytte seg av overvåking som redskap. Politiet vil kunne argumentere for at overvåkingen av borgernes adferdsmønstre og personlig informasjon i denne tidsperioden kan rettferdiggjøres gjennom tanken om at overvåkingen kan forhindre et angrep som potensielt kan skade mange tusen. Waldron (2006) diskuterer dette som en *«trade off»* hvor vi i bytte for sikkerhet, gir staten tillatelse til å ta bort litt av vår frihet fordi vi forventer at staten kan beskytte oss. Det man er bekymret for ved denne utviklingen, er at grensen for bruker av sterke inngripende midler vil bli mindre og mindre tydelig. I tillegg er overvåking et redskap som ikke kun benyttes av statsmakter.

Som Benthams prinsipp om makt tilsier, kan hvem som helst styre maskineriet (overvåkingen) og få utøvelsen av et viss herredømme. For eksempel, for at internettbrukere skal få benytte seg av Google sine tjenester, må brukerne samtykke til Google sine vilkår. I vilkårene står det beskrevet at Google vil innhente informasjon om brukernes adferdsmønster og personlig opplysninger til eget formål. At internettbrukere samtykker til at Google har disse rettighetene tilsier at Google har et «visst herredømme» over individers personlige opplysninger og adferdsmønstre. Hvis både private og offentlige aktører utøver inngripelser av den overnevnte art, kan det ikke bare ha effekt og konsekvens for politiets arbeidet, men fremtidens internettfrihet. I tillegg kan man lese fra utsagnet til informant seks, at sårbarheten til internettbrukere skaper et stort kommersielt marked for sikkerhetstjenester. Det kan ha sine ulemper. Dette vil bli diskutert mer i del 4.3.

Som vist i diskusjonen ovenfor, har politiet redskaper som kan benyttes til å utøve makt på nett. Selv om det kan skape en viss trygghet kan benyttelsen av teknologiske verktøy i maktutøvelse også gjør samfunnet og borgerne sårbare. En økning i bruk av overvåking, hvor overvåking blir et redskap som også benyttes mot de som ikke bryter loven, kan få utslag i

hvordan borgerne oppfatter politiet sin legitimitet. Det kan være en konsekvens politiet må vurdere når de tar stilling til hva det vil si å utøve politimakt på nett.

4.2.2 Synlig profil på nett

En annen problemstilling som politiet må ta stilling til, er hvordan de skal være synlige, uniformerte, og tilstede på internett. Ute på gaten kan borgerne ut fra uniform, politibil og legitimasjon skille ut hvem som jobber i politiet. Det å bære uniformen markerer en tydelig symbolsk funksjon at 'nå er det politiet man snakker med' (Finstad, 2003). Holmberg og Balvig (2004) bemerker seg i tillegg at uniformen skaper en viss frykt, ved at uniformertpoliti oppfattes som at 'nå er det problem på gang'. Når politiet bærer uniformen må de forholde seg til uniformsreglementet, dette gjelder også politibilens stand (Finstad, 2003). Uniformen fungerer både som gjenkjennelse og som et symbol på statens makt. På internett virker det som det er noe mer vanskelig å opprette denne funksjonen.

I 2015 opprettet KRIPOS nettpatruljen[5]. Nettpatruljen er en tjeneste med hovedformål å aktivt patruljere Facebook og mottar henvendelser fra publikum, med hensikt å forebygge og bekjempe kriminalitet på nett. Funksjonen til nettpatruljen er både rådgiving, mottak av tips og håndhevelse av loven der de har mulighet til det. I tillegg til KRIPOS er det snakk om at alle distriktene skal opprett en egen nettpatrulje. En av spesialistene med politihøgskolebakgrunn forklarer endringsprosessen som er i gang:

> Informant 9: Hva er nettpatruljen og hva er det egentlig vi har bestilt? Jo det er en politipost på nett og den skal rulles ut i distriktene. Det er ikke noe som bare skal være på KRIPOS. Det må på en måte ut til alle, det må på en måte være inn som en pilar i politiet, da. Politiet må jobbe for å skape trygghet på nett. Politiet må snu dette her. Eller så vil folk miste tilliten.

At politiet må være tilstede og synlig på nett var noe informantene mente var en selvfølge. Å ha tillitt fra borgerne var viktig for informantene, derfor måtte nettpatruljen bli en del av alle distriktene. Nettpatruljen skal være et sted på nett som borgerne kan henvende seg til hvis de trengte råd, tips eller ønsker hjelp med saker på nett. Informantene uttrykte at det å opprette nettpatrulje krevde gjennomtenkte vurderingen. Det var mye som skulle falle på plass:

> Informant 8: Men vi ønsker fortsatt å gå mer på personnivå. Vi ønsker å ha profil. Vi ønsker å gå ut og gjøre det. Årsaken til at vi ikke har profil er mange. Det finnes politi i Finland, Estland

[5] https://www.politiet.no/rad/trygg-nettbruk/politiets-nettpatrulje/

> som har webkonstabler. De har valgt det. De har valgt å ha personligprofiler som går på navn. Webkonstabler som bruker sine personligprofiler, identifiserer seg med å være politi. Legitimerer seg som politi altså gjennom profilene sine, og bruker den i aktiv tjeneste. Det har selvfølgelig en del sårbarheter ved at du er på jobb hele tiden. Du har ikke noe backup. Hva hvis det kommer tidskritisk informasjon som du ikke svarer på, ikke sant. Så det er mye sånt. Hva hvis du slutter i jobbet? Derfor har vi ikke valgt å lage sånne profiler foreløpig.

Som informanten peker på, nettet er «døgnåpent», her må politiet ta vurderinger i forhold til ansattes arbeidstider og personvern, ikke bare brukervennlighet for borgerne. Nettpatruljen skal passe inn med intern kultur, lovverk og sosiale forventninger. I tillegg må politiet kunne utøve lignende legitimeringen som de gjør på gata, gjennom uniform, bil og identifikasjon. I samtalene med informantene kunne de fortelle at det å autorisere seg korrekt på nett var vanskelig, og en problemstilling de jobbet aktivt med å finne løsninger på. Informantene mente at riktig autorisering var viktig for å sikre at borgerne skulle bli betrygget om at det faktisk var politiet de snakket med og ingen andre som utgav seg for å være politiet. Som man kan se fra maktutøvelse eksempelet, og synliggjøring av politiet sin profil, må politiet ta stilling til vesentlige elementer som borgerne forbinder med politiet. Politiet står ovenfor vurderinger i henhold til hva det vil si å være politiet i en virtuell sfære. Hvis politiet ikke får til en tydelig profil på internett medfører det et kontinuert fravær av tilstedeværelse og utøvelse av sosial kontroll på internett. En trend som da dukker opp er borgere som i økende grad henvender seg til andre aktører.

4.3 Konkurranse eller naturlig utvikling?

I dag pålegges politiet alt for mange og forskjellige oppgaver, hvilket tvinger frem tverrfaglige samarbeid og tendenser til at flere ikke-statelige aktører utfører såkalt polisiær virksomhet (Gundhus og Larsson, 2007:19). Polisiær virksomhet er det norskeordet for *«policing»,* som refererer til en prosess hvor man driver med formell kontroll med hensikt om å skape sikkerhet og sosial orden (Reiner, 2010). Det er ikke nytt at private aktører tilbyr lignende tjenester som politiet. Zedner (2006) skriver blant annet at politiet aldri har vært alene om å utøve kriminalitets kontroll. Forebygging og opprettholdelse av ro og orden er ansvarsområder som har vært fordelt mellom private, kommuner og sikkerhetsinstitusjoner (Zedner, 2006). Til tross for politiets ambivalensen, har politiet anerkjent at private sikkerhetsaktører bidrar til å møte offentlige og bedrifters krav til beskyttelse (Zedner, 2006). Likevel dukker det opp en rekke problemstillinger når ulike aktører forsøker å utøver kriminalitetskontroll på nett (Yar, 2013:143). En synlig utviklende trend er at skillet mellom hva som er offentlig og private oppgaver viskes ut. Det skaper et konkurransemarked, hvor offentlige og private aktører konkurrerer om å levere sikkerhetstjenester (Gundhus og Larsson, 2007:19). En av informantene med sivil bakgrunn forteller:

> Informant 2: Innenfor datakrimområdet så har private aktører nærmest for lengst tatt over den banen sammen med NSM. Det er vektere som tar datakriminaliteten i Norge. «Vektere» i gåseøyne. Private sikkerhetsselskaper og store sikkerhetsavdelinger i de store sikkerhetskonsernene.

Informanten fortsetter videre:

> Informant 2: De tar over kriminalitetsbekjempelsen fordi politiet ikke har tatt sin plass i den, på det området.

Norsk sikkerhetsmyndighet (NSM) er statlig eid og ligger under Forsvarsdepartementet. På hjemmesiden til NSM står det at: *«Direktoratet er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser».* Naturlig nok har de en vesentlig rolle i bekjempelsen av cyberkriminalitet og er en av politiets viktige samarbeidspartnere. De andre private sikkerhetsaktørene som informanten sikter til - «vekterne», blir i konkurranse med politiet. Som informant to forteller tar de over politiets kriminalitetsbekjempelsen, og skyver politiet ut på sidelinjen fordi politiet ikke har klart å følge opp. Utviklingen kan bli oppfattet som en trussel mot politiets profesjon (Gundhus og Larsson, 2007). På en annen side, cyberkriminalitetens kompleksitet trekker inn flere

fagprofesjoner og krever samarbeidsløsninger. Yar (2013) skriver at, den enorme mengden med saker med tilknytning til internett gjør det nødvendig for politiet å velge ut de sakene som er mest alvorlige, kritiske og som utgjør størst skade. Wall (2007:161) refererer til dette som *«De minimis trap».* Loven håndterer ikke bagateller. At ansvaret fordeles mellom flere aktører må ikke nødvendigvis være negativt eller bidra til konkurranse. Andre aktører som tar på seg noen ansvarsområdet som politiet har, kan frigjøre politiets ressurser (Gundhus, 2007). I neoliberalistiske samfunn, har staten åpent akseptert at det er flere som må ha ansvaret for kriminalitetskontroll (Zedner, 2006). Neoliberalisme referer til en politisk og økonomisk doktrine som har fokus på prinsippene om fritt marked gjennom konkurranse på kryss av landegrenser, og vektlegger minimal statlig intervensjon (Aas, 2013:263). Staten, gjennom sin ideologiske tankemåte, oppfordrer til et et markedssamfunn gjennom promotering om samarbeid og konkurranse (Zedner, 2006). Konkurranse på levering av tjenester ser ut til å bli utfordrende i saker som trekker inn flere aktører.

4.3.1 Eierskapsproblematikk

Det kommer frem i samtalene med informantene at politiet strever med eierskapsproblematikk vedrørende cyberkriminalitetssakene. lNoen av informantene forklarte at uklarhet i eierskap til saker internt, fører til at cyberkriminalitetssakene kan faller ut av systemet:

> Informant 6: Det som gjerne skjer med de datakrimsakene er at. Min erfaring, da, gjennom årene her er at, det er veldig vanskelig å vite hvem som skal ha eierskap til de sakene. Så de havner gjerne hos en seksjon som hverken har kompetanse eller interesse for å si det sånn, til å etterforske de. Dermed så blir det gjerne stuet inn i et hjørne fordi ingen vet hva de skal gjøre med det, og da når de heller kanskje aldri opp på prioriteringslisten».

Fra fortellingen kan det tolkes at cyberkriminalitet blir nedprioritert innad i politiet både på grunn av eierskapsproblematikk, og på grunn av manglende kunnskap. Politiet har en internprosess om sortering av saker til etterforskning gjennom kriminalitetskategorier. Informanten forteller:

> Informant 1: En såkalt trekkinstruks som sier noe om hvem som skal ha de forskjellige saken. Det er en intern greie. Sykkel tyveri trekker stasjonen der sykkel tyveriet skjedde. Drap er det voldsavsnittet som skal ha. Bare en måte å sortere sakene på.

Cyberkriminalitet karakteriseres ved at kriminaliteten foregår gjennom nettverksteknologi, men det vil ikke nødvendigvis tilsi at kriminaliteten er noe særegent. Kriminaliteten som

utføres ved hjelp av nettverksteknologien faller inn under mange ulike tradisjonelle beskrivelser av kriminalitetskategorier. Som beskrevet i del 1.3.3, vil det å sette «cyber»[6] foran betegnelsen skape et inntrykk av at det er noe særegent, hvilket er misvisende. I et snart gjennomdigitalisert samfunn er så og si all kriminalitet knyttet opp mot nettverksteknologien. Ved at politiet har en egne seksjoner og avdelinger som skal håndtere cyberkriminalitet, kan det skape forvirring internt. Det er til tross for at cyberkriminalitets seksjonene og avdelingene i politietaten skal, hovedsakelig understøtte all type polititjeneste. En av beslutningstakerne forteller at politiorganisasjonen ikke er god på utnytte hverandres kunnskap. Det er vern om fagretningene internt. Beslutningstakeren illustrerer:

> Informant 3: Når vi får et drap så er det jo voldsenheten som etterforsker det. Det kan hende at en saken hadde blitt løst svært effektivt hvis org.krim hadde vært inni den saken fra første stund.

Fra det informant seks forteller, politiet er mindre effektive i sakshåndteringen når saken tilhører flere seksjoner. Det medfører at saken faller mellom, og hvis ingen av seksjonen har ressurser eller kompetanse nok til å ta saken, faller saken ut. En konsekvens ved at sakene blir *«stuet bort i et hjørne»,* kom frem i en studie fra Nederland. Leukfeldt, Veenstra og Stol (2013) fant at cyberkriminalitetssakene ville bli henlagt eller flyte ut av systemet hvis de som satt og sorterte ut sakene ikke hadde tilstrekkelig kunnskap om feltet. At sakene ikke entrer systemet tilsier at avskrekkelsestaktikken vil feile. Det kan føre til en oppfordring til cyberkriminalitet fordi risikoen for å bli tatt er lav. Som tidligere nevnt, en økning i cyberkriminalitet på nett kan føre til en økt spredning av private aktører som tar over oppdrag som politiet ikke håndterer. Det trekker frem ulike problemstillinger.

Private aktører kan stort sett drive sine virksomheter fritt ut fra interesser og behov (Lomell, 2015). Det gjør det vanskelig å kontrollere og overvåke det private aktører gjør. Politiet, som offentlig instans, styres av utviklede mekanismer som skal forsikrer at politiet gjør det de skal gjøre. Politiet må stå til rette for og rettferdiggjøre sine handlinger og arbeidsutførelse til borgerne (Yar, 2013). Det eksisterer ikke samme mekanismer for private aktører. Beslutningstakeren forteller:

[6] Politiet bruker definisjonene datakriminalitet og seksjonen for digitalt politiarbeid.

> Informant 3: Det tror jeg kanskje kan være en utfordring. Fordi at det er ikke noen sertifiseringsordning for å drive sikkerhet. Innenfor sikkerhet, informasjonssikkerhetstjeneste i Norge. Så du kan jo påropе deg å ha kunnskap også kjøper bedrifter tjenester fra usertifisert personell, uten kunnskap. Også tror dem at dem er sikret.

Private handlinger foregår stort sett ukontrollert og usynlig (Lomell, 2015). Fra det beslutningstakeren forteller er den negative konsekvensen, at borgerne i god tro kjøper sikkerhetstjenester, men som verken er verifisert eller autentiske. Samtidig får politiet liten oversikt når omfanget blir stort. Det skaper en type kjedereaksjon. Nye former for sårbarhet øker etterspørselen etter sikkerhet og trygghet, som igjen setter nye krav til politiet og utfordrer politiet og statens oppfattelse av hva som er deres ansvarsområde (Aas, 2013). På internett kan det være vanskelig å tegne opp grensen for hva som er offentlig og private ansvarsområder, hvilket medfører at private aktører tar over oppgaver som tilhører den offentlige virksomheten. Samtidig, et samfunn som sentrerer rundt fare, risiko og sikkerhet skaper et samfunn med et veldig negativt preg (Ericson og Haggerty, 1997). Ericson og Haggerty (1997) skriver at, samfunnet får en kognitivt oppfattelse om de hele tiden må forberede seg på det verste. Lengselen etter sikkerhet driver frem en umettelig etterspørsel etter mer og bedre kunnskap om risiko og en etterspørsel etter tjenester som tilbyr betryggelser (Ericson og Haggerty, 1997). En annen konsekvens er at det kan skape en større sosialekskludering ved at private aktører tilbyr «offentlig goder» som en salgsvare. Zedner (2003) syns det er ironisk at sikkerhetsindustrien promoterer fordelaktige goder for alle, men som egentlig bidrar til økt sosialekskludering. Det Zedner sikter til er at det blir et klasseskiller hvor de «rike» kan kjøpe seg sikkerhet, mens de «fattige» må belage seg på hjelp fra politiet. Jewkes (2010) skriver lignende, at når sikkerhet blir en salgsvare kan det skape ulikheter i samfunnet ved at man kan kjøpe seg tjenester som egentlig er grunnleggende menneskelige rettigheter (Jewkes, 2010). I politiloven §2 (1995) står det skrevet at politiet skal *«opprettholde den offentlige orden og sikkerhet».*Politiet skal tilby likhet tjenester for alle i samfunnet. Denne tankegangen bærer sterke likhetstrekk med den neoklassiske troen fra det 19århundre som så på politiets som en forutsetning for frihet og som en integrert del av borgernes sømmelighet, skriver Zedner (2006). Den tankegangen viker fra moderne neoliberalistiske samfunn, hvor kriminalitetskontroll utøves av mange instanser, og hvor staten ønsker samarbeid og konkurranse på levering av tjenester (Zedner, 2007).

Som skrevet innledningsvis, cyberkriminelle kan hurtig utføre handlinger mot flere mennesker, i mange forskjellige land, samtidig. Instanser som utøver kriminalitetskontroll, vil møte på vanskeligheter både internt og eksternt ved at identifiseringen av én problemeier blir utfordrende på nett. I en kronikk i NRK kalt *«Cyberangrep-Hvem har ansvaret?»,* tok Karsten Friis fra Norsk utenrikspolitisk institutt (NUPI) opp eierskapsproblematikken når han diskuterte temaet opp mot cybersikkerhet:

> *«Det er langt flere stater enn disse (USA, Kina, Russland) som gjør internett utrygt, og det er ikke minst en rekke kriminelle og kommersielle aktører som i stadig økende grad (mis)bruker nettet til egne formål... Cybersikkerhet innebærer alt fra enkeltpersoners ansvar for å ikke laste ned skadelig programvare til beskyttelse av nasjonal sikkerhet og kritisk infrastruktur. Dette er et massivt problemområdet».*

På grunn av internett sin rekkevidde, anonymitet og teknologiske komponenter, treffer ansvarsområdet mange forskjellige instanser. Det gjør det utfordrende å utpeke en eier. Hvilket gjør det vanskelig å få til et effektiv og stabilt samarbeid mellom instanser og enkelt personer. Informant fem presenterte en litt annen vinkling. Det var å forstå hvorfor kriminaliteten lot seg gjennomføre. Gjennom forståelse for gjennomførelsen kan man peke ut problemeieren og sådan løse problemet:

> Informant 5: De som er problemeierne i dette er relevant å identifisere fordi at politiet kan være problemet her, politiet kan ha en åpenbar rolle, åpenbart ansvar for å hjelpe eller demme opp et problem. Men det kan også være at hvis vi har en tydeligere forståelse av hva som er konsekvensen, så kan det også være andre naturlig problemeiere som det vil være lettere å peke på som har et ansvar.

Vinklingen bærer sterke likhetstrekk med panoptikon og styring fra avstand. At individer, bedrifter og kommuner oppfordres til å ta ansvar for egen risiko og sikkerhet gjennom instrumentell styring, er et tankesett som man finner igjen i det antatte risikosamfunnet som vi lever i. I korte hovedtrekk vil risikosamfunn tenker annerledes på hvordan borgerne skal styres for å ha et velfungerende samfunn (Aas, 2013:153). Her vektlegges proaktivitet fremfor kontroll av avvikende adferd som allerede har oppstått. Til sammenligning finnes den samme tankegangen i det nye arbeidspraksisen til politiet som vektlegger kunnskapsstyrt politiarbeid og underkategorien problemorientert politiarbeid (POP). Det er ikke til oppgavens hensikt å gå dypt inn i tema, men presentere en arbeidsform som eksisterer i politiet. POP retter fokuset mot problemer og jobber aktivt ut ifra dem (Gundhus, 2009). Målet er å identifisere problemeierne og pålegge dem ansvaret om å rydde opp og

forebygge risikoen (Gundhus, 2009). Det at politiet peker ut problemeiere og pålegger dem å ta ansvar er kanskje ikke en ugunstig løsning. Wall (2001) argumenterer for at flere aktører har en viktig rolle i polisiær virksomhet på nett. På grunn av størrelsen og omfanget til internett vil alt fra enkeltindivider, kommuner og internettleverandører ha et kritisk ansvar for å kontrollere adferd og regelverk på nett. Det var det samme Karsten Friis argumenterte for og det samme som utheves i NSM (2018) sin risikorapport. Rapporten uthever en oppfordring til at individer og bedrifter burde styrke egen kunnskap om sikkerhetstiltak på internett.

4.4 Endring i rekruttering?

4.4.1 *«Det er jo ikke nødvendigvis de som hopper høyest og løper fortest som løser alle politioppgavene best»*

I de foregående avsnittene har jeg trukket frem noen av mange problemstillinger som informantene pekte på at politiet står ovenfor. I denne delen skal jeg trekke frem informantenes ønsker til løsning.

I dag, etter vedtak fra Stortinget om politiets ti grunnprinsipper utarbeidet i 1981, utdanner politihøgskolen det man kaller «generalister» (St.meld.nr.42, 2004-2005). En som kan brukes til alt, som har generell kunnskap om flere områder og gjøremål, men som ikke kan brukes i saker som krever høyere kunnskapskrav (Birkeland, 2007:32). Samtlige av informantene var enige om at politiet må se på hva de trenger av kompetanse og hvilke rekrutteringskriterier de må sette for å oppnå det kompetansenivået de er i behov av. En av beslutningstakerne med politihøgskolebakgrunn viste en stor oppgitthet.

> Informant 3: Og så må vi slutte å telle politiskjorter. Vi må begynne å se på hva vi faktisk trenger av kompetanse. Ja, det er klart, vi trenger blåskjorter i gata. Men vi trenger også annen type kompetanse innenfor denne teigen da. NØDT til å se på politiutdanninga. Ikke minst, se på hvilken tilleggskompetanse. Sivilkompetanse vi trenger.

En av spesialistene med sivilspesialistbakgrunn uttrykte:

> Informant 1: Hvordan vet vi at Norges beste etterforsker ikke sitter i rullestol. Vi gjør ikke det. For han kan ikke løpe 100 meter. Men han trenger ikke kunne det for å etterforske? Du trenger ikke å kunne sette folk i håndjern for å prate med folk på nett. Du kan utmerket gjøre det godt fra en god stol og om den stolen har hjul spiller ingen rolle.

Krav fra samfunnet, en økning i kompleksitet, mangfold og teknologi gjør at politiets ansvarsområder og antall gjøremål øker (Birkeland, 2007:33). Utviklingen gjør at det logisk nok, både fra samfunnet og politiets side, settes spørsmålstegn ved om *«generalistens tid er forbi»* (Birkeland, 2007:33). En av informantene forteller:

> Informant 2: I dag så er jo det du lærer der, å løpe fort, skyte og sloss. Satt på spissen selvfølgelig, men det er det man er opptatt av når man tar opp folk til politihøyskolen. Det er det hoved utdanningen går ut på.

Fra historiene til informantene kan det forståes at politiet er tradisjonelle i måten de rekrutterer på. Å fortsette og rekruttere på samme måten, ekskluderer andre kvaliteter som informantene mener er nødvendig fremover. Informantene samtykket om behovet for en generalist. Likevel uttrykte informantene behov for å ta en vurdering av generalistutdannelsen, spesielt med fokus på å tilby grunnleggende opplæring i hvordan digitaliseringen påvirker borgerne i samfunnet. Størsteparten av informantene var kritiske til PHS sin vurdering av dette i dag:

> Informant 7: Mange av de sakene vi får i dag har opphav fra internett, så det tvinger seg jo frem at vi må kunne mer om digitalisering. Der bør jo også PHS ha et enda større fokus, med tanke på utdanning.

En av beslutningstakerne illustrerte hvorfor PHS burde vektlegge å ha dette i grunnutdannelsen:

> Informant 4: Jeg vil at politifolk skal lære hvordan verden fungerer. Når du putter Philips 20w inn i lampa di hjemme og kan styre den med telefonen din, hva er det som foregår? Hvordan klarer de å kommunisere? Hvordan konsekvenser har kunstig intelligens for eksempel? Hvordan styrer den her bilen seg selv? Altså bare lære litt om verden og hvordan sporkilder er det for eksempel å hente rundt omkring. Når du har låst opp dørlåsen din hjemme fra mobiltelefonen. Er det relevant for politiet? Ja, kanskje det. Kanskje vi kan se loggen der og se hvem som var inni huset ditt på den tiden. Sånne ting. Bare lære litt mer om verden, rett og slett. Helt basic.

I diskursen om rekrutering og kompetansebehov ble det uttrykt at det krever en bedring av den digitale forståelsen innad i etaten og revurdering av rekruteringskriteriene, og utdanningsforløpet på politihøgskolen. Likevel ble det uttrykt at det ikke er noe nytt at politiet går gjennom endringer, heller ikke at de tilpasset seg nye samfunnsbehov:

> Informant 1: Det er Bare en større endring. Og en annen type endring. Oppdagelsen av fingeravtrykk, DNA. Gjorde ordentlig store endringer i hvordan man gjør etterforskning. Oppdagelsen av vitnepsykologi som fagområdet gjorde store endringer i hvordan man tar avhør og den går fremdeles verden rundt. Til og med, med norskefolk i front. Men hva med internett? Ja, vi må gjøre endringer der og. Måten vi jobber på.

Fra utviklingstrekk kan det virke som PHS tar tak i det informantene ønsker. 15 februar 2018 sendte Justis og beredskapsdepartementet ut rapporten *«Politi -og lensmannsetatens kapasitet – og kompetansebehov de kommende tiårene»,* på høring til politihøgskolen. I april

2018 kom høringssvaret. Når det gjelder rekruteringen av spesialister, uttalte Nina Skarpsnes, rektor på PHS dette:

> *«Politihøgskolen er positiv til å øke innsatsen for at flere uten politifaglig bakgrunn kan få utdanning innen spesialområder, for å styrke den totale kompetansen i politiet. Et viktig innsatsområde her er selvsagt digital kompetanse, også på spesialistnivå».*

Som man kan lese fra utdraget ovenfor, PHS er positive til endringer i forhold til nytt samfunnsbehov. Det kom likevel frem av høringssvaret at PHS var skeptisk til å gjøre store endringer i grunnutdannelsen. Generalisten skal fortsette å være hovedaktøren fordi de er politietatens *«bærebjelke».* PHS har liten tiltro til en linjedelt, spesialisert grunnutdanning fordi det vil svekke grunnutdannelsen og etaten. På tross av dette er det foreslått at sivile skal kunne komme inn og få utdanning på PHS innen spesialområder. I tillegg kommer det til uttrykk at PHS i fremtiden skal rekrutering inn et større antall med sivilkompetanse særlig fra informatikk, teknologi og økonomi. Dette er i tråd med hva informanten ønsker skal skje, men det var også andre endringer informantene ønsket seg.

I samtalene som dreiet rundt spisskompetansen som spesialistseksjonen var i behov, ytret alle informantene at det var en kompetanse som en politibetjent ikke kunne bli god på. Den type kompetanse måtte ut og hentes. Hvorfor informanten mente at dette, kommer frem i disse historiene:

> Informant 6: Jeg tror det er lettere å lage en politiansatt av en som jobber teknisk med informasjonssikkerhet enn omvendt, da. Fordi at det er en så, det er en del veldig intrikate tekniske problemstillinger som man må forstå, da må man ha veldig bred, teknisk forståelse. Man må forstå nettverk, og så må man forstå mindsettet til den type kriminelle, da. Og det tror jeg du ikke får inn i løpet av PHS da. Det er en helt annen kriminalitetstanke gang enn hos en tradisjonell kriminell, da.

> Informant 9: Når vi prøver å finne spisskompetanse så prøver vi ikke å finne en politimann som kan det tekniske. Da tar vi inn en ingeniør da, som kan det, som har spisset seg på et felt. Så kan vi heller få han til å fungere i politiet. Og så må du kanskje noen ganger ha den rollen med å prøve å få sydd alt sammen. Få den spisse kompetansen til å passe inn i politiet. Men man er veldig der at vi skal ha politi som skal lære en eller annen spesialoppgave, eller hente den spisskompetansen og tilpasse den politioppgaver. Det er to forskjellige ting. Det er lettere å lære å tilpasse en politioppgave, mer enn å lære en politibetjent å bli teknolog.

Birkeland (2007) skriver det at politiet er i behov av spesialister til mange ulike område, men han stiller spørsmålstegn ved om spesialistene må i tillegg være politifolk for å løse oppgaver for politiet. Vi trenger spesialister, men vi trenger ikke politispesialister (Birkeland, 2007).

Lignende ble tatt opp av Barry Loveday (2017) som skriver at politiet trenger en radikal reform for å møte cyberkriminaliteten. Ikke bare krever cyberkriminalitet høyt kompetent personell, men den type kunnskap og utdannelsesbakgrunn samsvarer ikke med den utdannelse og rekrutteringen politiet gjør. Aas (2013) skriver at internett er noe som er forbundet med høy sosial status, hvilket tilsier at de som utfører cyberkriminaliteten er høyt kvalifiserte og utdannede. Dette utfordrer bildet om at kriminalitet utføres av fattige med lav utdannelse. For å møte et endret kriminalitetsbilde, ønsket informantene endring i tankegangen rundt rekrutteringskriterier. Holt og Bossler (2015) mener at å jobbe med de mest intrikate cyberkriminalitetssakene (les CK1), ikke bare krever kompetanseheving, men teknologiskinteresse. Det mente også denne informanten:

> Informant 6: Det finnes og en del ekstremt dyktige teknologer, holdt jeg på å si, der ute som begår ganske kompliserte.. Som utvikler kompliserte verktøy og som setter i sving ganske sofistikerte angrep da. Og det krever en ganske inngående teknisk bredde forståelse, eller hva jeg skal si. For å etterforske de sakene da. Og da kan du på en måte ikke.. Jeg tror ikke at du kan holde på med andre ting, andre type etterforskning innimellom da. Det er ikke en ting du bare, det er ikke. Jeg tror ikke at du kan sitte å etterforske en drapssak til vanlig, eller drapssaker og sedelighetssaker til vanlig. Du må hele tiden holde deg oppdatert og det er en fulltidsjobb.

At cyberkriminelle selv besitter en dyp, teknisk kunnskap utfordrer de som jobber med dette daglig. Fra informantens historie ovenfor kan det forståes at som cyberkriminalitetsspesialist må du ligge frem på hvis du skal henge med. Utdannelsen som politigeneralist trekker frem helt andre forståelser og interesseområder enn hos de som utdanner seg til å bli teknologer og nettverksspesialister.

4.4.2 *«Vi må forstå samfunnet og da trenger vi mer sivilkompetanse»*

Fra politiet sine hjemmesider står det i statistikken over antall årsverk at politiet, inkludert særorganene (ikke PST), har 5853 sivilt ansatte av totalt 16375. Dette tallet er ekskludert antall jurister. I Oslo politidistrikt er tallet 825 sivile av 3143. Det vil da være sivile med variert bakgrunn. Hvis man skal trekke det ned til cyberkriminalitet og nettverkskompetanse kunne en av informanten fortelle at det er ca. tretti spesialister på cyberkriminalitet i Oslo politidistrikt og noen til i resten av landets politidistrikter. Særorganene er da ikke inkludert. Av de tretti var det ca. femten som hadde sivilbakgrunn. Beslutningstakerne kunne fortelle at de bevisst går inn for å ha en femti/femti prosent fordeling mellom politifolk og teknologer, fordi CK1 saker krevde sivilspesialister med variert teknologisk bakgrunn.

Når samtalen dreide seg rundt hva det betyr for de ulike distriktene at det var såpass få som hadde kompetanse, fortalte en av beslutningstakerne at det var en skjev fordeling i distriktene hvor Oslo satt med relativt høy og god kompetanse. Det kunne skape ulikheter i saksbehandling, og det gikk utover arbeidsoppgavene til som satt med relevant kompetanse:

> Informant 3: Hvis jeg skal anslå. 60-70% av tiden vår brukes på opplæring, kursing, utdanning av de vi bistår i straffesaksporet, altså første linje. Vi holder interne temadager, kurs osv. Vi er med å utvikler tjenesten lokalt der det skal leveres.

At de få ansatte som besitter relevant kompetanse bruker tiden sin på kursing, reduserer politiorganisasjonens kapasitet til sakshåndtering. En annen av informantene fra et av særorganene forteller:

> Informant 9: Disse avdelingene som jobber med cyberkriminalitet er små da og de har ikke kapasitet til å håndtere det store volumet, og generalisten har ikke kompetansen.

Som nevnt i 4.4.1, ble det ytret at det ville være vanskelig for politiet å trene opp en generalist til å kunne være kompetent nok til å håndtere de mest kompliserte sakene. Det gjenspeiles i politiets datakrimstrategien fra 2015, hvor det står skrevet at politiet må få på plass den digitale grunnkompetansen og at sivile med relevant tekniskkunnskap må få større innpass (POD, 2015). I tidligere studier av politikultur diskuteres det at politiet er kritiske til å få inn andre fagprofesjoner. Lofthus (2009) skriver for eksempel, at det er fordi politiet hevder at sivile ikke vil ha den virkelige forståelsen av politirollen, i likhet med at de vil ha begrenset maktutøvelse som fører til at de får lav status internt. Jewkes (2010) beskriver det at, en veldig tradisjonell yrkeskultur som politiet motsetter seg endringene cyberkriminalitet frembringer fordi det tvinger politiet til å undersøke sin kapasitet til å respondere, det krever høyt teknisk fagpersonell som igjen vil avvike fra det teorien om politiet kulturer har beskrevet som «ekte» politiarbeid (se del 4.4.3). Fra de to overnevnte argumentene kan det forståes at det å gi sivile teknologiske spesialister en ganske så sentral rolle i politiet, kan være et mindre populært valg for en politiorganisasjon som belager seg på en stor prosess for å velge ut sine egne.

I boken til Finstad (2003) blir opptakskravene til PHS beskrevet som startpunktet for utvalgsprosessen. Her vil politiet starte å sorte ut egnede kandidater. Ved å endre på hvilke

opptakskrav som skal settes, vil man rokke på grunnleggendeverdier som kanskje foretrekkes. Eksempelvis, i politikulturteorien skrives det gjentakende om at politiideal er bygget opp på maskuline trekk. Den ideelle politimannen har en aura av tøffhet og hyller maktutøvelse fordi jobben tilsier at denne politimannen befinner seg i en verden full av konstant fare og konflikter (Lofthus, 2009:96). Det bærer sterke likhetstrekk med det man definerer som moderne hegemoniskmaskuliniteten. Forestillingen om hegemoniskmaskulinitet understreker verdier som aggressivitet, konkurranseinstinkt, opptatthet av konfliktforestillinger, overdreven heteroseksuell orientering, sterk lojalitet og tilknytning til «inn-grupper». Det er trekk som definerer den ultimate maskuline mannen (Eriksson, 2000:28). Å ha denne oppfattelsen om den ideelle politimannen vil være stereotypisk og begrensende. Det norske politiet i dag består av mangfold. I tillegg, som tidligere nevnt, det er hyppig kritisert i politikulturen fordi det ikke samsvarer med det dagligdagse politiarbeidet og heller ikke krav til arbeidsutførelse. På den andre siden, kan disse beskrivelsen bli funnet igjen i oppfattelsen til et par av informantene. En av beslutningstakerne med politihøgskolebakgrunn illustrerer:

> Informant 4: Min personlig opplevelse, jeg er aldri i fare når jeg er på jobb for eksempel. Det er sjeldent jeg har adrenalinrush når jeg er på jobb, det hadde jeg annenhver dag når jeg jobbet på gata. Det er ikke så mye blålyskjøring og sånne ting. Det er helt annerledes. Det har tatt lang tid for meg å svelge og bli fortrolig med at jeg faktisk ikke.. For det alle vil når de går PHS er å kjøre politibil i full fart. Det er akkurat så kult som det ser ut som, det er sinnsykt morsom. Jeg har aldri hatt det så gøy på jobb som når jeg jobbet ute det året. Du blir lei av det også, men da var jeg fersk. Men det er så fantastisk morsomt å være ute. Og det å skulle være den som løser noe når noe skjer.

Her kan man lese at operativt arbeid som *«kjennes på kroppen»,* blir verdsatt, mens det å jobbe *«inne»* var en tanke informanten måtte jobbe med å godta. Gundhus (2009:106) skriver i sitt studiet at: *«ordentlig politiarbeid er tett knyttet til nærhet til det som utspiller seg av kriminell aktivitet på gata»*. Reuss Ianni (1993:6) referer til dette som «Street cop»-kulturen. «Street cop» kulturen blir beskrevet som den kulturen som gir mening og viktighet til hele politiorganisasjonen «Street cops» må følge mageføelsen, ta hurtige beslutninger i akutte situasjoner. Til motsetning trekker hun frem «Management cops» som tar rasjonelle valg på bakgrunn av standard prosedyrer og regler. «Street cop» kulturen kan sammenlignes med Bourdieus beskrivelser av begrepet Habitus. Habitus som en kulturell forståelse er basert på at handlingsmønsteret er noe som sitter i kroppen, og er refleksiv. Den er trent inn fra tidlig stadiet i livet. Fra det som blir demonstrert her kan det virke som kulturen som blir

innarbeidet i polititreningen, skaper en kroppsliggjort forståelse av arbeidspraksis og er en kulturellforståelse som bærer forrang i politiorganisasjonen. Action, fart, spenning og «fare» er alle elementene i det som defineres som «ekte» politiarbeid.

4.4.3 Det «ekte» politiarbeidet

Det «ekte» også omtalt som «ordentlige» politiarbeidet, diskuteres i politikulturen som det arbeidet som får høyest status innad i politiet og mest bevilgninger utenfra (Crank, 2004; Finstad;2003; Johannessen, 2013). «Ekte» politiarbeid er oppdragsorientert, har momenter av fare og vekker politibetjentens følelsen av å være en kriger som er ute for å utgjøre en forskjell (Crank, 2004:167). Granér (2015) sier at det er mulig å identifisere hva som defineres som ordentlig politiarbeid gjennom tre kriteriet. Det første kriteriet er at lovbruddet skal være tydelig gjenkjennbart som galt. Det andre er at det skal ha en høy straffeverdi, og det å ta gjerningspersonen skal være ytterst viktig. Det tredje går ut på at ordentlige politiarbeid skal inneholde dramatikk, spenning og jakt, fordi det er i disse situasjonene politiet får brukt det de er trent til og maktmiddelet de besitter (Granér, 2015:142). Generelt er det ordenspatrulje og etterforskning som blir klassifisert som ordentlig arbeid, mens forebygging faller nederst på klassifiseringsstigen. Det har blitt kritisert fordi empirisk forskning kan vise til at politiet bruker kun en liten prosentandel av arbeidstiden på å håndtere kriminalitet (Ericson og Haggerty, 1997). Finstad (2003) forklarer opplevelsen av «ekte» politiarbeid med generasjon og kjønnsforskjeller, hvor holdninger til arbeidet nedfeller seg i ulike praksiser og observasjoner. I tillegg skriver Finstad (2003: 102) at fremstillingen om at politiarbeidet handler om blålys og action er en konstruksjon for å gi yrket mer innhold og status. Til tross for dette, virker det som forebyggendearbeid er mindre attraktivt og får minst annerkjennelse fordi teoretisktilnærming og dialog vektlegges (Granér, 2015:142). Tanken om «ekte» politiarbeid bryte med tankesettet til det nye paradigmet som har dukket opp. Paradigmet som vektlegger kunnskapsbasert metodetilnærming med fokus på forebygging og risikovurderinger (Fyfe, Gundhus og Rønn, 2018). Dette vil bli diskutert videre i kapittel fem.

Som vist fra fortellingen til informant fire kan det tolkes at det er en forskjell på å være ute og det å være inne. Det bærer likhetstrekk med funn gjort av Gundhus (2009), som observerer at arbeidsoppdrag som trekker frem det maskuline vil få høyere annerkjennelse. Å være spesialisten i organisasjonen som jobber bak en datamaskin vil kanskje klassifiseres

som «datanerd»-jobben. Eller som Gundhus (2009:229) beskriver: *«kontorpolitiet»*. Å jobbe inne settes i sammenheng med analytiske egenskaper og proaktive arbeidsmodeller. Satt i sammenheng med egenskapene til «ekte» politiarbeid, kan disse egenskapene anses som «avvikende» egenskaper. I litteraturen har «avvikere» blitt diskutert i form av rase og kjønn. For eksempel, kvinner var tidligere oppfattet som det «avvikende» kjønn og ble møtt med trakassering og ulike hindringer fordi deres kjønn truer verdier og bildet av den ideelle, maskuline politimannen (Eriksson, 2000:28).

Fra diskursen om politiarbeid med informantene kom det frem trekk som kan stamme fra det Reiner (2010:115) kaller *«core characteristics»*. Til tross for at informantene viste lignende kulturelle trekk som det Reiner beskriver, viste alle informantene stor interesse og positivitet i henhold til å få inn profesjoner som bryter med politiets foretrekkende habitus. Det understreker poenget med at de kulturelle verdiene i politiorganisasjonen bestemmes ut fra situasjonelle faktorer og endringer. I tillegg, hvis man tar utgangspunkt i at kriminalitetsbekjempelse er politiets viktigste rolle (Ericsson, 2000:29), vil lojaliteten til arbeidsoppdraget vektlegges mer enn de kulturelle verdiene, som igjen tilsier at inntoget av sivile teknologiske spesialister er en nødvendighet for at politiet skal håndtere samfunnsoppdragene i dagens samfunn. Som igjen rettferdiggjør endring.

4.5 Oppsummering

I analyse kapitel fire drøftet jeg historiene til informantene opp mot tidligere observasjoner gjort i politikulturen. Nettverksteknologien ble presentert og tolket gjennomgående i kapittelet sammen med historiene til informantene og politikulturen. I kapittelet kom det frem at informantene mente at politietaten i sin helhet mangler både generell og nok spesialistkunnskap, kompetanse og ressurser til å håndtere cyberkriminalitet. Internett som medium, var i liten grad en integrert del av politiet. I historiene kom det frem at internett var en såpass stor del av samfunnet forøvrig, at det skapte ulike problemstillinger for politiet når de selv ikke handlet ut fra kunnskap om dette mediet.

En problemstilling som ble trukket frem var at politiet måtte vurdere maktutøvelsen de har, opp mot samfunnets utvikling. Her ble det diskutert at politiet for det meste har belaget seg på bruk av tvangsmakt og derfor strever med å utøve makt på internett. Et politiet som strevet med å finne løsning på aspekt som gjør politi til politi, ble diskutert opp mot en mulig legitimitetskrise. Her ble det konkludert med at legitimitet vil være umulig å oppnå kun på muligheten til å utøve makt. Politiets måte å håndtere sin rollen, gjennom å utføre sine arbeidsoppgaver respektfullt, verdig og rettferdig, har skapt et tillittsbånd som vil ha noe å si for deres status som legitim autoritet. Utvikling som forskere har ytret bekymring for er at politiet i økende grad skal benytter seg av overvåking på nett. Det kan ledet mot begrenset frihet og utfordre personvernet til borgerne som igjen kan lede mot legitimitetskrise og minkende tillitt.

En annen problemstilling som dukket opp i kapittel fire er et politi som møter på konkurranse fra private aktører. Som trukket frem i analysen, er det ikke nødvendigvis ugunstig at ansvaret på internett fordeles mellom flere, men litteraturen viser at det trekke frem ulike problemstillinger. Private aktører kan ha et annet formål og ikke vil ikke bli regulert på samme måte som det offentlige. At demokratiske verdier blir en salgsvare, har skapt en bekymret for at balansen mellom offentlige og private ansvarsområder vil vippe over og skap store ulikheter. I samtalene med informantene ble det uttrykt at politiet har blitt skjøvet ut på sidelinjen når det gjaldt cyberkriminalitet sakene. Politiet har ikke kunnskap eller ressurser nok til å håndtere den enorme mengden med saker som kom inn. For at politiet skal opprettholde balansen mellom offentlig og private ansvarsområdet må politiet tydeliggjøre sitt ansvarsområde på nett i større grad enn det de gjør i dag.

I siste del ble informantenes løsning presentert. Informantene ønsket at internett skulle bli en naturlig, integrert del av politiets arbeidspraksis. Informantene ønsket at PHS tilpasset generalistutdannelse, og at politiorganisasjonen rekrutterte inn en høyere antall sivile teknologer. Her ble det konkludert med at informantene ønsket endringer velkommen både fordi det var i korrelasjon med samfunnsendringen, men også fordi det kunne virke som lojaliteten til arbeidsoppgavene veide mest. Å utføre oppdragene på en slik måte at det er i samhandling med politiets formål i samfunnet virket som rettferdiggjorde endringene informantene håpet på. Det var til tross for at endringene strider mot det innøvde og stabile.

5. Ledelse og kultur

Der hvor forrige kapittel fokuserte på politikulturens innflytelse på politiets arbeidspraksis, vil dette kapittelet komplimentere med å se på ytre beslutningsprosesser og styringsmodeller som påvirker spesialistenes arbeidshverdag.

5.1 Ytre prosesser- indre kamper

Endring i politiets arbeidspraksis er i stor grad bestemt ut fra ytre politiske krav (Hestehave, 2018:71). Politiske strategier og utforminger blir konstruert ut fra kriser eller forventede kriser (Reiner, 2010:36). De sosiale, økonomiske og kulturelle transformasjonene man har vært vitne til i det 21. århundre har skapt store endringer for politiet og uromomenter for utførelse av arbeidet (Reiner, 2010:35). Eksempelvis, etter 11. september 2001 kom USA sin deklarasjonen om *«War on terrorism»,* hvor det ble et internasjonalt fokus på risikoanalyser og økt overvåkning. Som en forlengelse av denne tankegangen finner vi nå i 2018, et stort fokus fra statsmakter på proaktivt polisiær virksomhet, hentet fra den risikostyrende modellen. Parallelt med et risikoorientert fokus sies det å ha vokst frem et nytt politiparadigme i den vestlige verden (Hestehave, 2018). Akademikere, politikere og det politiske internasjonalemiljøet har konkludert med at politiet må utarbeide nye, smartere løsninger for å møte nye samfunnsutfordringer (Hestehave, 2018). Politiarbeidet skal i høyere grad være problemorientert, ressursene skal konkretiseres og brukes mer effektivt, og strategiene skal være innovative og fokuserte (Hestehave, 2018). Ideen bak politiets ny arbeidspraksis er at politiet skal bli bedre på å forebygge og respondere på kriminalitet og trusler. Metodikker skal utformes på bakgrunn av kunnskapsbaserte analyser, og i mindre grad på situasjonsorientert erfaring. På en annen side ser man at politiets erfaringsbaserte, reaktive modell fortsatt står stødig som politiets primære arbeidsmodell. Modellen dominerer fortsatt politiets arbeidsmetodikk (Hestehave, 2018).

I diskursene til informantene om ledelse og kultur blir det tydelig uttrykt at politiorganisasjonen blir styrt av en tradisjonell, byråkratisk modell, hvor det gatenære og situasjonsbestemte bærer forrang. Spesielt er det gjeldene i henhold til ressursfordeling innad i organisasjonen. Det kan virke som ressursbevilgninger blir styrt at hvor stor

emosjonell og fysisk skade den kriminelle handlingen har på den som blir utsatt for det. For eksempel kunne fem av ni informanter fortelle at cyberkriminalitet ofte blir nedprioritert fordi de som blir utsatt for denne type kriminalitet ikke synes på samme måte. Informant tre illustrerer:

> Informant 3: Når det er kuler og krutt og blod så gjør det noe med oss. Det er enkelt å forholde seg til. Det som skjer digitalt synes ikke, man ser det ikke, man ser ikke risiko, man opplever ikke risiko før det rammer m e g. Og det gjør noe med valga. Uten tvil…
> Vi hadde justisministeren på besøk her. Og da står vi og forteller i tjue minutter om utfordringen, den digitale utfordringen, risikoarbeidet … Og det er ikke ETT spørsmål ifra salen. Han hadde med seg åtte stykk fra departementet. Annet enn: «Jaja, det er viktig det her, det er viktig det her». INGEN kritiske spørsmål til det som ble lagt frem. Også den neste presentøren. Forteller om bombegruppa i Oslo politidistrikt. Vi trenger en (.....) til 300 000. Det var FULLT engasjement rundt bordet der. Selvfølgelig må vi ha (....). Så enkelt er det.

Det at det ikke er fysisk kontakt mellom den som utgjør en kriminell handling og offeret for den handlingen (Aas, 2013:186), gjør noe med vurderingene. Det bærer likhetstrekk med Granér (2015:141) tre kriterier for hva som blir definert som «ekte» politiarbeid. Det kan virke som det er de samme kriteriene som styrer ressurser og politiske beslutninger. Fra det informant tre forteller kan det forståes at cyberkriminalitet ikke kjennes fysisk på kroppen og tar ikke liv. Faremomentet blir borte. Et sentralt tema i politikulturteorien er fare. Det å forberede seg på og tilrettelegge arbeidet rundt momentet fare er en del av den innarbeidede politikulturen (Crank, 2009:157). I teorien har det blitt kritisert, fordi statistikker og empirisk forskning viser til at politiet sjeldent befinner seg i risikofylte og farlige situasjoner (Crank, 2009: 157; Finstad, 2003; Reiner, 2010). Likevel kan det virke som fare, skade og risiko er de sentrale karakteristikkene for politiske utforminger og tilnærminger. Holt og Bossler (2012) fant for eksempel i deres studie at politibetjenter klassifiserte alvorlighetsgraden ut fra disse vurderingene. Blant annet var pedofili trukket frem som den mest alvorlige typen av cyberkriminalitet. Kriminaliteten ble ansett som at den ville utgjøre størst skade og fare. Å klassifisere kriminalitet ut fra alvorlighetsgrad er ikke nytt for cyberspace, men kompleksiteten her tilsier at når det «*digitalt ikke synes»,* vil det gjøre noe med prioriteringene. Opplevelsen til informant tre, samsvarer med at det er den tradisjonelle styrings modellen som regjerer i politiet. Derimot ser det ut til at kunnskapsbasert arbeid og markedstilpasset styring har begynt å få fotfeste.

Finstad (2015) beskriver en endring i kriminalpolitikken fra strafferettslig standard, til mål og resultatstyring. Bruk av måltall som styring vokste frem på 90-tallet hvor styringsmiddelet ble en ny kontrollform som gav politiet et markedstilpasset preg (Reiner, 2010). Styringsformen kalles vanligvis new public management (NPM) (Granér og Kronkvist, 2014). Formålet til NPM er at lederpraksisen skal omfavne forretning og markedstilpasset styring. Økonomi, effektivitet og synlig resultater fremstår som viktige elementer, mens verdier som rettferdighet og omsorg får mindre plass i et politi som skal være markedstilpasset (Granér og Kronkvist, 2014). Til tross for at NPM ideologien har fått større innpass i politiet, ser det ikke ut til at styringsformen har en plass i spesialistenes daglig tjeneste. Tre av informantene forteller at ledere i politiet ikke har ytre krav på å vise til resultater i henhold til cyberkriminalitet. Det medfører at spesialistene ikke blir målt på arbeidsprestasjon. En informant fra et av særorganene forteller om hva det betyr:

> Informant 9: Ja, det er liksom ikke noe ris bak speilet, men ikke noen gulrot heller da. Man ser ikke noen bevilgninger. Man ser det på et NC3 så har det jo vært et ønske fra politikerne om å få dette på plass og etaten, men så kommer det ikke noen bevilgninger og ikke noen melding om å iverksette det. Ikke noen utredning om hvordan det skal se ut, hva de skal gjøre da. Det er på en måte ingen som i særlig grad har tatt noe ansvar for digitaliseringen av politiet da.

En annen av spesialistinformantene fortalte:

> Informant 1: Det finnes en motivator for de aller fleste. Det er bare snakk om å finne den motivatoren. Jeg tror at for mye mellomledelse så handler det om hva blir de målt på.

NPM styring benytter teknologi som verktøy for å overvåke, styre kostnadskontroll, styring av resultater og som en indikatorer til bruk i risikovurderinger (Gundhus, 2009:21). Måltall indikerer suksess (Lofthus, 2009). Historiene viser et fravær av NPM styring. Det oppfattes som at det påvirker fremdriften og utviklingen til cyberkriminalitetsavdelingene. Slik jeg forstod, ut fra samtalene jeg hadde, anerkjenner ikke ledere cyberkriminalitet som et prioriteringsområdet. Det kan forståes som at det ikke har vært en stor entusiasme eller driv til å heve kapasiteten her. Til tross for at informantene peker på positive sider ved NPM styring, viser litteraturen at det oppstår konflikter ved denne styringsmetoden. At politiet styres av mål og resultater for å øke effektiviteten, har blitt kraftig kritisert. Eksempelvis, Gundhus (2009) fant en motstand fra polititjenestemenn å bli styrt på den overnevnte måten. Det passet ikke inn med erfaring og opplevelser politibetjentene hadde om det «ekte» politiarbeidet. I stedet for å ha den menneskelige tilnærming blir det en stor

automatikk i arbeidsutførelse, hvor målet blir viktigere enn selv arbeidet. Likedan oppleves NPM som en styringsform som står i konflikt med det tradisjonelle, innøvde og stabile (Granér og Kronkvist, 2014). Politiet er i all hovedsak regel og lovverk styrt. Et markedstilpasset politi blir i mindre grad trygt og stabilt og i høyere grad uforutsigbart og robotisert (Granér og Kronkvist, 2014). Menneskene i situasjonen blir mindre viktig. Det er situasjonen i seg selv som skal løses, hurtigst mulig. Disse oppfattelsene kom ikke til syne i samtalen med informanten om NPM. Her ytret informantene et savn etter en denne type styring. Den samme informantspesialisten som ovenfor, forklarer:

> Informant 1: Det som blir målt. Det blir gjort. Hvis politidirektøren har sagt at nå skal vi måle antall timer på kurs der internett står i kursbeskrivelse. Da skal jeg love deg det hadde blitt mye kurs på internett.

Som informanten peker på, vil det å bli målt og resultatstyrt være viktig. Det skaper et økt fokus på det området som blir målt. Det gjenspeiles i observasjoner gjort av Lofthus (2009:102). Hun skriver at politiarbeid som ikke kan tallfestes ikke blir satt pris på i organisasjonen. Arbeidet blir ikke anerkjent, satt pris på eller prioritert. At ledelsen ikke setter krav til måltall og resultater kan settes i sammenheng med problemet med å kvantifisere cyberkriminaliteten. Det er et uoversiktlig, uforutsigbart felt som igjen kan gjøre det vanskelig å forutberegne. Cyberkriminalitet kan dekke en rekke aktiviteter og handlinger (Aas, 2013). Distribueringen og naturen til cyberkriminalitet representerer dermed en rekke utfordringer for politiet som kan få vanskeligheter med å konkretisere effektive tiltak (Aas, 2013).

Når politiet ikke måles på cyberkriminalitet kan det virke som om det ikke bare påvirke resultatoppnåelser, men det tar bort politiets evne til å veilede borgerne. Med begrensede midler til sakshåndtering, etterforskning og utarbeiding av verktøy, begrenses politiets erfaring og kunnskap. Politiet strekker ikke til og borgerne kan oppleve å få mindre hjelp, støtte og veiledning. Effektiviteten til politiet kan bli synkende fordi man på underordnet nivå mangler konkrete mål å jobbe ut ifra. En av beslutningstakerne forteller:

> Informant 3: Når vi ikke har kunnskap om hva vi skal opplyse om, så får vi heller ikke opplyst. Vi mangler et definert bilde av hva vi skal levere av polititjenester i dag.

Det kan virke som internetteknologien har blitt en integrert del av informantenes forståelse av sin verden, men at det samme ikke gjelder for ledelsen. De fleste informantene uttrykte at toppledelsen i politiet manglet forståelse. Begrunnelsen var at de som sitter som ledere i politiet i dag har blitt trent opp og løst arbeidsoppgavene på en annen måte enn det som settes som krav til arbeidsutførelsen i dag. Ledelsen i politiet er en forlengelse av overordnet styresett, og vil representerer muligheter gjennom belønning, profitt og oppnåelser (Gundhus, 2007). Når leder og politiskbeslutninger ikke samsvarer med samfunnsbehovet vil det heller ikke skje store endringer. En av beslutningstakerne med lang fartstid i politiet forteller:

> Informant 2: De gjennomgående kulturelle endringene kommer ikke nede i fra ikke sant. De må komme ovenfra. Da må du ha ledere som etterspør i større grad mål og resultatorientering. Jeg kommer jo fra (…). Som er vant til å ha individuelle planer, og mål og bli fulgt opp i hu og ræva ikke sant. Det var et helt system for hvordan vi ble målt og veid. Fikk jo bonuser og alt mulig sånn. Det funker! Kan si det så enkelt. Det er plusser og minuser med det, men det funker.

En leder som ser verdien av politiarbeid som kroppslig og sitert i det fysiske rom vil skape mindre muligheter for arbeid som omhandler cyberkriminalitet. Det kan virke som suksessfulle måltall settes på de kriminalitetsområdene som kan gi en viss populisme. Kriminalitets som synes og kjennes på kroppen. Høye oppklaringsprosenter, alle helst på alvorlig kriminalitet, er et viktig suksesskriterium (Gundhus, 2007. Det informant to forteller er at ledere vil belønne arbeidstakerne når de viser til resultatoppnåelser som er i tråd med hva lederen har satt som mål. Det er ledelsens sitt fokus som påvirker hvordan ansatte i virksomheten utfører sin arbeidspraksis og hvilket områder de ansatte skal prioritere. At informantene har en annen samfunnsforståelse enn politiorganisasjonens ledelse kan skape frustrasjon, og politiorganisasjonen kan fremstå som lite enhetlig ved at informantene må finne løsninger på problemstillinger som ledelsen ikke ser eller prioriterer.

Likevel fortalte informantene at de opplevde at politiet er i en brytningsfase. Informantene opplevde at flere i politiet begynte å ta innover seg verdien av internett som arbeidskilde. De møtte ikke like mye motstand som før, politiets ledere hadde blitt mer åpne. I tillegg kom det frem observerte endring fra politiskhold.

> Informant 6: Fagfeltet i seg selv innenfor politiet har jo fått mer trykk, sånn politisk sett, sånn at vi vokser jo ganske fort i antall mennesker i avdelinger og inne på seksjonen.

> Informant 7: Det ser jo jeg og siden jeg kom hit i da var det ikke snakk om noe sånt. Da var det jo sånn at man ønsket meg lykke til med jobbingen med (..), tenkte ikke at dette kom til å bli noe, men i dag ser man at situasjonen er helt annerledes. I dag ser man jo hvor skoen trykker og hvor vi bør være.

At fagfeltet har fått et sterkere politisk trykk, understøtter argumentet om at politiske prioriteringer bestemmer politiets kurs. Ut fra historiene oppfattet jeg at det har skjedd store endringer på bare et par år som berører holdninger og prioriteringer internt. Endringen som informantene merket kan naturlig nok settes i sammenheng med strategier, målsettinger og utforminger som vektlegges i politiet på nåværende tidspunkt (se del 2.1.1). Det kan virke som politiorganisasjonen begynner å ta innover seg nettverksteknologiens sentrale funksjon i samfunnet og cyberkriminalitetens omfang, hvilket har startet en synergisk prosess i politiet. Det er likevel ulike hindringer som kan bremse ned prosessen.

5.2 Byråkratisk styring i møte med spesialistene

En klassisk byråkratisk modell har tradisjon på å utføre arbeid stødig og langsomt (Johannessen, 2013:211). Arbeidet skal være lett å dokumentere, standardisere og kontrollere (Granér og Kronkvist 2015). Det gjør den byråkratiske modellen tunge, tradisjonelle og repetitiv i sin arbeidspraksis. En slik modell kolliderer med den hurtige moderne samfunnsutviklingen, som tilsier at man må jobb hurtig og på tvers av fagområder fordi sakene som forekommer vil gripe inn på ulike arbeidsfelt (Johannessen, 2013:211). Fra informantenes historier kan det virke som om alle informantene har akseptert at politiorganisasjonen er tung og tradisjonell. Sånn er det bare. En av spesialistene med politihøyskole bakgrunn og flere år med tidligere operativtjenesteerfaring, hadde dette å si når samtalen dreiet rundt politiet mot 2025:

> Informant 9: Det er en ambisiøs målsetting om man klarer det på kort tid i forhold til hvor treg etaten ellers er til å bli snudd da på en måte. Her er det jo. Man har ikke noen særlig gode verktøy for å påvirke, endre kulturen og arbeidsmønster i etaten sånn totalt sett da.

Lignende svar var gjentagende hos flere informanter i fortellinger om utviklingen i politiorganisasjonen:

> Informant 3: Vi er for tradisjonelle. Vi har ikke noe tradisjon å være innovative innad i etaten på den måten. Vi bare velger å prioritere det tradisjonelle og analoge.

Det informantene forteller understøtter litteraturen om den byråkratisktenkemåten. Det overordnede systemet som styrer organisasjonen, prioritere *«det tradisjonelle og analoge».* Prioriterer det som er trygt. At internett blir en naturlig, integrert del av politiets arbeidspraksis vil da skje som en stødig prosess, ikke som en hurtig omveltning. Det bærer likhetstrekk med funn gjort av Gundhus (2009). Hun peker på at: *«teknologien tilpasses, reintegreres og normaliseres først og fremst i forlengelse av tradisjonelle måter å tenke om politiarbeidet på»* (2009:209). Teknologisk implementering blir en del av en modningsprosess. Det samme ble tidligere observert av Chan (2001) som mener at teknologien vil gradvis komme inn og endre politiet. Det vil være en stødig, men sakte fremgang. Til sammenligning, kan det virke som situasjonen er annerledes i noen andre europeiske land.

Fra informant åtte i del 4.1.2 kommer det frem at Finland og Estland allerede har utarbeidet web konstabler og i Danmark ble et nasjonalt cyberkriminalitetssenter opprettet i 2014 (Trædal, 2017a). Det landet som ligger lengt fremme er likevel Storbritannia. I Storbritannia har den nasjonale strategien for cyberkriminalitet dukket opp med deres forståelse av risikoen cyberkriminaliteten utgjør (Bennet og Stephens, 2014). Alle politidistrikt har en slags spesialenhet som håndterer ulike varianter av cyberkriminaliteten (Yar, 2013). På nasjonalt nivå opprettet Storbritannia, i 2001, et National Hi-tech Crime Unit (NHTCU) som sentraliserer spesialist kompetansen og styrer distriktenes enheter. I 2009 ble Police Central e-crime Unit (PCeU) etabler som har hovedansvaret for å håndtere de mest seriøse cyberkriminalitet sakene relatert til hacking, malware angrep, DDoS angrep og bedrageri (Yar, 2013). I 2011 ble 63 millioner£ øremerket fra regjeringen til å videreutvikle den nasjonale responsen til cyberkriminalitet (Yar, 2013). I 2015 viste regjeringer igjen at de tok grep og utviklet en overordnet strategisk plan *«cyber crime stategy»* (Bennet og Stephens, 2014). Forøvrig, styres britisk politi av det samme byråkratiske styresettet, men her virker det som cyberkriminalitetsfeltet har blitt ansett som et viktig prioritert område i mange år. Til tross for dette, skriver Loveday (2017a) at det er kun de mest seriøse, organiserte cyberkriminalitet sakene som blir etterforsket fordi gruppene nedover i hierarkiet ikke har kapasitet til å håndtere cyberkriminalitetsaker som treffer lokalsamfunnet. Behovet for ledelse som implementerer strategier til å håndtere de mindre kritiske cyberkriminalitet hendelser, har blitt et anerkjent og etablert faktum, og den største utfordringen i britisk politi, skriver han.

Utviklingstrekk i Norge viser at, der hvor Storbritannia var frempå for langt over ti år siden, kommer Norge nå etter. Fra stortingsmeldingen (St. meld. nr 42, 2004-2005) kom det frem at cyberkriminalitet stod høyt på politisk dagsorden over områder politiet skulle prioritere. I 2003 ble åpnet politiet sitt første datakrimsenter, som senere har blitt lagt under KRIPOS (Schølberg, 2017). Til tross for dette har politiorganisasjonen som en helhet, hatt lite fremdrift de siste ti årene. Derimot ser det ut til at politiorganisasjonen nå er i en brytningsfase. Som fortalt innledningsvis, regjeringen nedsatte en gruppe i 2015 som skulle kartlegge og vurdere behovene som politiet har. Den gruppen ble i desember 2017 ferdig med vurderingen og rapporten lå ute på høring på vårparten 2018. I 2017 kom også beskjeden fra politidirektøren om at det i 2018 skulle for fullt jobbes med å etablere et

nasjonalt cyberkriminalitets senter (NC3) som blir politi Norges ekspertorgan på cyberkriminalitet (Trædal, 2017b). Utviklingstrekkene kan da forståes som om at politietaten og staten forøvrig, begynner å ta innover seg cyberkriminalitetens omfang og trusselnivå, men som informantene forteller, det er mye som gjenstår og det vil ta tid. Gundhus (2009:209) skriver blant annet at; *«å mobilisere nytt politiarbeid krever mer enn bruk av ny teknologi. Det krever nye kontroll, og belønningssystemer, andre forståelser av politiarbeidet og strukturelle endringer»*. Det kan forståes som at en helomvending ikke er realistisk, fordi det er mye som skal falle på plass.

På en annen side, selv om informantene godtok at endringer tok tid i politietaten, kom det frem fra diskursene at det lå en slags underliggende konflikt mellom spesialistinformantene og det overordnede styresettet.

> Informant 7: Folk har jo våknet opp underveis, det har jo bare utviklet seg til det positive da, men det tar tid. Og det er som det er. Vi skal gjennom så mange ledd før man får et ja da til å komme i gang. Grunnen til det vet jeg ikke, men kanskje man er redd for å tråkke feil eller redd for å ikke gjøre noe på riktig måte. Vi har jo enda en vei å gå, vi er ikke i mål på langt nær enda. I 2017 er spørsmålet om vi skal opprett nettpatrulje i alle distrikt eller ikke liksom.

Gjennom det informanten sier her, *«folk har jo våknet opp underveis»* kan tolkes som om informantene har sittet å vente på at resten av organisasjonen skal se det de har sett lenge. Det kom i tillegg frem en viss oppgitthet og frustrasjon da informanten snakket om *«redselen for å tråkke feil»* som kan tolkes som om at stabile, innøvde og trygge arbeidspraksiser hindrer fremgang. I den forbindelse kommer byråkratiets uegnethet inn. Informantenes fremtidsrettede og innovative fokus står i kontrast til byråkratisk styring. Frustrasjon kan tolkes som om at politiorganisasjonen burde eksempelvis ha ferdigvurdert nettpatruljen for lenge siden. Hvorfor etaten har bruk tid på *«å våkne opp»* kan ha en sammenheng med hva en av beslutningstakerne forteller:

> Informant 5: Jeg tror man strever litt med å finne ut hvordan man skal få til dette taktskifte da. Fordi det er det det handler om. Det er et skifte som må til egentlig. Måten man tenker, løsningen av politioppdraget, også har man selvfølgelig masse andre krav og forventninger på seg i disse reform tidene med alle andre funksjoner man skal etablere og instanser man ikke skal. Ja, man skal bygge ned instanser og man skal levere på responstid og mot så mange ting som man skal gjøre. Så totalen i forhold til hvor man skal ha fokuset er ganske stor da.

Det informantene sikter til er at politiorganisasjonen i nåværende tid, går igjennom store omjusteringer for å passe inn med en ny nærpolitireform (Prop. 61 LS, 2014-2015). Det at

politiet har en rekke ansvarsområder, krav og må forholde seg til en ny reform kan ha en sterk innvirkning på fremdrift i henhold til cyberkriminalitet. Det informant fem forteller er at det blir det mange områder å ha fokus på. På en annen side, er det kanskje ikke unaturlig at informantene føler på en viss frustrasjon når overordnede bestemmelser kan skape begrensninger. Som beskrevet, det er et fåtall cyberkriminalitet spesialister i politiorganisasjonen i Norge. Det gjør at spesialistene sitter i en særegen posisjon som kanskje kan oppleves som isolerende fra resten av organisasjonen. Spesialistavdelinger og særorganer har en unik, adskilt posisjon i politietaten. Informantene jobber med cyberkriminalitet daglig, ser utfordringer og vil naturlignok tilpasse arbeidspraksis etter behov. I de få observasjonen som er gjort av spesialistkulturer i politiet, observeres det at spesialistene ofte ikke velger å prioritere og følge den byråkratiske modellen (Johannessen, 2013: 73). Til sammenligning, i organisasjonsteorien diskuteres det at små grupper vil ha evnene til å mobilisere og endre seg i et mye hurtigere tempo enn organisasjoner i sin helhet (Schein, 2010). Med det som utgangspunkt kan det tolkes dithen at informantspesialistene gjør innovative valg for å finne praktiske og gode løsninger i sin arbeidshverdag, men som nødvendigvis ikke samsvarer med det innøvde og stabile. Det kan skape en sterk gruppetilhørighet og gruppelojalitet (Johannessen, 2013:73-74).

Isolasjon og solidaritet har i teorien blitt diskutert i forhold til arbeidsoppdrag og tjenestemenn sin opplevelse av å være avskilt fra resten av verden *utenfor* organisasjonen (Lofthus, 2009; Reiner, 2010; Crank, 2004). Det bunner i tjenestemenns særegne posisjon i samfunnet (Crank, 2004). Det kan være at de samme trekkene kan bli gjenfunnet *innenfor* organisasjonen. I akademia bemerkes det ofte at politiet viser unaturlig høy solidaritet seg imellom (Skolnick, 2005; Reiner, 2010). Det sies at faremomentet og autoritets elementene er kontribuerende til politiets sterke solidaritetsfølelse. Det ble tidligere nevnt at spesialistene ikke vil føle sterkt på faremomentet. Deres solidaritetsfølelse kan komme av helt andre ting. Eksempelvis, gruppetilhørighet, lignende kompetansebakgrunn og felles mål. Schein (2010:67) skriver blant annet at i mikrokultur vil delte oppfatninger være et resultat av mange timers arbeidspraksis hvor gruppen har vært gjensidig avhengig av hverandre og samarbeid. Det kan gjøre at gruppen får en avvisendeholdning til andre som ikke jobber og tenker på samme måte (Schein, 2010). Det Schein peker på kan settes i sammenheng med informantenes frustrasjon og avvisende holdning. At politiorganisasjonen styres av en

byråkratisk modell styrer lederes vurderinger og prioriteringer. Som vist, det er den tradisjonelle, reaktive modellen som bærer forrang i organisasjonen. Å holde fast på det stabile og innøvde kan skape frustrasjon og begrensninger for spesialistene. Det er tydelig at informantene jobber i tråd med samfunnsutvikling og i takt med samfunnsbehovet. At spesialistene ser nye utviklingsbehov og ledere ikke gjør det kan skape en sterk solidaritetsfølelse mellom spesialistene , hvor solidariteten reflekteres i holdningene de har mot nåværende styresett.

5.3 *«Det er for mange dinosaurer på norskledernivå».*

Loveday (2017) forteller at en stor utfordring i britisk politi er ledere som ikke setter inn nødvendige strategier til å håndtere cyberkriminaliteten. Til sammenligning, kom lignende oppfattelser til uttrykk i samtalene med informantene. Nedenfor har jeg trukket ut tre av informantenes syn på ledelsere i politiet. En sivil med spesialistkunnskap, en beslutningstaker og en spesialist med politihøgskolebakgrunn. Forøvrig, ingen av de tre nevnte kommer fra samme avdeling eller seksjon.

> Informant 2: Det handler om ledelse og kultur. Manglende evne til omstilling. Manglende evne til å endre seg … For dette er gjerne politifolk som har vært ledere, jurister for den saksskyld. Som har jobbet seg oppover i etaten. Kan faget sitt. Kan veldig mye. Også blir de ledere. Også tror de fremdeles at de kan veldig mye når de har vært ledere etter et år. Problemet er at da har kunnskapen deres bokstavelig talt gått ut på dato.

> Informant 5: Men den tiden at leder i norsk politi kan si at teknologi og internett og sånn så det må jeg overlate til andre. Den tid er forbi da.

> Informant 9: Tror på en måte at man må innse at lederen i etaten er viktig da. Man har liksom ikke noe, hatt noe fokus på kompetanseløft for ledere. Lederutdanning. Så på en måte lederen har vært på en måte opptatt av de dagligdagse problemstillingene og lite i endring og utvikling da.

I diskursene fra informantene kommer det frem kritikk av politiets ledelse. Kritikken går ut på at ledelsen nesten har fraskrevet seg sitt ansvar om å følge med i samtiden. Informantene uttrykker et ønske om at det skal være et større fokus på å etterutdanne ledere. Det kan tolkes dithen at spesialistene opplever at arbeidet stagnerer imøte med ledere som ikke har fokus på *«endring og utvikling».* Tidligere diskutert, ledere som har lite fokus på endring og utvikling forhindrer utarbeidelse av riktig arbeidsmetodikk og fordeling av ressurser. I de foregående delkapitlene har ledelsens vurderinger blitt diskutert opp imot styringsmodeller

og politikultur. I refleksjonen rundt lederes valg dukket det ofte opp en annen vikling. I begrunnelsene til informantene om hvorfor ledere ikke viste stor vilje til omstilling, kom det frem at ledere i politiorganisasjonen bestod av generasjonen ikke-digitaltinnfødte, hvilket betyr at nettverksteknologien ikke har vært en del av den kulturen lederne har vokst opp med. Informantene forteller:

> Informant 9: Det er fortsatt mange i etaten som synes digitale ting er vanskelig da. Generasjonen som er eldre enn deg og meg, som kanskje ikke har vokst opp med internett da. Vi var kanskje de første som vokste opp med internett. Vi har liksom fått det med oss gjennom barndom og ungdomsårene også kommer generasjonen etter oss som har hatt datautstyr fra de var født. Har det på skolen ikke sant og får lekser på skolen som på en måte vil pushe oss da. På det digitale.
>
> Informant 5: Disse digitalt innfødte som går på PHS i dag og kanskje for en tid tilbake også, men de som er ferskest. Politiutdannet. Har ofte også mest digital kompetanse ikke sant. Så de vil naturlig være med å dra dette fremover og prege utviklingen og forståelse over tid.

Lofthus (2009:193) skriver at, politiorganisasjonen et sted hvor det hele tiden kommer inn nye kulturer med generasjonsskifter som konfronterer og setter spørsmålstegn ved de eksisterende kulturene. De digitaltinnfødte som informant fem forteller om, blir også omtalt i litteraturen. Digitalt innfødte er en generasjon som har utøvd meste parten av sin interaksjoner i den virtuelle verden og deres daglig behov og ønsker blir tilfredsstilt av teknologiske enheter (Holt og Bossler, 2015). Internetteknologien kan nesten forståes som digitaltinnfødes medfødte kultur. Generasjonen med digitaltinnfødte vil vurdere og handle gjennom bruk og forståelse for internett. Deres forståelse av verden kan sette spørsmålstegn ved forståelsen til ikke-digitaltinnfødte og utfordre det tradisjonelle med det nye. Ut fra historien kan det forståes som at politiets ledelse faller under kategorien ikke-digitaltinnfødte. De vil ha vanskeligheter med å tilpasse seg internettutviklingen og derfor viser de en viss motvilje til omstilling. Digitaltinnfødte har ikke samme vanskeligheter. Internett er en del av en innarbeidet forståelse, trent inn fra tidlig stadiet og gjennom hele oppveksten. De digitaltinnfødte vil naturlig nok dra politiet fremover. I litteraturen kommer det frem at, det er forventet at digitaltinnfødte vil bevege seg inn i rettsvesenet og politiet, og øke det teknologiske nivået (Ablon og Libicki, 2015). De vil være med på gjør omveltende endringer. Lofthus (2009), på den andre siden, mener at nye generasjoner og kulturer kan ha en påvirkning på eksisterende kultur, men at det vil bli feilaktig å si at de vil overstyre. I relasjon til politiet mener hun at nye generasjoner ikke vil ha avgjørende innvirkning på den

hegemoniske kulturen som står stødig og har gjort det gjennom generasjoner og årtier. Hun mener at det er fordi det vil kreve en radikal demontering av synet politiet har av sin egen rolle og en kraftig revurdering av den rollen sett i samfunnsperspektiv. Det kan virke som at det stemmer til en viss grad med oppdagelser gjort i oppgaven. Det har blitt vist at den dominerende operative yrkesforståelsen står stødig hos ledelsen i politiorganisasjonen. Til tross for dette peker utviklingstrekk og nye styringsmodeller på endringer som allerede har funnet plass og som i en viss grad har startet å endre politiets arbeidspraksis. Det kan virksom nye samfunnskrav og ny generasjon sammen presser frem endringer. Endringer informantene peker på at er nødvendig. I likhet med at digitaltinnfødte sprer seg i arbeidsmarkedet vil de i like økende grad, være de som utfører cyberkriminalitet. Endring i samfunnskrav og kriminalitetsbilde har potensiale til å sette i gang store overstyrende prosesser, men om det er inntoget av en ny generasjon som skaper endringen er noe mer vagt diskutert i litteraturen.

5.4 Oppsummering

I kapittel fem introduserte jeg hva informantene tenkte om ledelse og beslutninger tatt på overordnet nivå. Her har politikultur blitt diskutert opp mot styringsformene risiko og markedstilpasset styring. Igjen valgte jeg å diskutere internetteknologien gjennomgående i drøftelsen. Her kom det frem at de nye type styringsformer utfordret politiet tradisjonelle arbeidspraksis.

Det kan virke som det operer to typer styringsformer i politiet. En tradisjonell styringsform, forankret i byråkratisk styresett, og en ny styringsform forankret i risikoorientert styring. Informantene opplevde at det var den tradisjonelle styringsformen som styrte deres arbeidsdag, men at de ønsker flere elementer fra den risiko, fremtidsrettede modellen fordi det ville effektivisere deres arbeid med cyberkriminalitet. Her ble det konkludert med at siden cyberkriminaliteten ikke utgjorde (foreløpig) en stor fysisk fare, så ble det heller ikke høyt prioritert. Politiske prioriteringer styres etter populisme, det som er tydelig og synlig. Når det ikke ble stilt krav til ledelsen i politietaten om å levere resultater i henhold til cyberkriminalitet, fikk spesialenhetene lite bevilgninger som igjen førte til at spesialistene manglet både gode verktøy og nok ansatte til å håndtere cyberkriminaliteten. Cyberkriminaliteten som ikke ble mål og resultatstyrt, ble det heller ikke prioritert.

Informantene følte på at de ikke er tilstrekkelig tilstede på internett. Det gjorde at informantene ytret savn etter å bli styrt gjennom NPM. Fordi det som ble målt ble gjort.

Videre ble Internetteknologien diskutert som et medium som har potensialet til endre tradisjonelle, byråkratiske arbeidsmåter. I samtalene med informanten ble det påpekt at politiorganisasjonen var tung og tradisjonell, sånn var det bare. Likevel ble ledelsen sterkt kritisert av informantene for å ikke tilpasse seg. Ledelsen som ikke hadde kompetanse om samfunnsutviklingen, og som skulle ta fremtidsrettede beslutninger ble møtt med motstand fra informantene. Her ble det konkludert med at ledelsen måtte ta ansvar og jobbe inn nettverksteknologien i sin egen forståelse av verden. På en annen side uttrykte flere informanter at det hadde skjedd en endring. Informantene merket en endring i politiskfokus og holdninger internt. Det ble satt i sammenheng med generasjonen av digitaltinnfødte. Internett ble diskutert som digitaltinnfødtes medfødte kulturell forståelse. Sammen med nye samfunnskrav og et inntoget av digitalt innfødte i politietaten opplevde informantene at det de siste årene hadde skjedd vesentlig forandringer i politiorganisasjonen.

6. Avslutning

Studiets hovedanliggende har vært å rette blikket mot informantenes erfaringer, tanker og opplevelser av møtet med cyberkriminalitet. Som beskrevet gjennomgående i oppgaven, er cyberkriminalitet kompleks. Hvorfor cyberkriminalitet oppfattes på denne måten, henger sammen med internetts natur. Nettverksteknologi har blitt en global kommunikasjonsplattform som har endret måten vi forholder oss til hverandre på. Internett går på kryss av landegrenser, og muliggjør hurtig deling og lagring av informasjon. Det gjør at strukturen på kriminalitetsutførelsen har forandret seg. Kriminalitetsforholdet har blitt asymmetrisk ved at individer og grupper kan utføre kriminelle handlinger som hurtig påvirker mange samtidig, i flere forskjellige land. For politiet betyr det at arbeidspraksisen må endres og tilpasses globale trender og rekkevidder. Tidligere kunne politiet gjøre lokale og nasjonale beslutninger, men digitaliseringen av samfunnet utfordrer politiets tradisjonelle arbeidsutførelse. I oppgaven kommer det frem at det er den samme teknologien som forandrer politiet som kan hjelpe politiet. Det krever likevel en teknologisk forståelse og vilje til å omstille seg. Denne delen vil kort oppsummere hva oppgaven har gjort, trekke frem hovedfunn, mulige konsekvenser for fremtiden, samt oppgavens bidrag.

Med utgangspunkt i en fenomenologisk tilnærming utførte jeg ni kvalitative intervjuer av cyberkriminalitetsspesialister i politiet. Jeg har fått innblikk i informantenes opplevelser av egen virkelighet i møte med cyberkriminalitet. Temaene som har blitt diskutert og drøftet i analysen har blitt valgt ut på bakgrunn av hva som fremstod som viktig for informantene å få frem. Temaene ble fort delt inn under to kategorier: informantenes interne opplevelser som kunne knyttes opp mot politikulturer og deres tanker om ytre beslutninger som kunne bli belyst gjennom overordnede kontrollprosesser. Fordi cyberkriminalitet er sterkt knyttet til internetteknologi, introduserte jeg internett som et ledd i moderne samfunn som spiller inn på politiets kulturer og politiorganisasjonens styresett. I oppgaven har jeg forsøkt å knytte politikulturer med ytre kontrollprosesser for å se hvordan de korrelerer og sammen former politiets møte med cyberkriminalitet. Videre skal jeg oppsummere hva hovedresultatet ble.

Oppgavene har hatt to hovedfunn. Det ene funnet er en delt bekymring blant informantene om at internett i dag i stor grad fremstår som et lovløst rom hvor politiet ikke har

tilstrekkelig tilstedeværelse og mulighet for å skape trygghet. At politiet ikke har utarbeidet tilstrekkelig tiltak på nett som kan skape trygghet og orden, gjør at internett oppfattes som et relativt lovtomt rom, hvor politiet i liten grad er tilstede. At politiet svikter i sitt formål på internettarenaer kan få utslag i borgernes syn på deres legitimitet. Legitimitet er et velkjent aspekt i forholdet politi–borger. Politiet er avhengig av at borgerne oppfatter deres nærvær som legalt for å fungere optimalt, estisk og lovlig. Taylor (2004) mener at politiet er avhengig av borgernes støtte i samfunnet for å kunne utføre sine arbeidsoppdrag. Et fravær av frivillig erkjennelse fra borgerne, vil føre til at politiet, i sterkere grad, må henvende seg til bruk av makt. At politiet utøver makt har blitt rettferdiggjort hvis maktutøvelsen er i tråd med lovverket og verdiene i samfunnet.

I analysekapittel fire ble maktutøvelse diskutert i form av overvåking på nett. Her ble det trukket frem at staten i høyere grad innfrir bruken av overvåking til kriminalitetskontroll fordi det er vurdert som et nyttig redskap i reduseringen av fremtidig risiko. En økning i bruk av makt vil være med på å undergrave politiets mål om å samarbeide med borgerne for å opprettholde verdiene i samfunnet, skriver (Taylor, 2004). At borgerne frivillig stiller seg bak politiet og følger deres ordre, skjer når borgerne bedømmer politiets posisjon og autoritet i samfunnet som legitim. Å bli vurdert som en legitim autoritet vil være umulig å oppnå kun ved evnen til å utøve makt (Tyler, 2004). Bottoms og Tankebe (2012) skriver at det holder ikke at politiet jobber i tråd med lovverket; de må demonstrere at de har kapasiteten til å oppnå effektive resultater. Et politi som belager seg på tillitt fra borgerne gjennom bruk av makt vil kun belage seg på en instrumentellforståelse av forholdet mellom politi-borger (Bottoms og Tankebe, 2012).

Som diskutert i analysekapittel fire, strever politiet med å løse hvordan de skal utøve makt på nett, og politiet har vist lite effektivitet i møtet med cyberkriminalitet. I analysen kom det frem fra informantenes historier, at det har resultert i at private aktører har tatt over cyberkriminalitetsbekjempelsen fordi politiet ikke er tilstede på internett. På den ene siden er det ikke nødvendigvis negativt at private aktører tar på seg noen ansvarsområdet som tilhører politiet. Det kan frigjøre ressurser gjennom riktig ansvarfordeling. Blant annet kom det frem at det å pålegge de som eier problemet ansvar, vil være en effektiv måte å løse problemet på. Dette er en ganske vanlig praksis også i den fysiske verden, hvor «problemeiere» må ha et visst ansvar for sin egen trygghet (Aas, 2007). På den andre siden,

kan private aktører stort sett drive fritt og ukontrollert ut ifra egne interesser og behov. Det kan skape sosial ekskludering og stor forskjell i arbeidsutførelse. I tillegg medfører det at skillet mellom offentlige og private ansvarsområder blir visket ut; politiets rolle og funksjon blir uklar. Når politiet ikke viser effektivitet, tar private aktører over, hvilket kan føre til uetiske håndteringer. En oppblomstring av private som tar på seg oppdraget å forfølge de som bryter loven og stille dem til rett, kan se ut til å ha blitt en trend på internett. I to nyhetsartikler, kommer det frem at en privatperson og et privateid selskap, jakter og avslører pedofile på nett (Gagnes, 2016; Valum, 2007). Deres handlinger kan ses på som et motsvar til at politiet ikke gjør jobben sin på denne arenaen. Når borgerne oppfatter at politiet ikke evner å løse sine politioppdrag, mister borgerne tillitt til at politiet ordner opp. Fra nyhetsartiklene kan det tolkes dithen at det leder mot en privat kontrollspiral av borgervernspredning på internett. Det kan trekkes tilbake til diskusjoner gjort av Gundhus (2007), som skriver at når politiarbeidet er ineffektivt fører det til økt mistillit, som igjen kan lede til en oppblomstring av borgervern. Å forhindre utviklingen av borgervern av ovennevnte art, krever at politiet tydeliggjør sine offentlige oppgaver og ansvarsområder, og viser at de har kapasitet til å håndtere ting på nett. Borgere vurderer effektivitet som et normativt kriterium, som politiet skal oppfylle, og gjennom det oppnår politiet tillitt og legitimitet (Bottoms og Tankebe, 2012). For at politiet skal kunne vise at de har kapasitet til å være effektive på nett, mener blant annet informantene at politiet må øke samarbeidet internt og eksternt, politiet burde hente inn mer sivil kompetanse og endre på generalistutdannelsen. Som vist, utfordrer det verdiene som politiorganisasjonen verdsetter.

Oppgavens andre funn viser at politikulturen ikke har endret seg i takt med teknologiske og sosiale endringer. Funn fra oppgaven peker mot en ledelse som ser verdien av politiarbeidet som kroppslig og situert i det fysiske rom. Dette preger både synet på siviles rolle i politiet og synet på generalistrollen. Denne manglende utviklingen i politikulturen gjenspeiles også i politiets styringsmodeller.

Som beskrevet, har det vokst frem nye type styringsmodeller. Utviklingstrekk viser til et samfunn som er risikoorientert og utvikler styringsmodeller på bakgrunn av tanken om at risikoene i samfunnet er menneskeskapt (Aakvaag, 2008). Det virker som det kan påvirke borgernes subjektive tilnærming til samfunnet rundt seg, ved at de endrer sin måte å oppfatte og forholde seg til sin verden på (ibid.). At fokuset sentrerer rundt fare, risiko og

sikkerhet gjør at samfunnet får et veldig negativt preg (Ericson og Haggerty, 1997). Fra funn i analysekapittel fem, kommer det frem at politiske bevilgninger bestemmes ut fra fysiologisk skade. Cyberkriminalitet, som ikke syns på samme måte, vil dermed få mindre ressurser. Et samfunn, som har en kognitivt oppfattelse om å hele tiden forbereder seg på det verste, drives frem en konkurranse på levering av sikkerhetstjenester. Det ser ut til å også være gjeldende på nett. Samtidig skjer det et skifte fra staten som hovedforsørger av sikkerhet, til at individer, bedrifter og kommuner som ansvarshavende og aktiv deltaker (Zedner, 2006).

Ut fra risikostyring har det vokst frem nye arbeidspraksiser i politiet som vektlegger markedstilpasninger og forebyggende arbeid. Kunnskapsstyrt politiarbeid vektlegger proaktivt, analytisk arbeid og oppfordrer til økt samarbeid og bruk av den enkeltes spesialiserte kunnskap (Gundhus, 2007). En risikoorientert, forebyggende tilnærming skaper en spesiell form for samarbeid og fokus i politiarbeidet. En negativ effekt av dette er at politiarbeidet vil ha hovedfokus på å nå måltall, hvilket kan åpne opp for en økning i bruk av instrumentell kontroll slik som overvåkning (Gundhus, 2007). Det gjør at borgernes personvern og rettigheter står sårbart. I tillegg blir politiarbeidet tilpasset systemeffektive samarbeidsmodeller, hvor kvantitet blir viktigere enn kvalitet. En politiorganisasjonen som benytter seg av markedsadopterte styringsformer, ser da viktigheten av resultater og kostnadseffektive målsettinger. I noen av informantenes fortellinger kommer det frem et ønsker om å få på plass risiko- og markedsstyrte kontrollformer i sin arbeidspraksis, fordi det markedstilpassede fokuset fører til økt samarbeid, mer bevilgninger, vektlegger den enkeltes kompetanse og jobber fremtidsrettet. Ut ifra tolkning gjort i analysen, kan det forståes slik at informantene mener at endringen kan bidra positivt til å øke politiets effektivitet i møte med cyberkriminalitet. Samtidig vil kontrollformen være i tråd med nettverksteknologiens sentrale plass i samfunnet.

På annen side viser blant annet Gundhus (2009), at denne styringsformen overser erfaringsbaser kunnskap. I studien viser hun at det skjer en ny endring i overgangen fra operativ kunnskap, til kunnskapsbasert og fremtidsrettet arbeidspraksis. Den nye oppfattelsen nedtoner verdien av operativ og «gatekunnskap» for å gjøre politiorganisasjonen mer markedstilpasset. I beretningene til informantene virket det som deres oppfattelser stagnerer i møte med politiledelse. Politiledere bedømte verdien i politiarbeidet ut ifra arbeid som er gatenært og fysisk. Hurtige beslutninger som må tas i

akutte, farlige situasjoner gir høy status og mer bevilgninger enn analytisk «kontor»-arbeid (Gundhus, 2009). Det er tydelig at abstrakt, analytisk og teknologisk kunnskap ikke er verdsatt og motstrider med det som kan forståes som habitusen til ledere i politiorganisasjonen. At ledelsen i politiet holder på faste tradisjonelle yrkesforståelser, kan settes i sammenheng med den byråkratiske modellen i politiorganisasjonen. Byråkratisk styringsmodell verdsetter det stabile, og vil gjøre endringer i en gradvis modningsprosess. Som vist, preger det forandringer som er nødvendige for at politiet skal holde takt med teknologiske og sosiale endringer. Det skaper en spenning mellom ønsker og behov informantene ser, og styring og prioriteringer som ledelsen setter. Informantene oppfatter at politiledere ikke styrer cyberkriminalitetsavdelingene etter markedsstyrte kontrollformer, hvilket da står i kontrast til utviklingstrekk som peker på nye politipraksiser i politiet som verdsetter fremtidsrettet, analytisk og vitenskapelige arbeidsmodeller. Ut fra diskusjoner og funn kan man da dra slutningen om at det parallelt opererer to forskjellige arbeidspraksiser i politiet.

I studiens overordnede problemstilling spør jeg hva som er politispesialistenes opplevelse av politiet i møte med cyberkriminalitet i Norge. Med bakgrunn i studiens analyse fremstår politiets møte med cyberkriminalitet som kompleks. Det er vanskelig å kvantifisere cyberkriminaliteten, fordi internett tilbyr uavhengig geografisk plassering, anonymitet, økning i bruk av malware, kunstig intelligens, 3D-printere, VR-teknologi, skyløsninger, mørkenettet, kryptering, kort lagringstid for elektroniske spor, bearbeiding av store mengder data og få anmeldelser. Det er bare noen eksempler på forhold som tilrettelegger, utvider og opprettholder nye former for lovbrudd. Det fremgår av informantenes historier at informantene selv har kunnskapen til å møte cyberkriminaliteten på en håndterlig måte, men de opplever at de ikke kan stå alene. De er avhengig av at resten av politietaten og politiske utforminger følger på. Uten riktig korrelering kan det virke som både arbeidsmengde og ansvar blir for stort, hvilket resulterer i henleggelser av saker, borgervernspredning, og et politi som ikke kan møte borgerne der de er. Potensielt sett kan det endre politiets formål i samfunnet.

Som en forlengelse av hovedproblemstillingen har jeg stilt spørsmålstegn ved hvordan cyberkriminaliteten utfordrer politiets kultur. I lys av politikulturen, kommer det frem i historiene til informantene at det finnes dominerende gjentagende elementer i kulturen.

Selv om kulturen ikke er homogen, kan det virke som om det finnes et sett med kjerneverdier som verdsettes. Internetteknologiens oppblomstring de siste 25 årene, utfordrer disse verdiene og det tradisjonelle styresettet gjennom rekkevidde, hurtighet og et uklart skille mellom fysisk og virtuell identitet. Cyberkriminaliteten utfordrer de tradisjonelle verdiene ved å endre kriminalitetsbildet og sette nye krav til politiorganisasjonen. For politiet er det ikke nytt å måtte tilpasse seg nye samfunnskrav. Politiet har gjentatte ganger gått igjennom endringsprosesser, men likevel står politiorganisasjonen fortsatt stødig i sin posisjon i samfunnet. Politiet har siden sin opprinnelse, vært et symbolsk uttrykk for statlig myndighet og en viktig grunnstein for den moderne stats eksistens. Selv om fremtiden er vanskelig å forutse, kan det se ut som politiet står overfor utviklingstrekk som kan rokke på de kulturelle verdiene som organisasjonen verdsetter, og som tenkelig kan endre på politiets funksjon og rolle i samfunnet. Tall fra rapporten til NorSiS (2016) viser at snart er hele det norske samfunnet knyttet opp mot internett, hvilket gjør Norge sårbart. Som diskutert, vil et sårbart samfunn i høyere grad søke etter mer sikkerhet og mer trygghet. Et spørsmål til ettertanke vil da være hvor realistisk er det at politiet skal klare å dekke dette behovet i fremtiden.

Oppgavens bidrag

Gjennom oppgaven har jeg tilegnet meg en bredere forståelse av politiorganisasjonen og en bedre oversikt over kompleksiteten til cyberkriminalitetsfeltet. Hovedmålet til oppgaven har vært å få en forståelse for spesialistenes tanker, erfaringer og utfordringer i møte med cyberkriminalitet fordi dette er et område hvor det er lite informasjon tilgjengelig. Det finnes flere aspekter innenfor dette temaet som kan studeres, men denne oppgaven berører kun et lite utsnitt av informantenes hverdagsliv. Forhåpentligvis har oppgaven bidratt med nyttig diskusjoner om temaer som foreløpig er lite belyst både av forskere og politiet. Den har kanskje til og med bidratt til en økt forståelse av spesialistenes møte med cyberkriminalitet.

Som man kan se ut ifra drøftingene gjort i analysekapitlene, kan det være fristende å sette spørsmålstegn ved om det er en ny politikultur på vei. I alle fall, kan de se ut som endringene som må til for å møte nye arbeidsoppdrag, beveger på elementene som tradisjonelt sett har tilhørt den dominerende delen av politikulturen, slik som beskrevet i litteraturen. Oppgaven har trukket frem og spurt om litteraturen på feltet er litt for utdatert og om man må få plass til mer empirisk forskning på andre politikulturer enn gatepoliti. De studiene som er gjort er

til tider veldig begrensende når man skal prøve å forstå andre ledd i politiorganisasjonen. I tillegg vil det være fordelaktig å gjøre mer empirisk forskning på politiet i møte med cyberkriminalitet. Det er et lite studert felt, hvor man har lite kunnskap.

Antall ord: 32442.

Litteraturliste

Aakvaag, G, C., 2008.

Pierre Bourdieu: En konfliktteoretisk syntese. *Moderne Sosiologisk Teori*. 148-171. Oslo: Abstrakt Forlag.

Aas, K, F., 2013.

Globalization and Crime. London: Sage Publications.

Ablon, L. & Libicki, M., 2015.

'Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data' *Defense Counsel Journal*, 2015, Vol. 82(2)

Balvig, F., og Holmberg, L., 2004.

Politi og tryghed : forsøg med nærpoliti i Danmark. København: Jurist- og Økonomforbundets Forlag.

Beck, U., 1986.

Risk Society: Towards a New Modernity. London: Sage Publications.

Bennet, D., og Stephens, P., 2014.

Preventing Digital Crime. I: Bryant, R., og Bryant, S., 2014. *Policing Digital Crime*. England: Ashgate.

Birkeland, Å., 2007.

Politigeneralisten, den modern state og polities legitimitet.31-48. I Gundhus, O, H., Larsson, P., Myhrer, T, G., 2007. *Polisiær virksomhet: Hva er det- Hvem gjør det?.* Politihøgskolen: Oslo.

Bittner, E., 2005.

Florence Nightingale in pursuit of Willie Sutton: A theory of the police. I T. Newburn (Ed.). *Policing: Key Readings* (s.150-172). Cullompton: Willan Publishing.

Bjørkelo, B., og Gundhus, O, H., 2015.

Å forbedre en etat: Om læring gjennom eksisterende systemer i politiorganisasjonen. Fagbokforlag. Journal Magma om økonomi og ledelse. 34-46. Tilgjengelig: https://brage.bibsys.no/xmlui/bitstream/handle/11250/279578/%c3%85%20forbedre%20en%20etat.pdf?sequence=1&isAllowed=y.

Bossler, A, M. og Holt, T, J., 2012.

Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management.* Vol. 35 Issue: 1, pp.165-181.

Bourdieu, P., 1998.

Practical Reason. Cambridge: Polity Press.

Castells, M., 2001

The internet galaxy: reflections on the internet, business and society. Oxford: Oxford University Press.

Christie, N., 2000.

Kriminalitetskontroll som Industri – Mot GULAG, vestlig type. 3 utg. Oslo: Universitetsforlaget.

Christie, N., 2004.

En passende mengde kriminalitet. Oslo: Universitetsforlaget.

Corbin, J., og Strauss, A., 2015.

Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. 4th Ed. London: Sage Publications.

Crank, J. P., 2004.

Understanding Police Culture. 2nd Ed. Anderson Publishing LexisNexis Group.

Curran, J., 2010.

Reinterpreting Internet History. I: Jewkes, Y., and Yar, M. *Handbook of Internet Crime.* Ed. 17-37. Oregon: Willan Publishing.

Chan, J, B, L., 1997

Changing Police Culture: Policing in a multicultural society. Cambridge: Cambridge University Press.

Chan, J, B, L., 2001.

The Technological Game: How Information Technology is Transforming Police Practice. *Journal of Criminology and Criminal Justice*. Volume: 1 issue: 2, page(s): 139-159. Issue published: May 1, 2001

Dvergsdal, H., 2018.

Internett definisjon. *Store Norske Leksikon*. 5 januar 2018. Tilgjengelig: «https://snl.no/Internett»

Enli, G., og Aalen, I., 2017.

Sosiale medier. *Store Norske Leksikon*. 12 desember 2017. Tilgjengelig: https://snl.no/sosiale_medier

Ericsson, K., 2000.

Maskulinitet, kriminalitet og kontroll. I Bekkevad, E, L. et al. Materalisten. *Tidskrift for forskning, fagkritikk og teoretisk debatt.* 28 (4) 2000 ss. 7-43.

Ericson, R, V., og Haggerty, K., D., 1997

Policing the risk society. Oxford: Oxford UniversityPress.

Eriksen, T, H., 2007

Øyeblikkets Tyranni: Rask og langsom tid i informasjonsalderen. Oslo: Aschehoug.

Finstad, L, 2003.

Politiblikket. Norge: Pax forlag

Finstad, L., 2015.

Det konflikt fylte politiarbeidet. I: Larsson, P., Gundhus, H, O, I., Granér, R., 2015. *Innføring i Politivitenskap.* 229-254. Oslo: Cappelen Damm Akademisk

Foucault, M., 1977.

Overvåkning og straff. Gyldendal Akademisk.

Foucault, M., 1991.

Governmentality I: *The Foucault effect. Studies in govermentality.* Burchell, G., Gordon, C., Miller, P. (Red.). Chicago: Chicago University press. S. 87-104.

Fyfe, N, R., Gundhus, H, O, I. og Rønn, K, V., 2018

Moral Issues in Intelligence-Led Policing. New York: Routledge.

Gagnes, I, L., 2016.

Jakter pedofile på nett: Eirik (46) blir «Jente (14)» i chatterom på nett. *Tv2 nettavis*. 06.02.16. Tilgjengelig fra: «https://www.tv2.no/a/8000126/».

Goodman, M, D., 1997.

Why the Police Don't Care about Computer Crime. Harvard Journal of Law and Technology. 10. 465-494. I: Wall, D, S., 2003. *Cyberspace Crime*. England: Ashgate Publishing limited.

Gordon, S., og Ford, R., 2006.

On the Definition and Classification of Cybercrime. *Journal in Computer Virology*. Aug 2006. Vol 2. Issue 1. pp 13-20.

Gottschalk, P., 2011.

Datakriminalitet i Norge. Norge: Unipub.

Granér, R., 2015.

Selvstendige sheriffer eller lojale byråkrater. I: Larsson, P., Gundhus, H, O, I., Granér, R. *Innføring i Politivitenskap.* 134-152. Oslo: Cappelen Damm Akademisk

Granér, R., og Kronkvist, O., 2014.

Kontroll av og i politiorganisasjonen. 53-77. I Larsson, P., Gundhus, H, O, I., Granér, R., 2014. *Innføring i Politivitenskap.* Oslo: Cappelen Damm Akademisk

Gundhus, O, H., 2009.

For sikkerhetsskyld. IKT, yrkeskultur og kunnskapsarbeid i politiet. Universitetet i Oslo.

Gundhus O, H., Larsson, P., 2007.

Policing i norsk perspektiv s. 11-30. I: Gundhus, O, H., Larsson, P., Myhrer, T, G., 2007a. *Polisiær virksomhet: Hva er det- Hvem gjør det?* Politihøgskolen: Oslo.

Gundhus, H, O, P., 2007.

Suksesskriterier for godt politiarbeid. Nordisk Tidsskrift for Kriminalvidenskab 2007. Tilgjengelig:https://brage.bibsys.no/xmlui/bitstream/handle/11250/174582/Suksesskriterier_for_godt_politiarbeid%20Gundhus.pdf?sequence=1&isAllowed=y

Halvorsen, K., 2012.

Å forske på samfunnet: en innføring i samfunnsvitenskapelig metode. Oslo: Cappelen Akademisk Forlag.

Harvey, W, S., 2011.

Strategies for Conducting Elite Interviews. 431-441. UK: Sage Publications. Tilgjengelig : http://journals.sagepub.com/doi/pdf/10.1177/1468794111404329.

Hestehave, N, K., 2018.

Predicting crime? On challenges to the police in becoming knowledgeable organizations. I: Fyfe, N, R., Gundhus, H, O, I. og Rønn, K, V., 2018. *Moral Issues in Intelligence-Led Policing*. New York: Routledge.

Holt, T, J. og Bossler, A, M., 2012.

Police Perceptions of Computer Crimes in Two Southeastern Cities: An Examination from the Viewpoint of Patrol Officers. *American Journal of Criminal Justice.* September 2012, Volume 37, Issue 3, pp 396–412.

Holt, T. J.og Bossler, A. M. 2015.

Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offences. London: Routledge.

Jewkes, Y., 2007.

Crime Online ed. Devon: Willian Publishing.

Jewkes, Y., og Yar, M., 2010.

Handbook of Internet Crime. Ed. Oregon: Willan Publishing.

Jewkes, Y., 2010.

Public policing and Internet crimes. 525-545. I: Jewkes, Y., and Yar, M., 2010. *Handbook of Internet Crime.* Ed. Oregon: Willan Publishing.

Johannessen, S, O., 2013

Politikultur: Identitet, makt og forandring i politiet. Trondheim: Akademika forlag.

Johannessen, S, O. og Glomseth, R., 2015.

Politiledelse. Oslo: Gyldendal akademisk

Jones, T., 2012.

Governing Security: Pluralization, Privatization and Polarization in Crime Control and Policing. I : Ed. Maguire, M, Morgan, R., og Reiner, R., 2012. *The Oxford Handbook of Criminology.* 5th Ed. 743-768. Oxford: Oxford University Press.

Jørgenrud, M., 2017.

NotPetya: Mærsk tapte opptil 2,5 milliarder kroner på dataangrep. *Digi.* Tilgjengelig: https://www.digi.no/artikler/maersk-tapte-opptil-2-5-milliarder-kroner-pa-dataangrep/411585 7. November. 2017.

Kvale, S., og Brinkmann, S., 2015.

Det Kvalitative Forskningsintervju. 3. Utgave. Oslo: Gyldendal Norsk Forlag AS.

Larsson, P., Gundhus, H, O, I., Granér, R., 2015.

Innføring i Politivitenskap. Oslo: Cappelen Damm Akademisk

Leukfeldt, R., Veenstra, S., og Stol, W., 2013.

High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands. International Journal of Cyber Criminology. Vol. 7, Iss. 1, (Jan-Jun 2013): 1-17.

Lofthus, B., 2009.

Police Culture in a Changing World. Oxford: Oxford University Press.

Lomell, H, M., 2015.

Polisær virksomhet utenfor politiet. 255-272. I: Larsson, P., Gundhus, H, O, I., Granér, R., 2015. *Innføring i Politivitenskap.* Oslo: Cappelen Damm Akademisk

Loveday, B., 2017a.

Still plodding along? The police response to the changing profile of crime in England and Wales*. International Journal of Police Science & Management*. 2017, Vol. 19(2) 101–109

Loveday, B., 2017b.

The Shape of Things to Come. Reflections on the potential implications of the 2016 Office of National Statistics Crime Survey for the police service of England and Wales. *Policing: A Journal of Policy and Practice.* 1-12. Tilgjengelig: https://academic.oup.com/policing/advance article/doi/10.1093/police/pax040/4058199

Lyon, D., 2006.

9/11 synopticon and scopohilia: Watching and being watched. (35-54). I: Ericson, R, V., Haggerty, K, D., 2016. *The new politics of surveillance and visibility* Toronto: University of Toronto Press.

Lysne, Olav, Grytting, Trond, Jarbekk, Eva, Lunde, Einar og Reusch, Christian., 2016.

Digitalt grenseforsvar (DGF): *Lysne II-utvalget.* Tilgjenglig: https://www.regjeringen.no/contentassets/ca1f705dbebd48cb9a61889d4cfee6bf/digitalt-grenseforsvar-lysne-ii-utvalget.pdf

Manning, P, K., 1992.

Information Technologies and the Police. *Crime and Justice.* Vol 15. 349-398.

Manning, P, K., 2008.

The technology of policing- Crime mapping, Information technology, and the rational of crime control. New York: New York University Press.

Matthews, B., og Ross, L., 2010.

Research methods: a practical guide for the social sciences. England: Pearson Education Limited.

Mathiesen, T., 1997.

The Viewers Society: Michel Foucault's 'Panopticon' Revisited. *Theoretical Criminology.* Vol 1(2):215-234. London: Sage Publications.

McQuade, S., 2006.

Technology-enabled crime, policing, and security. *Journal of Technology studies.* 33-42.

Myhrer, T, G., 2015.

Politiretten-samfunnsbeskyttelse og rettssikkerhet. I: Larsson, P., Gundhus, H, O, I., Granér, R. *Innføring i Politivitenskap. S*. 79-109. Oslo: Cappelen Damm Akademisk

Nasjonal sikkerhetsmyndighet., 2018.

NSM årlige risikorapport. 2018. Tilgjengelig: https://nsm.stat.no/publikasjoner/rapporter/rapport-om-sikkerhetstilstanden/.

Norsk senter for Informasjonssikring (NorSIS)., 2017.

Nordmenn og digital sikkerhetskultur. Rapport tilgjengelig: «https://norsis.no/wp-content/uploads/2017/11/Nordmenn-og-digital-sikkerhetskultur-2017.pdf»

Norges Politi Lederlag., 2016

Politiets strategi mot 2025. Tilgjengelig: «*https://www.politilederen.no/64-nyheter/1579-politiets-strategi-mot-2025»* .Publisert 21 november 2016.

NOU: 2012:14.

Rapporten fra 22.juli kommisjonen. Tilgjengelig: https://www.regjeringen.no/no/dokumenter/nou-2012-14/id697260/.

Newburn, T., 2013.

Criminology. 2nd Ed. London: London: Routledge.

Næringslivets sikkerhetsråd., 2016.

Mørketall. Tilgjengelig: https://www.nsr-org.no/moerketall/ .

Politidirektoratet, 2012.

Politiet i det digitale samfunnet. En arbeidsgruppe rapport om elektroniske spor, IKT kriminalitet, politiarbeid på internett. Tilgjengelig:

https://medlem.ntl.no/Content/103500/cache=20122109105334/Politiet%20i%20det%20digitale%20samfunn%20juli%2012.pdf.

Politidirektoratet., 2015.

Datakrimstrategi. Tilgjengelig: https://www.regjeringen.no/contentassets/4d2ba37bf2ae4cc9ac39afdf20a2f41b/datakrimstrategi_2015.pdf.

Politidirektoratet, 2015-2017.

Pilotprosjektet. Delrapport.

Politihøgskolen., 2018.

Høringssvar – Rapporten om kapasitet –og kompetansebehov i politiet dei kommende tiårene. Tilgjengelig: https://www.phs.no/Documents/1_Om%20PHS/H%c3%b8ringssvar/H%c3%b8ringssvar%20-%20rapport%20om%20kapasitet-%20og%20kompetansebehovet%20i%20politiet%20de%20kommende%20ti%c3%a5rene.pdf. 22.03.2018.

Politiloven., 1995.

LOV-1995-08-04-53. Tilgjengelig: «https://lovdata.no/dokument/NL/lov/1995-08-04-53»

Politiets sikkerhets tjeneste., 2018.

Trusselvurdering. Tilgjengelig: «https://pst.no/alle-artikler/trusselvurderinger/annual-threat-assessment-2018/

Prop. 61 LS., 2014-2015.

Endringer i politiloven mv. (trygghet i hverdagen – nærpolitireformen). Oslo: Justis- og beredskapsdepartementet. Tilgjengelig: https://www.regjeringen.no/no/dokumenter/prop.-61-s-2014-2015/id2398784/

Reiner, R., 2010.

Politics of the police. 4th Ed. Oxford: Oxford University Press.

Reisig, M, D. og Kane, R, J., 2014.

Police legitimacy. I *The Oxfordhandbook of police and policing Ed.* Tilgjengelig: http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199843886.001.0001/oxfordhb-9780199843886-e-017?print=pdf

Reus-Ianni, E., 1993.

Two cultures of policing: Street cops and management cops. New Brunswick: Transaction Publishers.

Richards, N, M., 2013.

The Dangers of Surveillance. *Harvard Law Review* .Vol. 126, No. 7 (MAY 2013). 1934-1965 . Tilgjengelig: http://www.jstor.org/stable/23415062?seq=2#page_scan_tab_contents

Ryen, A., 2002.

Det kvalitative intervjuet: Fra vitenskapsteori til feltarbeid. Bergen: Fagbokforlaget.

Schein, E. H., 2010.

Organizational Culture and Leadership. 4th Ed. United States of America: Wiley Imprint.

Schølberg, S., 2017.

Cyberkriminalitet. Oslo: Universitetsforlaget

Shearing, C., og Wood, J., 2001.

Nodal Governance, Democracy, and the New `Denizens'. *Journal of Law and Society*. Vol 30. No 3. 400-419.

Skolnick, J., 1966.

Justice without a Trial: Law enforcement in democratic society. New York: Wiley.

Skolnick, J., 2005.

A sketch of the policeman's 'working personality'. I: T. Newburn (Ed.) *Policing: Key Readings* s.150-172. Cullompton: Willan Publishing.

Senjo, S., 2004.

An Analysis of Computer-related Crime: Comparing Police Officer Perceptions with Empirical Data. *Security Journal.* April 2004, Volume 17, Issue 2, pp 55–71. Tilgjengelig: https://link.springer.com/article/10.1057/palgrave.sj.8340168 .

St.meld. nr. 42., 2004-2005.

Politiets rolle og oppgaver. Oslo: Justis og beredskapsdepartementet. Tilgjengelig: https://www.regjeringen.no/no/dokumenter/stmeld-nr-42-2004-2005-/id199239/

Sunde, I, M., 2016a.

Datakriminalitet: En fremstilling av strafferettslige regler om datakriminalitet. Bergen. Fagbokforlaget.

Sunde, I. M. 2016b.

A new thing under the sun? Crime in the digitized society. I A. Kinnunen (Ed.), *NSfK's 58. Research Seminar: New challenges in criminology: Can old theories be used to explain or understand new crimes?* (p. 60-79). Bifröst: Scandinavian Research Counsil for Criminology. Tilgjengelig: https://brage.bibsys.no/xmlui/handle/11250/2418829.

Thagaard, T., 2013.

Systematikk og innlevelse: En innføring i kvalitativ metode. 4 utg. Oslo: Fagbokforlaget.

Thomas, D., og Loader, B, D., 2000.

Cybercrime: Law enforcement, security and surveillance in the information age. Ed. London: Routledge.

Trædal, T., 2017a.

Politiet i andre land satser på nasjonalt cybersenter. Her hjemme frykter flere at norsk politi sakker akterut på nett*. Politiforum*. 26 juni 2017. Tilgjengelig: http://dybde.politiforum.no/nc3.html

Trædal, T, J., 2017b

Nå får politiet sitt «NC3» - et eget senter for cyberkriminalitet. *Politiforum.* Tilgjengelig: «https://www.politiforum.no/artikler/na-far-politiet-sitt-nc3-et-eget-senter-for-cyberkriminalitet/412189». 16 nov 2017.

Tyler, T, R., 2004.

Enchancing police legitimacy. *The annals of American academy of political and social science.* Vol 593, Issue 1, 2004. Tilgjengelig: http://journals.sagepub.com/doi/pdf/10.1177/0002716203262627.

Valum, S., 2007.

Avslører pedofile på nett. Politiforum. 18 januar 2007. Tilgjengelig fra: https://www.politiforum.no/artikler/avslorer-pedofile-pa-nett/383604.

Waddington, P. A. J. 1999.

Police (canteen) sub-culture. An appreciation. *British Journal of Criminology*, 39 (2), s. 287-309.

Waldron, J, J., 2006.

Safety and Security. *Nebraska Law Review*. Vol 85, Issue 2. Article 5. 455-495.

Wall, D., 2001.

Crime and the Internet. Ed. London: Routledge.

Wall, D., 2003

Cyberspace Crime. Ed. Burlington: Ashgate og Dartmouth Publishing.

Wall, D., 2007.

Cybercrime: The Transformation of Crime in the Information Age. United Kingdom: Polity Press.

Wall, D., 2017.

Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing (July 20, 2017). *Centre for Criminal Justice Studies.* University of Leeds: UK. Tilgjengelig: http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199680832.001.0001/oxfordhb-9780199680832-e-65.

Wall, D. and Williams, M, L., 2013.

Policing cybercrime: networked and social media technologies and the challenges for policing. *Policing and Society* Vol. 23, Issue. 4, 2013. Tilgjengelig: https://www.tandfonline.com/doi/full/10.1080/10439463.2013.780222.

Westmarland, L., 2001.

Gender and policing: Sex, power and police culture. Cullompton: Willan publishing.

Workman-Stark A.L., 2017.

Understanding Police Culture. In: *Inclusive Policing from the Inside Out.* Advanced Sciences and Technologies for Security Applications. Springer, Cham. pp 19-35.

Yar, M., 2013.

Cybercrime and Society. 2nd Ed. London: Sage publications.

Zedner, L., 2003.

Too much security? *International Journal of the Sociology of Law.* Vol 31, Issue 3. Sep 2003. 155-184. Tilgjengelig fra: https://www.sciencedirect.com/science/article/pii/S0194659503000388

Zedner, L., 2006.

Policing before and after the police. *British Journal of Criminology*. 46 (1): 78-96. Tilgjengelig fra: https://academic.oup.com/bjc/article/46/1/78/430336

Zedner, L., og Ashworth, A., 2014.

Introduction/Historical origin of the preventive state. *Preventive Justice*. 1-50. Oxford: Oxford University Press.

Vedlegg

Vedlegg 1

Katja Franko
Institutt for kriminologi og rettssosiologi Universitetet i Oslo
Postboks 6706 St. Olavs plass
0130 OSLO

Vår dato: 29.05.2017 Vår ref: 54259 / 3 / BGH Deres dato: Deres ref:

TILBAKEMELDING PÅ MELDING OM BEHANDLING AV PERSONOPPLYSNINGER

Vi viser til melding om behandling av personopplysninger, mottatt 28.04.2017. Meldingen gjelder prosjektet:

54259	*Digitalisert politiarbeid: Hvilken rolle tenker politiet ha på nett i fremtiden? Vil kompetanseheving og nye ressursser være med på å påvirke den rollen?*
Behandlingsansvarlig	*Universitetet i Oslo, ved institusjonens øverste leder*
Daglig ansvarlig	*Katja Franko*
Student	*June Nerlien*

Personvernombudet har vurdert prosjektet og finner at behandlingen av personopplysninger er meldepliktig i henhold til personopplysningsloven § 31. Behandlingen tilfredsstiller kravene i personopplysningsloven.

Personvernombudets vurdering forutsetter at prosjektet gjennomføres i tråd med opplysningene gitt i meldeskjemaet, korrespondanse med ombudet, ombudets kommentarer samt personopplysningsloven og helseregisterloven med forskrifter. Behandlingen av personopplysninger kan settes i gang.

Det gjøres oppmerksom på at det skal gis ny melding dersom behandlingen endres i forhold til de opplysninger som ligger til grunn for personvernombudets vurdering. Endringsmeldinger gis via et eget skjema, http://www.nsd.uib.no/personvernombud/meld_prosjekt/meld_endringer.html. Det skal også gis melding etter tre år dersom prosjektet fortsatt pågår. Meldinger skal skje skriftlig til ombudet.

Personvernombudet har lagt ut opplysninger om prosjektet i en offentlig database, http://pvo.nsd.no/prosjekt.

Personvernombudet vil ved prosjektets avslutning, 31.07.2018, rette en henvendelse angående status for behandlingen av personopplysninger.

Vennlig hilsen

Kjersti Haugstvedt

Belinda Gloppen Helle

Dokumentet er elektronisk produsert og godkjent ved NSDs rutiner for elektronisk godkjenning.

Vedlegg 2

Forespørsel om deltakelse i forskningsprosjekt

Tema: «Hvilken rolle ser politiet for seg å ha på nett i fremtiden?»

Hei, mitt navn er June Nerlien.
Jeg er masterstudent på Instituttet for kriminologi og rettssosiologi på Universitet i Oslo. Jeg holder på med en avsluttende masteroppgave som handler om digitalt politiarbeid og hvilken rolle politiet ser for seg å ha på nett i fremtiden. Jeg ønsker i den forbindelse å intervjue personer i politietaten som har kunnskap om dette feltet.

Bakgrunn og formål

Formålet med studiet er å belyse temaet fra politiets egne perspektiver, få frem deres erfaringer, opplevelser og skape en bredere forståelse av avhandlingens problemstilling. Grunnet den hurtige utviklingen på nett ser man at politiet i Norge, per i dag, har store kunnskapsgap vedrørende teknologi og datakriminalitetsbekjempelse og det kreves en større avklaring om rolle og ansvarsfordeling. Nå som politiet selv er inne i en forandringsfase og selv jobber aktivt med å kartlegge sin egen kompetanse, er det ønskelig å gjøre en empirisk undersøkelse av denne utviklingen. Ved å gjøre kvalitativintervjuanalyse med personer som jobber i politietaten så vil målet til oppgavene være å få en dypere forståelse av hvilken posisjon politiet har på nett i dag, hvordan de ser for seg sin rolle på nett i fremtiden og forstå bedre aktørene som jobber med datakriminalitet daglig. De personene som blir spurt om å delta i dette studiet har blitt valgt ut på bakgrunn av deres kompetanse og arbeidsplass som sees på som relevant for studiet.

Hva innebærer deltakelse i studien?

Ved å delta i studiet vil deltagere bli deltagende i et 1:1 intervjuet og spurt 15-20 spørsmål om deres fagbakgrunn, kompetanseutfordringer, framtidsutsikter og hvor fremtredende og avgjørende deres arbeid er i forhold til kriminalitet som begås på nett i dag. Det vil ikke bli spurt spørsmål om sensitiv informasjon og det vil heller ikke bli stilt spørsmål som bryter med taushetsplikt. Som forsker er jeg mer interessert i temaet enn eksempler på saksnivå.

Intervjuet vil bli tatt opp på båndopptaker og det vil også bli skrevet notater underveis i intervjuet. Selve intervjuet vil ta ca 1- 1 og halv time.

Hva skjer med informasjonen om deg?

Alle personopplysninger vil bli behandlet konfidensielt og deltagere vil bli anonymisert. Alt av sensitivt materiale vil bli lagret på en slik måte at det ivaretar personvern og det vil kun være jeg som forsker som vil ha tilgang til datamaterialet. Det vil bli opprettet en koblingsnøkkel som erstatte navn, personnummer, e-epostadresse eller andre personentydige kjennetegn i et datasett med en kode/nummer som viser til en atskilt liste der hver kode/nummer viser til navn. Koblingsnøkkelen vil bli oppbevart separat fra selve datamaterialet for å sikre at utenforstående ikke får tilgang til koblingen mellom navn og kode. Datamaterialet vil bli håndtert på en slik måte at deltakere ikke vil bli gjenkjent i en publikasjon. Prosjektet skal etter planen avsluttes i juni 2018. Ved prosjektslutt vil datamaterialet og personopplysninger slettes.

Frivillig deltakelse

Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Dersom du trekker deg, vil alle opplysninger om deg bli anonymisert og slettet.

Dersom du ønsker å delta eller har spørsmål til studien, ta kontakt med:

Forsker June Nerlien:

Mail: june.nerlien@student.jus.uio.no.

Tlf: 97023265

Veileder Katja Franko:

katja.franko@jus.uio.no

Studien er godkjent av Personvernombudet for forskning, NSD - Norsk senter for forskningsdata AS.

Vedlegg 3

Intervjuguide

Del 1 – Kompetanse

1. Kan du begynne med å fortelle litt om din kompetanse og fagbakgrunn?
2. Kan du kort beskrive en vanlig arbeidsdag.
3. Hvilken kompetanse og fagbakgrunn har dere og hvilke er det behov for?

Del 2 – Politiet på nett

4. Hvordan vil du beskrive kunnskapen politiet i Norge har i dag om cyber/data/kriminalitet?
5. I hvilken grad vil du si at politiet spiller en viktig rolle på nett i dag? *Evt i hvilken grad er det behov for en forandring?*
6. I hvilken grad vil du si at folket, bedrifter har tillit til politiets arbeid på internett i dag?
7. I hvilken grad påvirker deres arbeid av private aktører som tilbyr lignende tjenester?
8. Hvis man tar bakgrunn i strategiplaner og rapporter som har blitt publisert de siste årene så ser det ut til at politiet planlegger å styrke kapasiteten og kompetansen i politiet på datakriminalitet og internett i politiarbeidet i Norge, hva slags tanker har du om det?
9. Hva slags dilemmaer tenker du kan oppstå når politiet tar i bruk ny teknologi og nye arbeidsmåter?
10. Hvilken rolle ser du for deg at politiet har på nett i 2025?
11. Hvilke tanker har du om NC3?