UiT
NORGES ARKTISKE UNIVERSITET

Fakultet for humaniora, samfunnsvitenskap og lærerutdanning

Institutt for språk og kultur

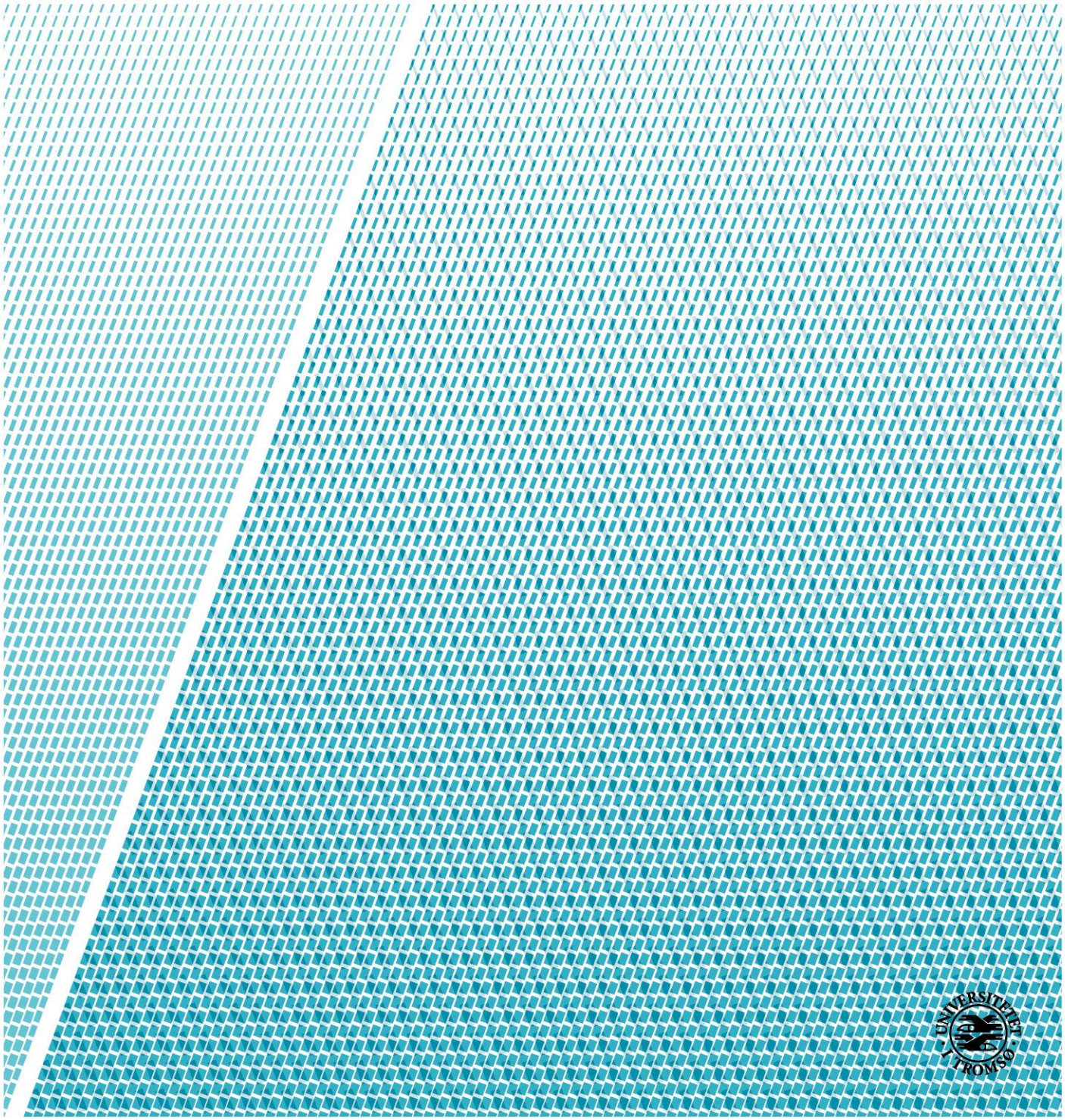
Norsk petroleumssektor i cyberspace

Materialitet, digitalisering og sikkerhet

—

Elizaveta Sergejevna Amundsen

MDV-3950 Mastergradsoppgave i medie- og dokumentasjonsvitenskap, mai 2018



Sammendrag

Den hyppige teknologiutviklingen har medført at risikobildet i samfunnet og verden for øvrig har endret seg. Norge, som et lite, men veldig digitalisert land møter de digitale utfordringene tidlig og er mer utsatt for truslene i cyberspace. For å klare å forebygge angrep fra det digitale rom, er det nødvendig å ha en god sikkerhetspolitikk, også i det digitale domenet. Sikkerhet handler om å verne om sentrale verdier. En av disse er nasjonens petroleumsvirksomhet. Olje- og gassindustrien i Norge har lenge bidratt til høy velferd, levestandard og økonomi. Stuxnet-ormen som skadet industrielle prosesser i det iranske atomprogrammet i 2010 kan sies å ha vært en tankevekker hva angår cyberangrep mot kritisk infrastruktur de siste årene. Det er ikke usannsynlig at et lignende angrep kan ta sted på norsk jord, rettet mot en eller flere olje- og gassinstallasjoner. I min avhandling utforsker jeg måtene petroleumssektoren er sikret på i Norge, med et spesielt fokus på materialitet. Målet er å få et bedre innblikk i hvordan avhengigheten av digitale løsninger har endret trusselbildet innad olje- og gassektoren, hvordan materielle aspekter av næringen kan bli rammet av angrep fra det digitale rom, og hvordan relevant myndighetspersonell og sikkerhetsaktører vektlegger disse angrepene i det forebyggende sikkerhetsarbeidet i petroleumsvirksomheten.

Forord

Takk til min veileder, Holger Pötzsch, som har hjulpet og oppmuntret meg hele veien i løpet av skriveprosessen.

Takk til de som har svart når jeg har spurt, enten det har angått data, olja eller statsforvaltninga.

Takk til min trofaste MDV-klasse – It's been real.

Takk til mamma som har vært en forståelsesfull pådriver til tross for å ikke fullt forstå hva jeg skriver om.

Forkortelser

APT	Advanced persistent threat
BYOD	Bring your own device
CCDCOE	(NATO) Cooperative Cyber Defence Centre of Excellence
CCIS	Center for Cyber and Information Security
CERT	Computer Emergency Response Team
CNI	Critical national infrastructure
CSIRT	Computer Security Incident Response Team
DGF	Digitalt grenseforsvar
DKS	Driftskontrollsystem
DoS	Denial of service
DP	Dynamisk posisjonering
DSB	Direktoratet for samfunnssikkerhet og beredskap
E-tjenesten	Etterretningstjenesten
FD	Forsvarsdepartementet
GNSS	Global Navigation Satellite System
ICS	Industrial control system
IKT	Informasjons- og kommunikasjonsteknologi
IO	Integrerte operasjoner
IT	Informasjonsteknologi
JD	Justis- og beredskapsdepartementet
NOROG	Norsk olje og gass
NOU	Norges offentlige utredninger
NSM	Nasjonal sikkerhetsmyndighet
NUPI	Norsk Utenrikspolitisk Institutt
NVE	Norges vassdrags- og energidirektorat
OD	Oljedirektoratet
OED	Olje- og energidepartementet
OT	Operasjonsteknologi
PISAS	Petroleum Industry Security Alert System
PST	Politiets sikkerhetstjeneste

Ptil	Petroleumstilsynet
RMA	Revolution in military affairs
SCADA	Supervisory Control and Data Acquisition
VDI	Varslingssystem for digital infrastruktur

Innhold

This is one for the good days
And I have it all here
In red, blue, green
Red, blue, green

– Radiohead, «Videotape»

1 – Introduksjon

Teknologi er til stede i stadig flere sfærer av livene våre, og bidrar til å både forenkle dem og utfordre dem. Internettet og samfunnets økte digitalisering er tveeggede sverd som på den ene siden bringer personer, kulturer og kunnskap nærmere hverandre, for eksempel ved hjelp av kommunikasjonsteknologi og sosiale medier, mens på den andre siden øker risikoen for at denne teknologien kan bli utnyttet for negative formål, for eksempel ved spredning av propaganda og falske nyheter.

Cyberspace er gjerne ordet som benyttes når vi snakker om hendelser som forekommer i det digitale rom. I Forsvarsdepartementets dokument *FDs cyberretningslinjer* brukes begrepet «cyberdomenet» med følgende definisjon: «Fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedia og data» (2014:5). Daniel Ventre, på sin side, mener at cyberspace må defineres som en femte dimensjon – i tillegg til de eksisterende land, sjø, luft og verdensrom. Cyberspace krysser alle de foregående domenene, og muliggjør dermed nærmest all menneskelig aktivitet i dagens teknologiske verden (Ventre 2013). Scott J. Shackelford, derimot, påpeker at ingen har lyktes med å frembringe en fullstendig og enstemmig definisjon av cyberspace til tross for iherdige forsøk. En grunn til dette er domenets løpende utvikling og endring i tillegg til en ignorering av cyberdomenets viktigste livsbetingelse, nemlig brukerne (Shackelford 2014).

Cyberspace er et bredt, åpent og stort plan med mange faktorer som er vanskelig å kapsle inn i én enkel beskrivelse. En konkret og allment akseptert definisjon av konseptet har altså enda til gode å se dagens lys. To fellesnevnere har likevel gått igjen i mange statlige konseptualiseringer av cyberspace: Cyberspace er et globalt nettverk av fysiske bestanddeler og materiale (*hardware*); og cyberspace er et informasjonsdomene som ofte blir utsatt for forsøk på overtakelse og kontroll av diverse cyberkrefter (Shackelford 2014). Disse to fellesnevnerne vil også være grunnlaget for hvordan jeg velger å definere cyberspace i tillegg til Ventres representasjon av cyberspace som et plan bestående av tre lag. Det første, L1, er et fysisk lag som omfatter materiale som kabler, nettverk, datamaskiner, satellitter og lignende. Det andre laget, L2, er applikasjonslaget og består av programvare, kode, protokoller og data. Det siste laget, L3, kaller Ventre for kognisjonslaget. Her kan potensielle cyberangrep for eksempel involvere en destabilisering av L2, manipulasjon av nettsider, spredning av konfidensiell og falsk informasjon, propaganda og lignende (Ventre 2013). L3 kan altså sies å

være et mer «abstrakt» lag der følelser og tanker til brukerne produseres og modifiseres på både godt og vondt.

På et så stort og åpent felt som cyberspace er det dermed også behov for sikkerhet. Historisk og politisk sett, har sikkerhet krigssentrerte konnotasjoner: Staten skulle beskyttes mot ytre fiender med hvilke midler som helst. Statens overlevelse var det eneste aksepterte utfallet i enhver væpnet konflikt. Med denne seieren, kom også status og makt. Om vi tar avstand fra den maktdominerende definisjonen av sikkerhet, kan vi i generelle ordelag beskrive sikkerhet som beskyttelse av et samfunns viktigste verdier. Hvilke verdier det dreier seg om, er det samfunnet selv som er nødt til å definere. En stor del av dette arbeidet er å se ting i sammenheng, og å forstå at mange av samfunnssfærene rundt oss er avhengig av hverandre, og at en trussel på ett plan, kan være en minst like stor trussel på flere.

Sikkerhet i dag består av mange kategorier, herunder også *cybersikkerhet*. Senter for Cyber- og Informasjonssikkerhet (CCIS – Center for Cyber and Information Security) definerer cybersikkerhet som en «[…] *sikring av ting som er sårbare* via IKT» (NTNU CCIS, årstall ikke angitt) det vil si en beskyttelse av de informasjons- og kommunikasjonsteknologiske datasystemer som styrer fysiske mekanismer, maskiner og industri. Cybersikkerhet, ifølge denne definisjonen, handler altså om *materialiteten* til de teknologiske funksjonene rundt oss. En sårbarhet i et IKT-nettverk som styrer viktige samfunnskritiske funksjoner kan skape betydelige ødeleggelser – også på andre samfunnsplan i tillegg til det teknologiske. Denne sårbarheten kan enten forekomme som følge av et uhell eller en tilsiktet handling i form av et *cyberangrep*. Cyberangrep kan, ifølge Shackelford, forstyrre kritiske nettverk, ødelegge militære kommando- eller informasjonssystemer, og forårsake brudd i elektrisitetstilførselen eller i finansielle tjenester. I verste fall kan et cyberangrep ha så store og fatale konsekvenser, at samfunnet mister tilgang til grunnleggende goder, og som et resultat av tapet; begynner å ødelegge seg selv. Et slikt scenario kan få oss til å trekke linjer til en postapokalyptisk verden, hvor internettet, mediene og den generelle teknologien har degradert til et ikke-eksisterende nivå, og menneskeheten har blitt slynget flere århundre tilbake i tid, forvirret, forvitret og fortapt. Et cyberangrep av slike proporsjoner er lite sannsynlig, men som Shackelford sier: «[…] it does not take a doomsday attack to raise flags» (Shackelford 2014:xix).

På grunn av dette, er fokuset i denne oppgaven nettopp cybersikkerhet. Ettersom det i seg selv er et bredt begrep, er fokuset snevret inn til å omhandle cybersikkerhet fra et norsk, industrielt perspektiv. Historien har vist at cyberangrep har vært grunnen til mange negative

konsekvenser i mangfoldige land, og Norge er intet unntak. Som et lite, men veldig digitalisert land, er vi spesielt utsatt for digitale sårbarheter, og møter disse utfordringene tidlig (IKT-sikkerhet 2017). Vi har allerede fått kjenne på hvilke trusler som ulmer i cyberspace: Nasjonal sikkerhetsmyndighet (NSM) skriver i sin risikoanalyse for 2017 blant annet at det har vært «[…] en rekke datanettverksoperasjoner rettet mot statlig forvaltning; blant annet gjennom forsøk på digital spionasje både mot departementer og underliggende etater» (Risiko 2017 2017:18) det siste året, altså 2016. Miljøpartiet De Grønne og Sosialistisk Venstreparti opplevde innbrudd i sine nettverk. Arbeiderpartiet og Stortinget var utsatt for et forsøk på det samme (Risiko 2017 2017).

Cyberspionasje, -kriminalitet, og -terrorisme er alle potensielle farer som samtlige hjørner av norsk samfunnsliv er utsatt for. Et av disse hjørnene er petroleumsvirksomheten. Denne industrien har bidratt til å sette lille Norge på kartet og gjort oss til et av verdens rikeste land. Norges olje- og gassinstallasjoner er betydningsfulle faktorer som bestemmer vår posisjon på den internasjonale arena samt vår egen velferd, økonomi og levestandard. Akkurat som et væpnet angrep eller et terroranslag, kan digitale trusler forårsake stor skade på kritisk infrastruktur, og petroleumsvirksomheten er sannsynligvis bare et ytterligere mål for *hackere*, det være seg med organisatorisk, sivil eller statlig bakgrunn. Det kan sågar se ut til at målrettede cyberangrep peker i retning av våre olje- og gassinstallasjoner: «Norske etterretningsmyndigheter advarer om en økning i digitale trusler rettet mot norsk industri. Hendelser de siste årene viser at energi- og petroleumssektoren er blant de mest utsatte» (Digitale Sårbarheter Olje & Gass 2015:1).

Sitatet ovenfor viser en presserende nødvendighet for å granske norsk petroleumsindustri nærmere i tilknytning til cyberspace og truslene det fører med seg. Vi snakker ofte om IKT-sikkerhet, noe som er utvilsomt viktig, men mitt hovedanliggende er ikke å rette oppmerksomheten mot informasjonen, opplysningene og dataene lagret i olje- og gassindustriens databaser, men heller mot de håndterlige bestanddelene som databasene og andre systemer er implementert i. Det er det materielle laget (L1), i samspill med det kodede laget (L2) av cyberspace, som står i sentrum. Mitt mål er å redegjøre for hvor stor funksjon internett og digitalisering egentlig har i norsk olje- og gassindustri samt hvordan disse funksjonene blir sikret av relevante instanser, og hvorvidt denne sikringen kan sies å være tilstrekkelig. Jeg ønsker å tydeliggjøre viktigheten av cybersikkerhet, ikke bare når det angår «myke» mål som personopplysninger eller gradert informasjon, men især når det dreier seg om samfunnskritiske funksjoner som – ved et alvorlig nok digitalt angrep – har potensiale til å

ødelegge ikke bare samfunnsstrukturen, men miljøet, målets omdømme, nasjonens økonomi og i verste fall; menneskeliv. På bakgrunn av det ovennevnte er avhandlingens sentrale problemstilling som følger:

«Hvordan blir petroleumsrelatert infrastruktur omtalt og sikret av nasjonale myndighetsaktører i rammen av cyberspace?»

Interessante momenter jeg vil strebe etter å belyse er blant annet den digitale sikkerhetskulturen i norsk olje- og gassektor i henhold til responsmiljøer, varsling om truende angrep, sikkerhetsinstanser med mer; hvordan ansvaret for cybersikkerheten i Norge er fordelt på myndighetsinstansene; hvilken posisjon olje- og gassinstallasjonene har i henhold til definisjonen «kritisk nasjonal infrastruktur»; hvordan en rekke dokumenter fra relevante instanser omtaler cybersikkerhet i det norske samfunn og især i tilknytning til petroleumsindustrien; og hvilke trusler det materielle laget av cyberspace kan rammes av samt potensielle konsekvenser av dette.

Som tidligere nevnt, ønsker jeg å holde fokus på cyberangrep som kan ha konsekvenser for den fysiske infrastrukturen som olje- og gassvirksomheten er avhengig av. Bakgrunnen for valget av et slikt hovedpunkt er flerfoldig. For det første håper jeg at det kan bidra til et originalt og friskt blikk på sammenføringen av *case* og teoriene som omhandler *the Copenhagen School* sitt utvidede sikkerhetsbegrep på den statsvitenskapelige siden samt medie- og nettverksarkeologi på det medievitenskapelige plan. For det andre er det ikke ukjent at cyberangrep med fysisk infrastruktur som mål har tatt sted tidligere, blant annet med den velkjente Stuxnet-ormen som manipulerte industrielle prosesser i det iranske atomprogrammet i 2010, og et lignende angrep på et tysk stålverk i 2014 der *hackere* manipulerte kontrollsystemene til den grad at det resulterte i massiv materiell ødeleggelse (Stouffer mfl. 2015). Ettersom verden har vært vitne til slike angrep tidligere, gir det oss desto større grunn til å forske på denne problematikken, og lære av tidligere hendelser. For det tredje sier norske myndigheter selv at fokuset for lenge har ligget på standard IKT-sikkerhet, mens digitale trusler innen industri ikke har vært omtalt i like stor grad: «Mens digitale sårbarheter har vært viet stor oppmerksomhet innen tradisjonell informasjons- og kommunikasjonsteknologi, har vektleggingen av slike sårbarheter innen prosess- og industrisektoren kommet det siste tiåret» (Digital sårbarhet - sikkert samfunn 2015:146).

Denne avhandlingen består videre av tre hoveddeler: Den første omhandler teorigrunnlaget som oppgavens tematikk og problemstilling er basert på. Den andre presenterer de metodiske fremgangsmåtene og empirien som har blitt generert i løpet av forskningsperioden. I siste hoveddel foretar jeg en nærmere presentasjon og drøfting av funnene knyttet opp mot det som har blitt kartlagt i de to foregående kapitlene. Avhandlingen avsluttes med en konklusjon hvor hovedinnholdet blir oppsummert.

2 – Teoretisk bakgrunn

2.1 – Innledning

I henhold til oppgavens problemstilling samt tilhørende forskningsspørsmål og metodisk bakgrunn, har to teoretiske tilnærminger blitt utvalgt med det formål å belyse dette. Disse er: Konseptet om et utvidet sikkerhetsbegrep og mediearkeologi.

Fokuset i oppgaven er på mange måter todelt – på den ene siden finner vi statsvitenskap med tilknytning til politiske prosesser, prosedyrer, regelverk og myndighet, mens på den andre siden ligger medievitenskap og dens digitale attributter, teknologi, *cyber* og internett. Grunnen for valg av teori er et ønske om å sammenfatte disse to disiplinene på et mer spesifikt og forhåpentligvis; et mer innovativt plan ved å se på sikkerhetspolitikk og mediearkeologi under ett.

Området som teorien spesielt og oppgaven i helhet sentrerer rundt er petroleumsrelatert infrastruktur i Norge. «Infrastruktur» er et viktig begrep her ettersom det peker på noe materielt, og det er nettopp det materielle aspektet av cyberdomenet som interesserer mest i avhandlingens kontekst. Mediearkeologi er et bredt felt som involverer mange perspektiver, tilnærminger og fokuspunkt. Et av teoriretningens viktigste aspekt er teknologiens materialitet. Et annet er ønsket om å belyse mediene og teknologiutviklingen fra andre vinkler enn det som tradisjonelt sett har vært vanligst. Mediearkeologi blir dermed et nyttig verktøy når vi skal analysere både den fysiske infrastrukturen som petroleumsnæringen er avhengig av, og selve cyberdomenets opphav og utvikling. En underkategori i dette perspektivet er nettverksarkeologi som ikke bare tar for seg de fysiske delene av vår teknologi, men også de koblinger og sammenhenger som har sørget, og fortsatt sørger for, at en slik teknologi er mulig.

Det utvidede sikkerhetsbegrepet er ment å særlig belyse hvordan cybersikkerhet har blitt en naturlig del av sikkerhetsdebatten i likhet med væpnet krig, militær maktbruk og masseødeleggelsesvåpen. Det utvidede sikkerhetsbegrepet stammer fra *the Copenhagen School* eller Københavnerskolen på norsk, og omfatter konseptet om en «[…] wider security agenda […]» (Buzan, Wæver og de Wilde 1998:7). En bredere sikkerhetsagenda fordrer en omfavnelse av flere sektorer i tillegg til den militære med et mål om å belyse hvordan eksistensielle trusler kan være vel så fremtredende i andre deler av det internasjonale samfunnet i tillegg til den krigssentrerte. Sektorene er en måte å forstå den utvidede

sikkerhetsagendaen på ved å forsøke å identifisere spesifikke eksistensielle trusler og referanseobjekter; altså det eller de som krever den nødvendige andel sikkerhet i hver av sektorene (Buzan, Wæver og de Wilde 1998). Sikkerhet i det store bildet refereres ofte til politiske og statlige affærer. Sikkerhet i cyberdomenet er sannsynligvis intet unntak. Ved å koble Københavnerskolens sektorer opp mot mediearkeologiens materialitet og nettverksarkeologiens fokus på strukturelle omstendigheter, ønsker jeg for det første å vise at materielle aspekter av teknologi er minst like viktige som de «usynlige», og at en beskyttelse av disse aspektene, i henhold til *securitization theory*, er like viktig som en beskyttelse av en stats befolkning eller staten selv.

Mange av dagens medier har en tilknytning til og en sammenheng med tidligere krigsorienterte innretninger – noe som blir utforsket senere i kapittelet og avhandlingen for øvrig – og gjør det desto enklere å tenke på teknologi som noe som både har legitime referanseobjekter og trusler i likhet med de andre sektorene som har blitt omfattet av det utvidede sikkerhetsbegrepet. I tillegg utgjør åpenbare negative konnotasjoner og historiske forhold en betydelig basis for en *securitization* av et bestemt konfliktområde (Peoples og Vaughan-Williams 2015). Allerede i 1982 forekom et av de største cyberangrepene verden har sett: En logisk bombe forårsaket en massiv eksplosjon i en gassrørledning i Sibir. Bomben ble angivelig skapt av CIA som plantet en trojansk hest (datavirus) i programvaren som de på forhånd visste at sovjetene ønsket å få tilgang til. Den amerikanske etterretningsorganisasjonen lot dermed sovjetene stjele programvaren for så å uoppdaget sabotere den sibirske gassinfrastrukturen (Melito, årstall ikke angitt, Hamnes 2012). Den senere tid har det vært debattert rundt hvorvidt det faktisk var CIA som stod bak hendelsen, men uavhengig av hvem eller hva som var sabotøren, er utfallet og omstendighetene fortsatt de samme: Digital sabotasje tok sted i en tid da to supermakter kjempet om politisk hegemoni, og oppfattet hverandre som bitre fiender. Retter vi oppmerksomheten mot 2016, får vi et lignende scenario der rollene er reversert: Et cyberangrep fra den tidligere Sovjetunionen ble rettet mot USA hvor e-postkontoene til medlemmer av det demokratiske partiet ble hacket under en presidentvalgkamp. Nok en gang fulgte spekulasjoner, tvil og debatt angående angrepets opphav. Episoden i Sibir 34 år tidligere har bidratt til å forme det historiske forholdet og konnotasjonene de to stormaktene imellom, og sannsynligvis muliggjort et markant skifte i hvordan statene utvikler og forvalter sikkerhetspolitikken sin på cyberområdet.

I hennes forord til *Internasjonal cyberstrategi for Norge* av 2017 skriver statsminister Erna Solberg blant annet at «Betydningen av det digitale rom for nasjoners økonomi, sikkerhet, vekst og utviklingsmuligheter er stor og økende» (2017:3). I Justis- og beredskapsdepartementets stortingsmelding om IKT-sikkerhet påpekes det at «IKT-infrastruktur og -systemer blir mer globale, omfattende og integrerte» (IKT-sikkerhet 2017:14), og at stadig flere enheter tilkobles internett. Nasjonale og internasjonale aktører er villige til å bruke digitale virkemidler for å påvirke prosesser og beslutninger på både politisk, økonomisk og forvaltningsmessig plan. Slike påvirkningsoperasjoner i cyberspace kan ha et omfang og effekt som vi aldri før har vært vitne til. Denne utviklingen peker på at en stats forhold, politikk og historie i relasjon til andre internasjonale aktører er nødt til å ses i sammenheng med den globale flyten og utbredelsen av informasjons- og kommunikasjonsteknologi, og at cybersikkerhet spiller en viktig rolle her.

I det følgende vil jeg skissere hovedlinjene i teoriretningene som danner grunnlaget for analyse og diskusjon av fastsatt problemstilling. Det greies først ut om sikkerhetsbegrepet. Deretter tar jeg for meg mediearkeologi generelt og nettverksarkeologi spesielt. I siste del av kapittelet, sammenfatter jeg de teoretiske tilnærmingene, og oppsummerer relevansen de har for oppgaven.

2.2 – Sikkerhetsbegrepets utvikling

Sikkerhet er et bredt og komplisert felt. I mange tilfeller, betyr sikkerhet ulike ting for ulike mennesker. Sikkerhet kan fremstå annerledes avhengig av kontekst og situasjon. Sikkerhet kan likeledes bli satt i sammenheng med graden av frihet, både positiv og negativ (Williams 2013); slik som henholdsvis frihet *til* grunnleggende menneskerettigheter, som vann, mat, klær og husly, og frihet *fra* ødeleggende trusler, som krig og konflikt, sult, sykdommer og generell berøvelse av et verdig liv. Uavhengig av hvordan vi velger å definere sikkerhet, har begrepet en mer eller mindre konstant kjerne som alltid vil være gjeldende: *Sikkerhet involverer en minimering av trusler mot sentrale verdier* (Williams 2013).

Tradisjonelt sett har sikkerhetsstudier beskjeftiget seg med det som nok kan sies å være selve behovet for en slik politikk, nemlig væpnet krig mellom stater. En grunnleggende sikkerhetspolitikk for en nasjon handlet om fraværet av trusselen om fysisk maktbruk fra omkringliggende stater, og evnen til å bekjempe slik maktbruk hvis det skulle være nødvendig (Hovi og Malnes 2011). Statsoverhodene var de fremste aktørene, nasjonens suverenitet,

integritet og autonomi var det som skulle beskyttes, og kraftige militære arsenal var midlene som skulle anvendes. Kort sagt er tradisjonell sikkerhetsteori nokså simpel og ensformig. Ronnie D. Lipschutz sier det så enkelt som at: «There exist threats to the territory of one state posed by the activities of other states» (1995:5). Den fremste funksjonen i enhver stat er selvforsvar, og i ytterste konsekvens – krig. I tradisjonell sikkerhetspolitisk tenkning finnes det naturligvis andre presserende trusler og konflikter, men disse er ikke definert som sikkerhetstrusler *per se* (Lipschutz 1995). Tradisjonelle tilnærminger til sikkerhetspolitikk er altså *statssentriske* hvilket betyr at staten er det som sikkerhetspolitikken sentrerer rundt, og de definerte truslene bunner i militær vold (Peoples og Vaughan-Williams 2015).

2.2.1 – Realisme

Grovt sett, kan vi identifisere to vesentlige filosofier i måten å omtale sikkerhet på: Realisme og konstruktivisme. Den første er nok den av teoriene som best kan sammenfattes med tradisjonell sikkerhetstenkning, og tar utgangspunkt i at sikkerhet er et resultat av tilegnelsen av makt (Williams 2013). Jo mer makt en stat har, desto høyere sikkerhet forvalter den. Realistene ser på sikkerhetspolitikk som noe som styres av objektive, universelle lover og staters egeninteresser (Goldstein og Pevehouse 2014). Disse interessene bunner som regel i staters ønske om å øke sin styrke og kapabilitet (Williams 2013). Denne styrken og kapabiliteten kan oppsummeres i begrepet om makt. Makt defineres i sin tur av evnen til å få en motpart til å enten avstå fra en handling vedkommende ellers ikke hadde avstått fra eller tvert imot; å sette i gang en handling hos motparten mot dennes vilje (Goldstein og Pevehouse 2014).

Denne tradisjonelle måten å se sikkerhet på har sine svakheter i at den fokuserer altfor mye på problemstillinger som var særlig relevante under den andre verdenskrig, og spesielt under den kalde krigen. Den sikkerhetspolitiske diskursen handlet om supermakter og deres arsenal av atomvåpen. Selv om dette var trusler som var særlig fremtredende under den gangs omstendigheter, har verden utviklet seg i en retning som fordrer oppmerksomhet rundt langt flere og mer ulike konflikter. Dette kunne man merke mot slutten av den kalde krigen, da flere og flere tok til ordet for at andre samfunnssfærer i tillegg til den militære, måtte få sin rettmessige plass på sikkerhetsagendaen. Det oppstod et behov for at *referanseobjektet*, altså det som krevde sikkerhet og beskyttelse, skulle dreie seg lenger bort fra staten, og over mot andre, mer «utradisjonelle» enheter. Stater har gjennomgått betydelige endringer i løpet av historien, og mange av dem er fremdeles på vei mot å utvikle og forbedre sine indre krefter

samt sin posisjon på den internasjonale arena. Siden starten av den industrielle revolusjonen, er det spesielt to aspekter ved statenes eksterne miljø som har hatt en innvirkning både på seg selv og på statenes omstendigheter, ifølge Barry Buzan. Disse er *the interaction capacity of the system* og *international society* (Lipschutz 1995).

Det førstnevnte aspektet, «systemets interaksjonskapasitet», omfavner teknologiske og organisatoriske faktorer som determinerer volumet og kvaliteten på varer og informasjon som forflyttes over de statlige grensene. Enklere sagt, kan dette gå for det samme som globalisering. Varer, informasjon og tjenester krysser landegrensene i enorm fart og med høy frekvens, noe som gir både nye muligheter, men også en god del utfordringer for individuelle stater. Samfunnene løper store risikoer ved at høy kontakt og åpne grenser kan ende i konflikt som et resultat av forurensing, sykdom, propaganda, eller innvandring. På den annen side åpner globalisering opp for at nyttig informasjon, kulturutveksling, assistanse, og økonomiske markeder får spille en betydelig rolle i utviklingen av samfunn, og dermed stater som helhet (Lipschutz 1995).

Buzans andre aspekt i påvirkningen av statenes realitet er «det internasjonale samfunnet» som han skriver bunner i at statene tildeler hverandre gjensidig anerkjennelse, og anser hverandre som lovlig likestilt. Det internasjonale samfunnet består av internasjonal lov, diplomati, regimer og organisasjoner. Innenfor disse rammene, kan statene interagere med hverandre, noe som gir dem anledning til å forme sine omgivelser, i tillegg til at slik deltakelse tilbyr en høyere grad av stabilitet og forutsigbarhet. Men som de fleste faktorer på det internasjonale plan, har også det internasjonale samfunnet sin skyggeside: Enkelte stater kan oppleve at lover og institusjoner begrenser deres frihet og ødelegger deres karakteristiske identitet. For eksempel kan spørsmål som angår menneskerettigheter, demokrati og ikke-spredning av kjernefysiske våpen, oppfattes som trusler og byrder for enkelte stater fordi disse områdene ikke samsvarer med statenes individuelle politiske og kulturelle identitet, utenrikspolitikk eller egeninteresser (Lipschutz 1995).

Buzans redegjørelse for systemets interaksjonskapasitet og det internasjonale samfunnet er en viktig del av forståelsen for hvordan og hvorfor sikkerhet har utviklet seg i den retningen den har. Teknologi og globalisering har gjort at det internasjonale plan har blitt mer sammenvevd – på både godt og vondt: «Both interaction capacity and international society have been increasing in scale and scope and, in doing so, have greatly expanded the menu of threats and opportunities that states face in their international environment» (Buzan 1995:194). Dette gjør

seg ikke minst gjeldende i koblingen til internett og cyberdomenet. Med inntoget av «hybrid krigføring», der stater kombinerer militære maktmidler med utradisjonelle og innovative kapabiliteter, har cyberspace blitt en sentral spillebrikke i deres avskrekkingsmekanismer og sabotasjer. I dagens internasjonale forhold, har Russland distansert seg ytterligere fra vesten og *vice versa*. Spenningen dette medfører, gjør at omkringliggende stater er nødt til å utvide sitt syn på sikkerhet, og tenke utover det som tidligere har vært nødvendig. Med Norges posisjon som verdens 2. ledende gasseksportør, og landets geografiske nærhet til Russland samt den politiske og sikkerhetssentrerte tilknytningen til NATO, gjør at den norske nasjonens sikkerhet i særlig grad blir påvirket og utfordret av Russlands nåværende interaksjon med vesten: «Norway, like other countries, needs to have a holistic view of the security threat, and not limit itself to focusing solely on conventional military threats» (Pijnenburg Muller, Gjesvik og Friis 2018:6).

2.2.2 – Konstruktivisme

På bakgrunn av det ovennevnte, begynner vi å bevege oss mot den andre teoretiske retningen innen sikkerhetsstudier, nemlig konstruktivismen. Denne tilnærmingen baserer seg på oppfatningen om at våre omgivelser er konstruert og betinget av sosial interaksjon. Dette er særlig forsterket i Buzans fremstilling av det internasjonale samfunnet samt Russlands nevnte forhold til vesten – stater samhandler med hverandre og andre instanser på den internasjonale arena, og skaper med dette relasjoner og situasjoner som legger føringer for videre handlinger, det være seg politiske eller militære.

Konstruktivistene står for at stater og deres sikkerhetspolitikk ikke styres av objektive, universelle regler, men spesifikke hendelser. Disse hendelsene trenger ikke nødvendigvis å være noe som har skjedd i nær fortid, men kan også være tidlige historiske forhold som fremdeles har innflytelse på statenes relasjoner den dag i dag. Mens realistene utelukkende fokuserer på militære kapabiliteter uavhengig av andre faktorer, mener for eksempel Alexander Wendt at et stort militært arsenal hos stat A ikke nødvendigvis medfører større usikkerhet for stat B. Denne usikkerheten hviler på hvilket *forhold* disse to statene har i utgangspunktet. Wendt eksemplifiserer det slik:

> 500 British nuclear weapons are less threatening to the United States than 5 North Korean nuclear weapons, because the British are friends of the United States and the North Koreans are not, and amity or enmity is a function of shared understandings (Wendt 1995:73).

Wendt tilhører det rammeverket innenfor konstruktivismen som ligger nærmest tradisjonelle sikkerhetspolitiske teorier, slike som realisme og liberalisme. Konvensjonell konstruktivisme peker på statenes *identitet* samt egeninteresser, og legger dette til grunn for hvordan de handler på den internasjonale arena. Her beskrives identitet som noe som kan bli avdekket gjennom analyse, et syn som henger tett sammen med positivistisk epistemologi. Innen et slikt rammeverk, blir identiteten sett på som relativt stabil og sedimentert, og legger dermed til rette for at analytikere kan utforske den ytre verdenen med et objektivt blikk (Williams 2013). For *kritiske* konstruktivister, derimot, er identitet noe som stadig forandrer seg, og gjør det dermed ikke mulig å forstå statenes sikkerhetspolitiske strategier på et overordnet plan fra «yttersida» – vi må inn i de spesifikke omstendighetene der og da, og forsøke å definere hvem «vi» er i forholdet med «de andre» som vi opplever at vi må beskytte oss mot (Williams 2013). Dermed kan vi si at generell konstruktivistisk tankeretning er mer tilbøyelig til å se verden fra litt flere sider.

2.3 – Securitization theory og tilhørende sektorer

Det er kanskje derfor konstruktivismen har bidratt til å gi opphav til en ny form for sikkerhetsteori, nemlig *securitization theory* eller «sikkerhetiseringsteori» – en avart jeg har valgt å bruke på bakgrunn av det norske «sikkerhetisere» eller «[…] 'sikkerhetiseres' […]», slik det blir presentert i John Kristen Skogan sin tekst på s.107 i antologien til Jon Hovi og Raino Malnes fra 2011. Det er nettopp denne teorien som kan sies å konseptualisere synet om et utvidet sikkerhetsbegrep *utover* staten som referanseobjekt. Sikkerhetisering handler ikke nødvendigvis om å fastslå konkrete og objektive trusler, sårbarheter eller forsvarsmekanismer, men mer om å *portrettere* eller skildre trusler som nettopp noe som truer sikkerheten innen et eller flere bestemte samfunnsaspekter. Teorien beskjeftiger seg med spørsmål rundt hvordan referanseobjekter og sikkerhetiseringsaktører tilrettelegger betingelser for at et problemområde som har blitt presentert som en sikkerhetstrussel blir allment akseptert som nettopp dette (Nissenbaum 2005).

Den allerede nevnte Barry Buzan utgjør, hovedsakelig sammen med Ole Wæver og Jaap de Wilde, *the Copenhagen School* – Københavnerskolen – som gjerne er den man forbinder med sikkerhetiseringsteorien. I motsetning til tradisjonalistene, som forsvarte en statssentrisk sikkerhetspolitikk, ønsket de å ekspandere begrepet om sikkerhet ytterligere. De tar sterk avstand fra at krig og makt skal være de eneste fokuspunktene i studien av sikkerhet, og mener at sikkerhetsagendaen bør være åpen for mange forskjellige typer trusler, så vel

militære som ikke-militære (Buzan, Wæver og de Wilde 1998). Ifølge Lene Hansen og Helen Nissenbaum er denne skolen også særdeles passende i denne oppgavens kontekst om cybersikkerhet fordi «[…] its understanding of security as a discursive modality with a particular rhetorical structure and political effect makes it particularly suited for a study of the formation and evolution of cyber security discourse» (2009:1156).

Buzan *et al*. presenterer *sektorer* hvor konkrete problemområder kan oppstå, og dermed også bli inkludert i sikkerhetsdebatten. Sektorene de legger frem er den militære, den politiske, den økonomiske, den samfunnsmessige, og den miljømessige. Disse fungerer som linser eller diskurser heller enn objektivt eksisterende fenomener (Hansen og Nissenbaum 2009). Et av stegene frem mot et utvidet sikkerhetsbegrep, var å forkaste staten som det sentrale fokusobjekt i alle sektorene, og tillate andre aspekter å komme inn (Buzan, Wæver og de Wilde 1998).

Jeg vil derfor ikke utdype den militære sektoren nevneverdig her ettersom den allerede har blitt behandlet tidligere både med utgangspunkt i den tradisjonelle sikkerhetstenkningen og ut fra den realistiske teorien. I stedet, foretar jeg heller en kort utgreiing av de øvrige sektorene som har spilt en rolle i utvidelsen av sikkerhetsbegrepet. Der det er relevant, vil jeg også kort relatere sektoren til avhandlingens fokus rundt norsk petroleumssektor og cybersikkerhet. Dette gjelder spesielt miljøsektoren og den økonomiske sektoren. En bredere diskusjon rundt dette vil påfølge senere i oppgaven.

2.3.1 – Miljøsektoren

Miljøsektoren har blitt omfavnet av det utvidede sikkerhetsbegrepet på bakgrunn av følgende problemstillinger: Den hurtige degraderingen av jorda, de høye forbruksnivåene av naturens energiressurser, og sannsynligheten for at den globale befolkningsøkningen både vil fortsette og forsterke de førstnevnte trendene (Peoples og Vaughan-Williams 2015). Klimaendringene vil nødvendigvis også gjelde innenfor denne kategorien.

Innen miljøsektoren peker Buzan *et al*. på to typer referanseobjekter; miljøet i seg selv, og sivilisasjonen eller *opprettholdelsen av nåværende sivilisasjonsnivå*. Fokuset på sivilisasjon og bekymringen for at denne kan gå tapt, har blitt overført til miljøsektoren fra den samme bekymringen omkring kjernevåpen under den kalde krigen (Buzan, Wæver og de Wilde 1998). En slik felles problemstilling i både den militære og den miljømessige sektoren har sannsynligvis gjort det mer akseptabelt og enkelt å inkorporere miljø inn i sikkerhetsbegrepet.

Menneskenes utnyttelse av naturens ressurser, ødeleggelse av økosystemer, utryddelse av dyrearter, og mye annet, legger føringer for negative konsekvenser både for miljøet selv, og for oss som er omgitt av det. Stabiliteten og levestandarden i en stat kan bli drastisk endret ved for eksempel et tilfelle av ressursknapphet. Michael T. Klare mener sågar at statenes sikkerhet til syvende og sist er avhengig av deres energiforsyning; beskyttelse av oljefelt og maritime handelsruter samt muligheten til å eksportere energiprodukter er sentrale bestanddeler i økonomisk konkurranse og følgelig – i statens overlevelse (Peoples og Vaughan-Williams 2015). I tillegg kan miljøet og økologien rundt olje- og gassinstallasjoner bli direkte negativt berørt hvis et digitalt angrep mot nevnte installasjoner resulterer i for eksempel oljesøl.

2.3.2 – Samfunnssektoren

Samfunnssektoren i et sikkerhetsmessig perspektiv sies av Københavnerskolen å være knyttet til beskyttelsen av fellesskap eller store identitetsgrupper. Samfunnssikkerhet kan derfor også omtales som «identitetssikkerhet» (Buzan, Wæver og de Wilde 1998). Slike fellesskap kan i dag defineres som stammer, minoritetsnasjoner, sivilisasjoner, religioner og raser (Buzan, Wæver og de Wilde 1998). Avhengig av hvilket samhold disse gruppene har, og hvilken identitet de identifiserer seg med, vil truslene de møter være ulike. Et eksempel på dette er hvordan Russland velger å se på seg selv – om nasjonen og dens befolkning blir tillagt en identitet som er typisk for slavofile, vil denne definisjonen medføre en rekke sikkerhetstrusler som kunne ha vært unngått om landet assosierte seg selv med en mer vestlig tankegang (Buzan, Wæver og de Wilde 1998). Trusler innen denne identitetssikkerheten handler om hva som kan bli konstruert som en trussel mot et «vi»: «Societal insecurity exists when communities of whatever kind define a development or potentiality as a threat to their survival as a community» (Buzan, Wæver og de Wilde 1998:119). Samfunnssikkerhet handler om å beskytte samfunn en selv identifiserer seg med, og må ikke forveksles med *sosial sikkerhet* som omfatter individer fremfor grupper (Buzan, Wæver og de Wilde 1998).

2.3.3 – Økonomisektoren

Den økonomiske sektoren er ekstremt kontroversiell og politisert. Kapitalistiske økonomer mener at selve grunnlaget i et marked nettopp er *usikkerhet* – ellers vil ikke markedet produsere effektivitet (Buzan, Wæver og de Wilde 1998).

Buzan *et al*. skriver at fem spesifikke problemstillinger kan trekkes frem innen den økonomiske sikkerhetssektoren: 1: Statens evne til å opprettholde en uavhengig militærproduksjon i et globalt marked, 2: Muligheten for at økonomiske avhengigheter innen det globale markedet, især olje, vil bli utnyttet for å nå politiske mål, 3: Frykten for at det globale markedet vil forsterke eksisterende ulikheter, 4: Frykten for ulovlig handel, blant annet med narkotiske stoffer, lette våpen og militær teknologi, og at et masseforbruk og utbredelsen av industrialiseringen vil legge et press på det globale miljøet, og 5: Frykten for at den internasjonale økonomien i seg selv vil lide et nederlag som et resultat av svekket politisk lederskap, økende grad av proteksjonisme, og ustabilitet i det globale finanssystemet (Buzan, Wæver og de Wilde 1998).

Økonomi er basisen og betingelsen for mange ting, fra en grunnleggende levestandard til eksklusive goder. Derfor har den økonomiske sektoren også innflytelse på andre sektorer, og omfatter ulike referanseobjekter (Buzan, Wæver og de Wilde 1998).

I relasjon til petroleumsnæringen, er økonomisektoren av stor betydning fordi en mulig produksjonsstopp som følge av et cyberangrep, kan få store konsekvenser for næringslivet og økonomien i helhet. Av de fem nevnte problemstillingene innen økonomisektoren, er spesielt nr.2 en betydningsfull trussel, for eksempel hvis en stat svekker, underminerer eller kutter Norges petroleumseksport til Europa ved digital sabotasje som et virkemiddel for å gjennomføre sin egen politiske agenda.

2.3.4 – Den politiske sektoren

Den politiske sektoren på den utvidede sikkerhetsagendaen omfatter en opprettholdelse og en beskyttelse av sosial orden med trusler mot statens suverenitet og organisasjonsstruktur som det sentrale problemområdet.

På den ene siden kan det argumenteres for at den politiske sektoren er et overflødig aspekt på sikkerhetsagendaen ettersom «[…] all security is political […]» (Buzan, Wæver og de Wilde 1998:141), men på den annen side har politisk sikkerhet en viss validitet fordi en kan identifisere mer eller mindre konkrete trusler som er særegne for nettopp denne sektoren. Politiske trusler handler om å gi eller frata anerkjennelse, støtte eller legitimitet. Slike trusler er politiske fordi de ikke er avhengige av militære, økonomiske eller andre midler fra de øvrige sektorene (Buzan, Wæver og de Wilde 1998). Referanseobjektet er i all hovedsak staten. For en suveren stat, kan trusler mot ideer som staten er bygget på og eksisterer i

henhold til, hvorav de viktigste nok er nasjonalisme og politisk ideologi, føre til en ustabilitet innen den politiske ro og orden (Buzan, Wæver og de Wilde 1998).

Det som gjør den politiske sektoren til en legitim del av det utvidede sikkerhetsbegrepet er ikke bare det faktum at staten fungerer som det vesentligste referanseobjektet, slik den også gjør i den tradisjonelle, militære sikkerhetssektoren, men også fordi de verste truslene faktisk kan være eksistensielt ødeleggende. *Suverenitet* er det som definerer en stat som stat, og innebærer at «[…] staten har monopol på legitim utøvelse av makt innenfor sitt territorium, og at det er regjeringen som definerer og håndhever statens interesser utad gjennom utenrikspolitikken» (Fermann 2011:32). En trussel mot statens suverenitet er derfor også en trussel mot statens overlevelse. Alt som kan bli presentert som brudd på suverenitet, kan bli definert som en sikkerhetstrussel (Buzan, Wæver og de Wilde 1998), og vil derfor være et effektivt utgangspunkt for en sikkerhetisering.

Et cyberangrep mot norsk petroleumssektor vil nok ikke anses som en direkte trussel mot statens suverenitet eller organisasjonsstruktur, men det har potensiale til å svekke tilliten som mottakerne av norsk olje og gass har til Norge. Norges petroleumsnæring vil få svekket omdømme, og hvis bakgrunnen for et vellykket cyberangrep med betydelige konsekvenser er resultatet av dårlige sikkerhetsrutiner i den norske olje- og gassektoren samt på myndighetsnivå, har dette også mulighet for å spre tvil blant europeiske kunder rundt Norges sikkerhet og stabilitet som olje- og gasseksportør. I verste fall, kan Norge miste legitimitet på dette området, men det vil sannsynligvis ikke påvirke det internasjonale samarbeidet på andre felt i nevneverdig grad.

2.4 – Cyberspace i en sikkerhetisert kontekst

Københavnerskolens sektorer viser et oppgjør med en snever og tradisjonalistisk sikkerhetstenkning. Blant nevnte utfordringer knyttet til klima, asylpolitikk og samfunn, finnes også problemområder innen cyberspace som, på lik linje med de foregående sektorene, kan omtales i en sikkerhetiseringskontekst. Cybertrusler kan bli presentert som eksistensielt ødeleggende på grunn av de mange nettverkene i samtlige datasystemer. Et angrep mot systemer som kontrollerer fysiske objekter, som for eksempel elektriske transformatorer, boreutstyr, rørledningspumper, kjemiske beholdere og radarer, kan resultere i konsekvenser som ikke bare går utover nettverkene selv, men også utover andre referanseobjekter i andre sektorer. Diskursen om cybersikkerhet flyter dermed sømløst mellom samtlige

samfunnsaspekter – mellom individets og kollektivets sikkerhet, offentlige myndigheter og private institusjoner, og mellom økonomisk og politisk-militær sikkerhet (Hansen og Nissenbaum 2009) – noe som legitimerer det sikkerhetiserte synet om at et eller flere cyberangrep på kritisk infrastrukturnettverk kan få betydelige samfunnsmessige ødeleggelser som kan true både staten og dens befolkning.

Et av de vesentligste bekymringsmomentene som nettverksteknologier fremmer, er muligheten de har for å forandre måten å konstruere ikke-territorielle samfunn og referanseobjekter på (Buzan og Hansen 2009): En betydelig problemstilling med angrep i cyberspace er at de gjennomføres i skjul. En kan aldri vite med full sikkerhet hvorvidt, og eventuelt; hvor et cyberangrep kan inntreffe. Ei heller kan man være fullstendig overbevist om hvor angrepet kom fra eller hvem som var skyldig. Justis- og beredskapsdepartementet skriver i sin melding til Stortinget om IKT-sikkerhet at «Sikkerhet var lettere å vurdere da det som skulle sikres, var noe fysisk, håndfast og stabilt. […] I den digitale verden kan man bli mer fremmedgjort når det gjelder sikkerhet. Vi har ikke lenger den samme oversikten over sårbarhetsbildet» (IKT-sikkerhet 2017:26). Cyberspace har ingen geografiske grenser, og aktørene i dette domenet er ofte usynlige eller ukjente. Det digitale rom er heller ikke «eid» eller styrt av én enkelt autoritet, sånn som for eksempel et statsoverhode vi kjenner til fra «fysiske» internasjonale relasjoner og tradisjonell sikkerhetstenkning. Dette gjør det desto vanskeligere å forholde seg til cyberspace som et konkret territorium, hvor de involverte har oversikt over hverandre, og hvor faste, stabile regler og normer er på plass. Dette faktumet har markert et skifte fra «[…] a territorial, well-defined enemy during the Cold War to the terrorist who moves anonymously until the moment he/she strikes […]» (Buzan og Hansen 2009:249).

2.5 – Mediearkeologien og dens særegenheter

I innledningen til dette kapittelet ble to teoretiske perspektiver presentert. Det ene – konseptet om et utvidet sikkerhetsbegrep med tilhørende sikkerhetiseringsteori – har jeg nå kartlagt. Den andre tilnærmingen tilhører medievitenskapen, og heter mediearkeologi. En underkategori til denne er nettverksarkeologi. Med grunnlag i dette prosjektets problemstilling, er det naturlig å analysere den ut fra et materialistisk og nettverkssentrert perspektiv, noe de nevnte medievitenskapelige teoriretningene er behjelpelig med. I det følgende vil det redegjøres for mediearkeologien generelt og nettverksarkeologien spesielt. Deretter vil tilnærmingene føres sammen med sikkerhetiseringsteorien for å bedre forstå

cyberdomenets posisjon i sikkerhetspolitikken samt digital sikkerhet i norsk petroleumsnæring.

Gunnar Iversen skriver at mediearkeologi er et vanskelig konsept å definere. Det er verken en profesjon, disiplin eller metode. Det finnes heller ikke bare én mediearkeologi, men flere typer bestående av et heuristisk metodisk anarki (2016). Den henter sin inspirasjon på tvers av en lang rekke disipliner og fagområder; fra humaniora via samfunnsfag til kunstvitenskap, noe som mer enn nok legitimerer mediearkeologien som en «traveling discipline» (Huhtamo og Parikka 2011). Best kan nok mediearkeologien beskrives som «[…] en motstander av strengt lineær historieskriving» (Iversen 2016:172). Den er et alternativ til normalvitenskapen og en utfordrer av fastsatte, tradisjonelle forskningsrammer innen mediehistorie og -vitenskap. Når vi benytter oss av mediearkeologien, betyr det at vi stiller spørsmålstegn ved etablerte sannheter, og forsøker å rette søkelyset mot de medieaspektene som ikke har fått like stor plass i utgreiingen av deres historiske utvikling.

Mediearkeologien ønsker også å ta avstand fra et kategorisk syn på «nye» og «gamle» medier. Det er ikke slik at ett medium erstattet et annet. Mediene har heller utviklet seg ved å bygge på hverandre, endre og forbedre seg i relasjon til menneskenes behov der og da. Thomas Elsaesser skriver at kinoen har for mange «foreldre» og «slektninger» til at dens historie utelukkende kan skildres ved hjelp av et enestående, lineært narrativ (2004). Slik kan vi også si at det er for de andre mediene. Den abstrakte datamaskinen utarbeidet av Alan Turing i 1936, som senere la grunnlaget for dekodingen av nazistenes krypterte meldinger under den andre verdenskrig, er ikke en forløper til den moderne datamaskinen slik vi kjenner den i dag – tvert imot er *alle* dagens datamaskiner Turing-maskiner fordi de bygger på samme konsept om et sett med algoritmer som fordrer maskinen til å utføre bestemte oppgaver (Mitchell og Hansen 2010). Likeledes ble ikke internettet unnfanget kun for internettets skyld. Det kommersielle nettet har, i likhet med Turing-maskinen, sine røtter i den militære sektoren, og bygger på et distribuert nettverk kalt (D)ARPANET fra 1969 – en teknologi utviklet av Paul Baran som muliggjorde sending av meldinger uten at denne prosessen ble avbrutt eller destruert av et atomangrep (Galloway 2004). I mediearkeologien lever alle teknologier side om side, og har ingen klare skillelinjer mellom «gammel» og «ny».

Et av mediearkeologenes fremste anliggender er *materialitet*, og Friedrich A. Kittlers kategoriske uttrykk «Media determine our situation […]» (Kittler 1999:xxxix) viser hvor sterkt materialiteten står, ikke bare i vitenskapen, men også i forholdet til oss mennesker og

samfunnet som omgir oss. Også Michel Foucaults tekster har spilt en stor rolle i utformingen av mediearkeologien med hans «[…] archaeology of knowledge and culture […]» (Parikka 2012:6). Her manifesterer den arkeologiske delen seg i utforskningen av de bakenforliggende betingelsene som muliggjør eksistensen av et bestemt objekt, et utsagn, en diskurs, et medieapparat eller en bruksvane i en spesifikk kulturell situasjon. (Parikka 2012). Kittler dro inspirasjon av og bygde videre på Foucaults tanker og ideer, men påpekte likevel at det lå et problem i Foucaults altfor tunge vektlegging av diskurs og hans altfor snevre fokus på teknologi og materialitet (Huhtamo og Parikka 2011).

Ved å rette oppmerksomheten mot materialitet i medieforskningen, tar man avstand fra det som ofte har vært vanligst å ha som utgangspunkt, nemlig abstrakte, immaterielle konsepter som meningsinnhold, retorikk, og tolkning. Disse bestanddelene tillegges nok mest «gamle» medier som TV og avis, men også blant «nye» medier blir uhåndgripelige fokuspunkt lagt stor vekt på. Når vi snakker om internett, for eksempel, tenker vi ofte på det som noe svevende i form av en «sky». Internettets *hardware,* på den annen side, forblir i periferien. En bør kjenne til hvordan mediet fungerer rent teknisk for å kunne være i stand til å tolke og forstå historien i sin helhet, mener mediearkeologen Wolfgang Ernst ifølge Iversen (Iversen 2016). En belysning av mediematerialitet fordrer også at vi tar stilling til hvordan teknologi er en aktiv agent i påvirkningen og utformingen av verdenen rundt oss (Parikka 2015).

Viktigheten og alvorlighetsgraden av kunnskap om mediets teknologiske funksjon og sammensetning er noe som også kommer til syne i sammenheng med oppgavens problemstilling som omtaler cyberangrep mot petroleumsrelatert infrastruktur: Det er ikke nok å være generelt teknisk kompetent med en innsikt i *software* og *hardware* – for å gjennomføre et digitalt sabotasjeangrep må en også kjenne til de konkrete prosess- og kontrollmekanismene som styrer innretningen som skal angripes. Slik omfattende kompetanse ligger stort sett hos statlige aktører, men kan også tilegnes av sivile, slik det blir utdypet senere.

2.5.1 – Nettverksarkeologi

For å unngå lineære narrativ i tilnærminger til mediehistorien, er vi som sagt nødt til å «tenke utenfor boksen», og ta tak i aspekter som det ikke alltid har vært snakket like mye om. En av dem som har gått en alternativ vei for å finne nye og innsiktsfulle sammenhenger i historien er Nicole Starosielski. I hennes *The Undersea Network* fra 2015 utforsker hun de undersjøiske

fiberoptiske kablene som transporterer 99% av all digital kommunikasjon, fra telefonsamtaler via fjernsyn til internett. Starosielski bruker *nettverksarkeologi* for å historisere «[…] the movements and connections enabled by distribution systems […]» (2015:15), og for å belyse de omstendigheter som er med på å forme vårt moderne medieomløp. Disse omstendighetene definerer hun som en kompleks sirkulasjonssamling, bestående av arbeid, økonomi, kultur, og politikk som legger føringer for vår digitale hverdag (Starosielski 2015).

Mange aktører spiller en rolle i utformingen av den digitale verdenen rundt oss innen alt fra underholdningsapplikasjoner til kritisk infrastruktur. Kritiske samfunnsfunksjoner har blitt avhengige av lange og uoversiktlige digitale verdikjeder (Digital sårbarhet - sikkert samfunn 2015); et konsept som gjerne kan kalles for *cyber supply chains*. I slike – ofte globale – verdikjeder igangsettes og gjennomføres prosesser knyttet til utvikling av *hardware* og *software*, leveranse av logistiske tjenester samt distribusjon og salg (Windelberg 2015). Nettverkene dette skaper medfører en risiko i at leverandørene ikke alltid opprettholder det nødvendige sikkerhetsnivået i varene de produserer eller at mottakerne av produktet ikke stiller høye nok krav til sikkerhet i systemene de får. For eksempel kan forfalsket *software*, utgitt for å være autentisk og velfungerende, være modifisert til å ødelegge systemet det implementeres i som følge av umoralske aktører i ett eller flere ledd i verdikjeden samt mangelen på sikkerhetshensyn hos sluttmottakeren.

Også i Norge er teknologiens utbredelse og livsvilkår avhengig av brede nettverk og risikoene disse bringer med seg, blant annet når sentrale samfunnstjenester leveres av internasjonale aktører uten at norske myndigheter har rettslig kontrollmyndighet over disse (Digital sårbarhet - sikkert samfunn 2015). Hvordan dette påvirker den norske olje- og gassnæringen vil bli eksemplifisert ved en senere anledning.

Ved å rette oppmerksomheten mot nettverk som et historisk studieobjekt, utvider man mediehistorien til å inkludere andre formidlingsformer enn de som det tradisjonelt sett har vært mest interesse for. Slike nye innfallsvinkler kan omhandle alt fra transportinfrastruktur til elektriske systemer eller som i denne oppgavens tilfelle; olje- og gassinstallasjoner på norsk sokkel og deres økende avhengighet av digitale nettverk. I motsetning til mediearkeologien, som først og fremst beskjeftiger seg med de materielle aspektene ved teknologien, ønsker nettverksarkeologene å analysere de mangfoldige og forskjellige nettverkene som bringer teknologiene sammen: «Replacing 'media' with 'network' marks a difference between focusing on media technologies […] and the analysis of network structures themselves,

tracing the nonrepresentational paths, addresses, and intersections of various objects and ideas» (Starosielski, Soderman og Cheek 2013). Cyberspace skaper nettverk på tvers av sektorer og operasjonelle prosesser, og medfører dermed en desto større nødvendighet for en robust digital sikkerhet. Hvordan denne sikkerheten utformes og implementeres er i høy grad betinget av politiske myndighetsavgjørelser. En slik prosess er også til stede i opprettholdelsen av norsk petroleumsindustri, og vil skildres etter hvert.

Starosielskis visjon kan dermed tolkes dithen at med sitt fokus på undersjøiske fiberoptiske kabler og deres geografiske samt historiske tilknytning, politiske styring, sikring, miljøsentrerte utfordringer, og påvirkning på lokalsamfunn kan hun skape et bredere bilde av hvordan overføringen av medialt innhold fungerer og henger sammen, og på samme tid trekke historiske linker til hvordan informasjonsflyten utartet seg før de «nye» medienes tid. Hennes nettverksarkeologiske forskning gir oss et nytt perspektiv på hva som faktisk ligger bak vårt rene, varige og tilsynelatende trådløse internett slik at vi i større grad blir klar over hvilke finansielle, sosiale, og miljømessige konsekvenser som blir resultatet av utbyggelsen, vedlikeholdelsen, forbedringen og omdirigeringen av de fiberoptiske kablene som vår internettbruk er avhengig av (Starosielski 2015). Denne tilnærmingen kommer blant annet til syne i hennes påpeking av koblinger mellom tidligere utbyggelser av kabelnettverk og dagens forhold. For eksempel, skriver hun, er de fiberoptiske kablene som knytter New Zealand til omverdenen, lokalisert i de samme sonene som telegrafkablene var fra begynnelsen av det 20.århundre. Samtidig har USA store kabelsentre på steder etablert under den kalde krigen (Starosielski 2015).

2.6 – Mediearkeologi og sikkerhetiseringsteori under ett

«[…] the reliability of undersea cables has been deemed 'absolutely essential' for the functioning of governments and the enforcement of national security», ifølge Starosielski (Starosielski 2015:1). Dette betyr at konflikter – det være seg sosiale, politiske eller, for den saks skyld; militære – brudd i internettilgangen eller ødeleggelse av infrastrukturen brukt til å holde internettavhengige systemer i gang, kan skape alvorlige følger for samtlige sektorer og referanseobjekter slik tilfellet kan være ved et sabotasjeangrep mot fysiske bestanddeler i petroleumsindustrien. Hansen og Nissenbaum sier at det er umulig å forholde seg til et syn på cybersikkerhet som noe adskilt fra de andre sikkerhetssektorene (2009). Teknologien spenner over mangfoldige samfunnssfærer, og en sårbarhet i én av disse, kan få betydelige konsekvenser for de andre. Både sivil og militær infrastruktur er i høy grad basert på

teknologiske løsninger og avhengig av internett. Dette tilsier at cybersikkerhet er, og må være til stede, i politiske, private, samfunnsmessige og bedriftsrelaterte enheter i tillegg til de rent tekniske og medierte.

Hansen og Nissenbaum mener at «[…] cyber security *is* successfully securitized […]» (2009:1157) som følge av en rekke institusjonelle grep. I amerikansk kontekst, er slike grep blant andre et eksplisitt fokus på cybersikkerhet i det amerikanske innenriksdepartementet, president George W. Bush sin strategi *The National Strategy to Secure Cyberspace* fra 2003, og etableringen av NATOs cyberforsvarssenter CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence) i Tallinn i 2008 (Hansen og Nissenbaum 2009). En institusjonalisering av sikkerhetiseringen ser vi, ifølge Buzan *et al.*, særlig i den militære sektoren, hvor stater lenge har måttet overleve både tvang og invasjon, og måttet etablere permanente forsvarsmekanismer i form av prosedyrer og militære virksomheter for å beskytte seg mot slike vedvarende og gjentakende trusler (Buzan, Wæver og de Wilde 1998). Dette, sammen med teknologiens og medienes røtter i krigstiden, har sannsynligvis forenklet og legitimert sikkerhetiseringen av cyberspace ytterligere.

Spesielt på 1990-tallet, og med inntoget av det kommersielle internett, ble søkelyset for alvor rettet mot cyberspace og dets potensiale til å endre sikkerhetspolitikk, krigføring, og det internasjonale fellesskap for øvrig. USAs mentalitet på den tiden var sterkt sentrert rundt informasjonsteknologi, og var med på å igangsette en «revolusjon i militære affærer» eller *revolution in military affairs*, forkortet RMA. Denne revolusjonen bunner i det amerikanske militærets oppfatning om at bruken av sivile samt militære teknologiinnovasjoner – især innen IT – ville forsterke og forbedre USAs krigføringsstrategier og angrep (Peoples og Vaughan-Williams 2015). Teknologiske stridsmetoder som global overvåkning, robotfly og sanntidssimuleringer, blant mange andre, ga opphav til nye måter å både se og definere krig på blant annet med betegnelser som «nettverkssentrert krigføring», «informasjonskrig», og ikke minst; *«cyberkrig»* (Peoples og Vaughan-Williams 2015). Teknologiske våpen eller «cybervåpen» har potensiale til å fremkalle store ødeleggelser i kommunikasjonsnettverk, satellitter og kritisk infrastruktur, det være seg både sivil og militær.

2.7 – Oppsummering

Cyberspace og -sikkerhet omfatter mange deler, faser og betingelser. Ikke minst er cyberspace og sikkerhet i det digitale rom oppbygd og avhengig av fysiske bestanddeler som må bli tatt

like mye hensyn til som programvare og operativsystem. I henhold til det som har blitt presentert om medie- og nettverksarkeologi tidligere i kapittelet, ser vi at den først og fremst hjelper oss å erkjenne at våre medier og teknologien de baserer seg på kan tolkes og analyseres fra flere vinkler med et ønske om å finne nye utviklingstrekk opp gjennom deres historie. Materialitet er en vesentlig del av denne prosessen, og viser at de teknologiske mulighetene som vi drar nytte av i dag er grunnlagt i håndgripelige og substansielle aspekter.

Digital sabotasje mot kritisk infrastruktur har ikke blitt snakket like mye om som digital spionasje, overvåkning, ulovlig informasjonsinnhenting, *hacking*, *fake news*, brudd på personvern, og lignende problemstillinger. Det virker som at mesteparten av oppmerksomheten har kretset omkring tradisjonell informasjonsteknologi, og mindre om operasjonsteknologien som styrer fysiske prosesser. Digitale sårbarheter innen prosess- og industrisektoren har begynt å vektlegges kun i løpet av det siste tiåret (Digital sårbarhet - sikkert samfunn 2015). Dette viser at temaet er mektig underdebattert, og må komme mer frem i lyset. Wolfgang Ernsts påstand om at en må kjenne til mediets funksjonalitet og sammensetning har også vist seg å være et betydningsfullt aspekt av dagens digitale trusselbilde, ettersom først og fremst statlige, men også andre, aktører ikke kan gjennomføre et digitalt angrep uten å kjenne til teknologien og systemene som ligger til grunn for mediets funksjon de har som mål å angripe.

Nettverksarkeologiens formål er å belyse hvordan både materielle, og andre, aspekter henger sammen, og hva som skal til for at vår digitale hverdag fungerer som den skal. Det digitale rom favner ikke utelukkende om materiale og system, men er i høy grad satt sammen av flere *cyber supply chains* og samfunnsmessige nettverk i alt fra tilegnelsen av nødvendige mineraler til markedsføringen av det ferdige produktet. Alt består av nettverk i så vel direkte forstand som i overført betydning: Cyberspace, digitalisering og internett kobler sammen både maskiner og mennesker, mens cybersikkerheten utformes av nettverk i form av politiske myndighetsprosesser, lovvedtak og -endringer, dokumentutforminger, debatter, utredninger, og så videre.

Mange vitale funksjoner i samfunnet er basert på internettavhengige og digitale løsninger, deriblant også petroleumssektoren i Norge. For å kunne sikre denne på best mulig vis, er cyberspace nødt til å være en sentral del av sikkerhetspolitikken. Dette gjelder ikke bare i den enkelte sektor, men på alle samfunnsnivåer der cyber er tilstedeværende ettersom et digitalt angrep kan spre seg i og sabotere flere punkt samtidig. Københavnerskolen og deres utvidede

sikkerhetsbegrep fastsetter en oppfatning om at sikkerhetskonteksten som de vanligste truslene omtales i er nødt til å inkludere andre problemområder utover de som er forbundet med makt og militære våpenarsenal. Den konkrete sikkerhetiseringsteorien taler for at cybersikkerhet er et like viktig emne på det sikkerhetspolitiske plan som konvensjonell militær krigføring. Et digitalt sabotasjeangrep mot norske olje- og gassinstallasjoner har potensiale til å ha massiv negativ innvirkning på både de fysiske produksjonsmekanismene i industrien og det norske næringslivet i helhet: «Slike angrep kan ha som formål å stanse eller forpurre den fysiske leveransen av olje og gass, og vil dermed ha direkte konsekvenser utenfor det digitale domenet» (NUPI, årstall ikke angitt). Menneskelig, økonomisk, politisk og miljømessig sikkerhet er alle avhengig av at sikkerhetsmodellen i petroleumssektorens digitale verdikjede er robust, oppdatert og velimplementert.

Det er nødvendig å utvide fokuset, som i stor grad til nå har sentrert rundt tradisjonell IKT-sikkerhet i olje- og gassnæringen, til et som tar for seg den fysiske infrastrukturen som næringen er basert på. Ved å få et nærmere innblikk i hvordan materielle objekter kan bli skadet av et immaterielt angrep, vil vi komme nærmere en helhetlig og hensiktsmessig sikkerhetspolitikk som vil gagne alle sektorene i landet.

3 – Metodisk bakgrunn

3.1 – Innledning

Denne avhandlingen er av en teoretisk karakter. Med bakgrunn i problemstillingen, har det vært mest hensiktsmessig å belyse den via teoretiske tilnærminger, som skissert i forrige kapittel. Metodearbeidet har i stor grad vært kvalitativt, og sentrert rundt dokumentanalyse.

Ettersom oppgaven tar for seg spørsmålet angående myndighetenes arbeid i sikringen av petroleumsrelatert infrastruktur mot alvorlige cyberangrep i Norge, har det vært naturlig å finne frem til dokumenter som omhandler dette temaet, for så å foreta en dokumentanalyse av disse, med en særlig inngående analyse av ett av dem. Grunnen for valget av en slik arbeidsmetode var for det første å skaffe et nærmere innblikk i og en bedre forståelse av hvordan den digitale sikkerhetspolitikken i det norske samfunn generelt og olje- og gassektoren spesielt fungerer per dags dato, og for det andre henger en slik dokumentanalyse godt sammen med nettverksarkeologi og oppfatningen om de mange verdikjedene som virker inn på departementenes, tilsynenes og sikkerhetsorganenes beslutninger, og dermed også på ikrafttredelsen av cybersikkerhet i samfunnet og utformingen av vår digitale hverdag.

Dokumentgrunnlaget har i hovedsak bestått av to rapporter, to stortingsmeldinger, én offentlig utredning, én samling retningslinjer, og én forskningsrapport. En liste over disse er lagt til i vedlegg 1. På grunn av begrensninger på både tid og avhandlingens lengde, har jeg valgt å ikke analysere alle leste dokumenter like grundig, men heller rette et konkret fokus mot ett av dem, som nevnt tidligere. Dokumentet som står sentralt i analysen, og avhandlingen for øvrig, er utredningen NOU 2015: 13 *Digital sårbarhet - sikkert samfunn* fra 2015. Nærmere presentasjon av denne vil påfølge senere.

Valget av dokumentanalyse som metode er tredelt: I første omgang, er avhandlingen basert på informasjonen som finnes i tekstene som har blitt lagt til grunn, og legitimerer med det dokumentenes funksjon som «kilder eller ressurser» i utforskningen av tema og *case*. I neste omgang, tegner den konkretiserte dokumentanalysen av NOU 2015: 13 et bilde av hvordan det politiske og organisatoriske arbeidet rundt implementeringen av forebyggende IKT-sikkerhet fortoner seg, blant annet ved å kartlegge hvilke følger NOU-en har fått i ettertid, og hvilke anbefalte tiltak som har trådt i kraft og ikke. I siste instans, legger den offentlige utredningen føringer for en generell diskurs rundt myndighetenes fokus på og omtale av

sabotasjehandlinger fra cyberspace mot materialitet, noe som vil bli vist i påfølgende avhandlingsdel.

Dette kapittelet er strukturert som følger: I første omgang vil jeg kort definere begrepet «dokument» og hvordan dette kan analyseres. Deretter vil jeg gå nærmere inn på kvalitativ dokumentanalyse, og sette denne inn i rammen av avhandlingens kontekst. Jeg vil så redegjøre for selve dokumentanalysen med NOU 2015: 13 som fokuspunkt. Til slutt vil jeg sammenfatte kapittelet i en oppsummering.

3.2 – Dokumentet og dets særegenheter

Begrepet «dokument» kan ha mange betydninger og tillegges mange forskjellige objekter. Dokumenter er for eksempel ikke utelukkende skriftlige kilder, men kan innta mange former og bestå av flere ulike medier. En tradisjonell oppfatning av et dokument er at det består av hovedsakelig tre sentrale deler; 1: Det er i fysisk format, altså noe du kan holde, for eksempel papir, 2: Det består av skriftlig informasjon, og 3: Det fungerer som bevis for enten en sannhet eller en usannhet. Denne dokumentoppfatningen er særlig fremtredende i forretningslivet eller når vi kontakter og samhandler med autoriteter (Windfeld Lund 2010), som for eksempel politikere og annet myndighetspersonell.

Med inntoget av teknologi og «new media» har denne oppfatningen blitt utfordret, og medført et dilemma særlig i henhold til dokumentets 1. sentrale del: Hvis noe blir skrevet og vist frem på en dataskjerm, er det da fortsatt et dokument? Niels Windfeld Lund skriver at det fysiske aspektet av et dokument ikke er en nødvendighet, og presenterer sin egen definisjon på hva et dokument kan være: «[…] any results of human efforts to tell, instruct, demonstrate, teach or produce a play, in short to document, by using some means in some ways» (Windfeld Lund 2010:743). På denne måten kan et dokument være nærmest hva som helst uavhengig av om det har sitt opphav i informasjonsteknologien eller andre steder. Nettopp derfor er det også essensielt å kunne klassifisere ulike dokumenter etter opphav, form og funksjon. Trine Syvertsen fremmer en rekke dimensjoner en kan ta i bruk når samtlige dokumenttyper skal kategoriseres, blant andre skrevne versus audiovisuelle dokumenter, publiserte versus upubliserte, offentlige versus ikke-offentlige, og offisielle versus private dokumenter (Syvertsen 1998).

I tilknytning til denne avhandlingen, er dokumentbegrepet mest nærliggende den tradisjonelle oppfatningen, og tilhører i all hovedsak kategorien for offisielle dokumenter. Alle kan

summeres opp i konseptet om «[…] written and true knowledge» (Windfeld Lund 2010:741) ettersom de er skrevet at kompetente aktører, som sikkerhetseksperter og departementer som, med sine rapporter, presenterer de ulike forhold i sentrale deler av samfunnet. Arbeidet med dokumentene kan karakteriseres av å være kvalitativt; det er innholdet og meningen med dokumentene som har vært av interesse. Helge Østbye *et al.* skriver at tre vesentlige aspekter må være til stede ved en analyse av kvalitative data: I første omgang må forskningsdata og analysen av denne forankres i overordnede problemstilling og teoretiske perspektiver. Deretter må innsamling og behandling av data foregå systematisk ved å kartlegge og stille spørsmål. Til slutt må relevansen dataene har til problemstillingen komme frem i lyset (Østbye mfl. 2007). Målet med kvalitative analyser er blant annet å komme frem til en helhetlig forståelse av spesifikke forhold, noe som forenes godt med dokumentanalysen av den offentlige utredningen *Digital sårbarhet - sikkert samfunn*, og de resterende dokumentene for øvrig.

3.3 – Dokumentanalyse

Dokumentanalyse innebefatter at man gjennomgår flere dokumenter for å finne svar på det man undersøker i forskningsprosjektet sitt. Dokumentene fungerer altså som «[…] *kilder eller ressurser i forskning om et sakstema* […]» (Østbye mfl. 2007:47). Dokumentene som har fungert som kilder i mitt forskningsprosjekt, har vært offentlige, og flere av dem har opphav i et regjeringsdepartement eller et utvalg nedsatt av et av departementene. Dokumentet som står i særskilt fokus i analysearbeidet er en offentlig utredning. Østbye *et al.* presiserer at selv om slike offentlige utredninger (og stortingsmeldinger) i prinsippet skal være nøytrale, må en alltid være klar over at det de presenterer ofte har en politisk hensikt, og kan være farget av utvalgets eller departementets egne ønsker (Østbye mfl. 2007).

I mitt analysearbeid har jeg først og fremst kartlagt alle leste dokumenter ved å skaffe en oversikt over dokumentets tittel, dokumentets publiserings- eller utgivelsesdato, dokumentets form (rapport, utredning, stortingsmelding og så videre), hvilken instans dokumentet er utarbeidet av, hvem dokumentet primært er ment for, og hvor det kan leses. I tillegg har jeg forsøkt å dra ut essensen av innholdet i hvert dokument, og skildre den med et par setninger for å gi et bilde av hvilket tema eller problematikk dokumentet omhandler. På grunn av det brede omfanget av NOU 2015: 13 *Digital sårbarhet - sikkert samfunn*, ble kun de mest sentrale deler og kapitler valgt ut og analysert. Dette vil gjøres rede for i påfølgende delkapittel, men aller først vil jeg kort greie ut om prosessen bak funnet av alle dokumentene.

3.4 – Innsamling av forskningsgrunnlag

Cybersikkerhet i norsk petroleumsindustri har, i datainnsamlingsprosessen, vist seg å være omfattet av en til dels høy grad av konfidensialitet. Det har vært svært vanskelig å komme frem til materiale som omhandler dette temaet spesifikt fordi dokumenter av slik karakter ikke er offentlig tilgjengelig. Dette vil nødvendigvis prege den helhetlige konkretiseringen av oppgavens problemstilling ettersom datagrunnlaget stort sett er basert på dokumenter som omhandler cybersikkerhet i samfunnet generelt, og ikke spesifikt i henhold til olje- og gassinstallasjonene i Norge. Arbeidsmetoden for funnet av disse dokumentene er skissert nedenfor.

Jeg startet i første omgang med et Google-søk på ord som «oljeindustri», «cybersikkerhet» og «infrastruktur» på både norsk og engelsk. I resultatlista kom det opp en del dokumenter som hadde risiko, cyberspace og sikkerhet til felles. Det som likevel viste seg å være mest fruktbart, var å gå direkte inn på nettsidene til organer som har en tilknytning til digital sikkerhet og olje- og gassektoren. Jeg gikk derfor innom: www.dnvgl.no (DNV GL), www.nsm.stat.no (Nasjonal sikkerhetsmyndighet), www.regjeringen.no (Regjeringen), www.ptil.no (Petroleumstilsynet), www.norsis.no (Norsk senter for informasjonssikring), www.npd.no (Oljedirektoratet), www.statoil.com (Statoil), og www.dsb.no (Direktoratet for samfunnssikkerhet og beredskap). Det var ikke på alle nettsidene at jeg fant frem til nyttige dokumenter.

På regjeringen sine nettsider, gikk jeg direkte inn på siden til tre relevante departementer; Forsvarsdepartementet, Olje- og energidepartementet, og Justis- og beredskapsdepartementet. Jeg gikk deretter til alternativet «Finn dokument», og skrev inn relevante søkeord i søkefeltet, som for eksempel «cyber», «olje» og «sikkerhet». Slik fant jeg fram til stortingsmeldinger og offentlige utredninger som omhandler noen av aspektene jeg tar for meg i min avhandling.

Som et ytterligere alternativ til å finne frem til relevant og nødvendig informasjon, sendte jeg 15.september en mail til fem instanser med en forespørsel om forslag til nyttige dokumenter som de kunne bistå meg i å få tak i. Instansene jeg kontaktet var Olje- og energidepartementet (OED), Forsvarsdepartementet (FD), Direktoratet for samfunnssikkerhet og beredskap (DSB), Petroleumstilsynet (Ptil) og Nasjonal sikkerhetsmyndighet (NSM). De eneste jeg fikk konkret respons fra var Petroleumstilsynet. Tilsynsorganet tipset meg om fem offentlige dokumenter som de mente var relevant i sammenheng med min problemstilling. Disse er:

- NOU 2015: 13 *Digital sårbarhet - sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden* (2015). Oslo: Utvalg v/Olav Lysne
- *Digitale Sårbarheter Olje & Gass* (2015). Stavanger: DNV GL
- *IKT-sikkerhet: Et felles ansvar* (2017). Oslo: Justis- og beredskapsdepartementet
- *Risiko i et trygt samfunn: Samfunnssikkerhet* (2016). Oslo: Justis- og beredskapsdepartementet
- *Helhetlig IKT-risikobilde 2016* (2016). Sandvika: NSM

Alle dokumenter kom til nytte, bortsett fra NSMs rapport *Helhetlig IKT-risikobilde 2016*. Jeg bestemte meg for å velge den bort ettersom jeg hadde lest deres risikorapport for 2017, og hadde med det mer oppdatert og aktuell informasjon som jeg kunne legge til grunn for mitt prosjekt.

Som en siste tilnærming til å finne relevante dokumenter, vurderte jeg å ta bruk den offentlige elektroniske postjournalen www.oep.no. Her kunne man foreta avanserte søk etter dokumenter man ønsket å lese ved å blant annet angi tidsperiode dokumentet skulle være fra, hvilken virksomhet det tilhørte, og lignende. Jeg oppdaget derimot at for å lese dokumentene, måtte man bestille innsyn, og det var usikkerheter rundt hvor lang tid det ville ta før jeg fikk innvilget dette, om jeg i det hele tatt fikk det. Jeg valgte derfor å gå bort fra denne måten å finne dokumenter på, og konsentrerte meg heller om den informasjonen jeg allerede hadde kommet frem til, noe som viste seg å være tilstrekkelig.

3.5 – Dokumentanalyse av *Digital sårbarhet - sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden*

3.5.1 – Utredningens form og funksjon

NOU står for «Norges offentlige utredninger», og benevner en samling rapporter som har som formål å kartlegge og drøfte bestemte forhold og problemområder i samfunnet. En vesentlig del av en NOU er også å foreslå mulige strategier eller videre veivalg innenfor det bestemte saksområdet. Utvalget som har utarbeidet utredningen består ofte av politisk uavhengige eksperter samt representanter fra ulike organisasjoner og næringsvirksomheter som er av relevans for saksområdet som blir utredet. Det er likevel hensiktsmessig å være inneforstått med at NOU-er først og fremst er et statlig anliggende, og kan ofte bære preg av konkrete politiske avveiinger, som nevnt tidligere.

NOU-en som er hovedfokuset i denne oppgaven heter *Digital sårbarhet - sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden*, og er skrevet av et utvalg ledet av Olav Lysne. Utvalget ble oppnevnt 20.juni 2014, og avga sin rapport til Justis- og beredskapsdepartementet (JD) 30.november 2015. Utredningen er nummer 13 av totalt 17 utredninger som kom ut i løpet av 2015. NOU 2015: 13 handler om hvordan Norge skal beskytte seg mot uønskede hendelser i det digitale rom. Forebyggende tiltak gjelder både individer, virksomheter, forvaltningen og samfunnet for øvrig. Det poengteres stadig at den økte digitaliseringen både har ført med seg effektivitet og forenkling i så vel private hjem som industri og næring, men også utfordringer og økt behov for beskyttende mekanismer og større kompetanse på IKT-området.

Vanligvis blir NOU-en grunnlag for en videre offentlig beslutningsprosess, og blir i første instans sendt ut på høring til berørte myndigheter, organisasjoner, næringsvirksomheter og andre aktører som blir sett på som særlig tilknyttet utredningens tema og funn. *Digital sårbarhet - sikkert samfunn* ble sendt på høring til en rekke instanser, og har også fått svar fra mange av disse. Oversikten over de involverte samt høringssvarene kan finnes på regjeringens nettsider.[1] Det er ikke hensiktsmessig for oppgavens overordnede tema å greie ut om responsen på utredningen fra alle parter. Det kan likevel nevnes at mange høringsinstanser som det er spesielt viktig å ta stilling til på bakgrunn av avhandlingens tema og *case*, er generelt positive til utvalgets anbefalinger og rapporten i helhet. Dette inkluderer blant andre: Norsk olje og gass (NOROG), Nasjonal sikkerhetsmyndighet (NSM), KraftCERT, Olje- og energidepartementet (OED) og Petroleumstilsynet (Ptil). På enkelte punkt presiserer disse instansene likevel alternative forslag til tiltak og/eller uenighet med utvalget. Ettersom det er utredningen selv, og ikke høringsuttalelsene som står i fokus i dette kapittelet, er det av hensyn til både tid og oppgavens omfang ikke relevant å presisere instansenes respons. I henhold til analysen, er det tilstrekkelig å påpeke at utredningen ble sendt ut på høring til relevante parter, slik det er forventet at den skal bli.

Etter høringen, blir NOU-en som oftest gjenstand for en politisk bearbeiding innad det departementet som har hatt det overordnede ansvaret for utredningen. Denne bearbeidingen kan så ende opp som en stortingsmelding som i sin tur danner det videre grunnlaget for Stortingets arbeid med det utredede saksområdet (Regjeringen, årstall ikke angitt, Hansen

[1] Regjeringen, https://www.regjeringen.no/no/dokumenter/horing--digital-sarbarhet--sikkert-samfunn-nou-201513/id2466319/?factbox=horingsbrev

2017). En ytterligere konsekvens av en NOU kan være en proposisjon til Stortinget der regjeringen fremmer forslag til ønskede vedtak, enten i form av stortingsvedtak, lovvedtak eller begge deler (Regjeringen, årstall ikke angitt).

Den utvidede sikkerhetsagendaen har fordret, både Norge og det internasjonale samfunnet for øvrig, til å rette et eget fokus mot cyberdomenet, som på mange måter har likhetstrekk med den tradisjonelle militære sfæren. Begreper som «cyberangrep», «cybermakt» og «cybervåpen» trekker konnotasjoner til konvensjonell krigføring der angrep, makt og våpen alle var viktige bestanddeler av sikkerhetspolitikken. Staten kan sågar innta funksjonen som referanseobjekt, og dersom befolkningen mister tilgangen til vitale goder som følge av at kritiske samfunnsfunksjoner er kompromitterte på grunn av cybersabotasje, vil det medfølge kraftige turbulente forhold, spesielt hvis de rammede funksjonene er utilgjengelige i lang tid. I henhold til Københavnerskolens sikkerhetiseringsteori, som kartlagt tidligere, har dagens teknologiske medier en naturlig plass i debatten om sikkerhet, noe også utredningsutvalget understøtter med sin rapport.

Grunnen til at NOU 2015: 13 er hovedfokuset for analysen er fordi den hjelper å se Norges arbeid på IKT-området i sammenheng ved å få en oversikt over hvilke samfunnsfunksjoner det blir lagt vekt på, hvilke styringsorganer som blir omtalt, og hvilke mangler og sårbarheter utvalget peker på som mest kritiske.

3.5.2 – Kartlegging av utredningen: Innsikt og oversikt

Utredningsutvalgets mandat var å greie ut om digitale sårbarheter i det norske samfunn og utfordringene disse fører med seg samt fremlegge forslag til tiltak innen bestemte plan og temaer (Digital sårbarhet - sikkert samfunn 2015). Grunnet et spesifisert fokus i avhandlingen, er det ikke alle deler av utredningen som er like relevante. Jeg har derfor gått frem som følger: Jeg tegnet opp to tabeller; én som beskriver alle kapitlene i utredningen kort, og én som tar for seg utelukkende de (del)kapitlene som jeg har definert som mest relevant for min problemstilling. Tabell nummer én heter «**Utredningens helhetlige komposisjon**». Tabell nummer to heter «**Utredningens særlig relevante deler**». Begge tabellene består av kolonner for **Kapittel, Overordnet tema/innhold** og **Merknader.** Sistnevnte tabell består også av en kolonne for **Begrunnelse** der jeg presenterer korte argumenter for hvorfor nettopp disse delene blir sett på som særs viktige i tilknytning til avhandlingens overordnede tema og problemstilling. Begge tabeller er å finne i vedlegg 2.

Del III *Sårbarheter i kritiske samfunnsfunksjoner* i utredningen består av kapitlene 11-23, og omhandler utvalgte samfunnsfunksjoner i Norge. Det er bare én slik funksjon som er relevant i avhandlingens tilfelle, nemlig kapittel 14 – **Olje og gass**. De andre funksjonene i form av elektronisk kommunikasjon, satellittbaserte tjenester, energiforsyning, vannforsyning, finansielle tjenester, helse og omsorg, og transport er derfor ikke nærmere omtalt i kapitteltabellen. Enkelte deler i noen av de nevnte funksjonene, spesielt innen energi- og vannforsyning, er riktignok relevante også for olje og gass, i hovedsak bruken av DKS (driftskontrollsystemer eller SCADA), men disse delene er ikke eksplisitt belyst som egne bestanddeler i noen av tabellene.

3.6 – Analyse av ni spefisikke tiltak

I utredningen presenterer utvalget, som tidligere nevnt, forebyggende tiltak for å bedre IKT-sikkerheten i Norge. Status på disse tiltakene blir fulgt opp og vurdert i stortingsmeldingen *IKT-sikkerhet – Et felles ansvar*, utarbeidet av Justis- og beredskapsdepartementet (JD) og lagt frem for Stortinget i desember 2016. Stortingsmeldingen kan sies å være en direkte konsekvens av NOU-en i henhold til den sedvanemessige prosessen Norges offentlige utredninger gjennomgår, som beskrevet i et tidligere avsnitt. Stortingsmeldinger legges gjerne frem av regjeringen slik at Stortinget kan diskutere en bestemt sak på prinsipielt grunnlag før arbeidet med en eventuell lovtekst påbegynnes (Østbye mfl. 2007).

JD skriver i innledningen til meldingen at statusoversikten vil bli brukt til å følge opp departementene i sivil sektor i det videre arbeidet med nasjonal IKT-sikkerhet, og at man ser et behov for en bred tilnærming til dette arbeidet fremover på grunn av at samme type (digitale) utfordringer er utbredt på tvers av ulike sektorer (IKT-sikkerhet 2017). Med grunnlag i dette utsagnet, fremgår det tydelig at også norske myndigheter aksepterer cyberspace som en naturlig del av sikkerhetsarbeidet.

I likhet med våpenarsenalet i den militære sektoren, har cybervåpen potensiale til å «[…] disrupt, destroy, and paralyze highly vulnerable communication, finance, or transportation systems» (Eun og Aßmann 2016:344). Sikkerhet i cyberspace er og bør være av vesentlig interesse for samfunnet på bakgrunn av den overordnede nasjonale sikkerheten og befolkningens velferd, en tankegang som både NOU-en og stortingsmeldingen opprettholder med sine anbefalte tiltak for å styrke IKT-sikkerheten og -forsvaret på tvers av sektorer.

Det vil bli for omfattende å gjengi progresjonen på alle tiltakene anbefalt av utredningsutvalget, men noen spesifikke oppfølginger kan med fordel kartlegges for å få en nærmere forståelse av hvordan NOU 2015: 13 har påvirket det politiske, organisatoriske og virksomhetssentrerte sikkerhetsarbeidet på IKT-feltet i tiden etter at utredningen ble offentliggjort.

I tabellen «**Utredningens særlig relevante deler**», har det blitt valgt ut spesifikke temaer med særskilt betydning for denne avhandlingen. Tre av disse er kapittel 14 – **Olje og gass**, kapittel 21 – **Avdekke og håndtere digitale angrep** og kapittel 23 – **Tverrsektorielle sårbarhetsreduserende tiltak**. Lysneutvalgets anbefalinger i disse kapitlene blir alle omtalt i Meld. St. 38, og for å få et bedre bilde av hvordan tiltakene har blitt fulgt opp eller ikke, har jeg valgt ut tre konkrete tiltaksforslag innen hvert kapittel, og forsøkt å finne resultatet av dem. Bakgrunnen for at nettopp de tre ovennevnte kapitlene og de tilhørende anbefalingene har blitt lagt til grunn for oversikten er at de henger godt sammen med avhandlingens utgangspunkt som tar for seg digitale angrep i norsk petroleumsnæring, og myndighetenes samt andre relevante aktørers forebyggende arbeid og ansvar innen IKT-sikkerhet. De resterende kapitlene og enhetene i tabellen inngår dessuten ikke i stortingsmeldingens oppfølging av anbefalingene til Lysneutvalget. En oversikt over Lysneutvalgets anbefalinger slik de står i NOU 2015: 13 og gjengitt i Meld. St. 38 samt status på området per våren 2018 basert på egne oppfølginger er lagt til i vedlegg 3, og kan brukes som navigeringsmidler i sammenheng med den mer inngående analysen presentert under.

Utviklingen av sikkerhetsbegrepet, har medført to sentrale oppfatninger som krever ekspertenes, beslutningstakernes og det offentliges oppmerksomhet og ressurser: Den ene omhandler individuelle systemer og nettverk, mens den andre fokuserer på kollektive og institusjonelle systemer, som blir utformet og påvirket av politiske og nasjonale sikkerhetsaktører. På samme måte som teknologiutviklingen under den kalde krigen bidro til å omforme samfunnets sikkerhetstankegang, har cyberspace gjort det samme: «Just as nuclear developments did in the past, cyber-weapons will ask us to revamp our policy and study of security, war, and power» (Eun og Aßmann 2016:356). Samfunnets og den samlede befolkningens verdier er i stor grad befestet i teknologiske systemer og enheter (Nissenbaum 2005), som ofte kan være sårbare for angrep fra det digitale rom. Mennesker med ansvar for implementeringen av sikkerheten vet at deres tiltak ikke nødvendigvis fører til et fullstendig beskyttet samfunn hver gang (Nissenbaum 2005), men de er også klar over at forebyggende sikkerhetstiltak vil fungere bedre enn fraværet av dem. Kraftige sabotasjeangrep fra en

cyberaktør mot fysisk infrastruktur kan eskalere utover det kompromitterte materialet, og få konsekvenser i den «virkelige» verdenen, både i form av skadeomfang, men også på det politiske plan på bakgrunn av den høye graden av anonymitet og misforståelser som eksisterer i cyberspace (Eun og Aßmann 2016).

Lysneutvalgets offentlige utredning og JDs påfølgende stortingsmelding viser at politiske og nasjonale sikkerhetsaktører former et institusjonelt nettverk som setter cybersikkerhet på den nasjonale sikkerhetsagendaen, og forsøker å bidra til å sikre det norske cyberdomenet til tross for dets mange verdikjeder, systemer og sårbarheter. Av de kritiske samfunnsfunksjonene som er omtalt i NOU-en, er det bare én av dem som er viktig i oppgavens kontekst: Norges petroleumsnæring.

3.6.1 – Anbefaling på området: IKT-sikkerhet

Konkretisering av tiltak: *Styrke IKT-sikkerheten på lik linje med HMS-kulturen*

Et digitalt sabotasjeangrep mot norske olje- og gassinstallasjoner kan få betydelige konsekvenser, noe som krever et høyt sikkerhetsnivå for hele næringen. JD skriver i *IKT-sikkerhet* at «Olje- og gassektoren har en lang sikkerhetstradisjon, en sterk sikkerhetskultur og høy kompetanse når det gjelder HMS. Denne gode sikkerhetstradisjonen bør videreføres til det digitale området» (2017:53). Som et tiltak til dette, har aktører i petroleumsnæringen, blant disse Petroleumstilsynet, utviklet en anbefalt praksis som skisserer standardiserte krav til IKT-sikkerhet for virksomheten med utgangspunkt i ISA/IEC-standardene. Standardisering bidrar til å forbedre teknologien, spare kostnader, og øke HMS-nivået i hele petroleumssektoren i tillegg til å forsikre at materiale, produkter og prosesser fungerer i henhold til sitt formål og bruksområde (Norsk olje og gass, årstall ikke angitt, ISO, årstall ikke angitt). Praksisen gir et rammeverk for hvordan olje- og gassnæringen kan bedre sikkerhetsnivået sitt med et særskilt fokus på operasjonsteknologi (OT).

OT er teknologien som styrer fysiske prosesser, og er av høy viktighetsgrad i de fleste industrier. Et angrep mot OT, kan forårsake at prosessene som styrer produksjonen og distribusjonen av olje og gass, blir forpurret, svekket eller manipulert til å utføre andre funksjoner enn de skal i utgangspunktet. Følgelig kan angrepet gi et utfall på materialiteten som petroleumsvirksomheten består av, og dermed yte stor skade, noe som utdypes senere i avhandlingen. Utarbeidelsen av den anbefalte praksisen for sikkerhetskrav i

petroleumsindustriens cyberdomene er et viktig sikkerhetiserende tiltak som bidrar til å øke bevisstheten rundt digitale sårbarheter i næringen.

3.6.2 – Anbefaling på området: Responsmiljø og prioritering av olje- og gassinstallasjoner i det forebyggende sikkerhetsarbeidet

To aspekter ved utformingen av cybersikkerheten i Norges petroleumsnæring er særlig fremtredende i kraft av sin relevans og behov. Det første aspektet er knyttet til olje- og gassektorens mangel på en formell prosedyre mellom sikkerhetsmyndighetene og selskapene for melding om digitale trusler. Det andre omhandler olje- og gassinstallasjonenes definisjon som kritisk infrastruktur.

Konkretisering av tiltak: *Vurdere tilknytning til et responsmiljø for petroleumssektoren, og igangsette en verdivurdering og klassifisering av petroleumsindustriens anlegg og IKT-systemer i forkant av revidert sikkerhetslov*

I sammenheng med det første aspektet, anbefaler utvalget av NOU 2015: 13 at «[…] virksomhetene i sektoren enten inngår et samarbeid med KraftCERT eller finner andre løsninger for operativt samarbeid» (Digital sårbarhet - sikkert samfunn 2015:158). KraftCERT er kraftbransjens egen responsgruppe for digitale nødsituasjoner. Etter å ha gått nærmere inn på statusen av denne anbefalingen, ser det ut til at petroleumssektoren ikke har inngått et medlemskap med KraftCERT. Omfanget av dette vil bli diskutert i påfølgende avhandlingskapittel. I nåværende omgang må det likevel nevnes at et felles kontaktpunkt for petroleumssektoren, enten i form av dens eget CERT eller i samarbeid med kraftbransjen, hadde hatt et stort potensial for å løfte det overordnede sikkerhetsnivået i hele virksomheten ettersom informasjonen og varslingen om truende cyberhendelser hadde nådd ut til flere av selskapene som opererer på norsk kontinentalsokkel, og sannsynligvis gjort det mulig å håndtere situasjonen raskere og mer effektivt enn i dag. Ved et sabotasjeangrep som kompromitterer store andeler av fysisk infrastruktur, er det avgjørende at instansene det gjelder får varsel om dette så tidlig som mulig.

Hva angår petroleumsinstallasjonene som kritisk infrastruktur, skriver utredningsutvalget følgende: «Ingen av olje- og gassinstallasjonene er per i dag definert som skjermingsverdige objekter i henhold til sikkerhetsloven» (Digital sårbarhet - sikkert samfunn 2015:157). I skrivende stund, avventes resultatet av en ny Lov om forebyggende sikkerhetstjeneste som, etter all formodning, vil implementere deler av Norges olje- og gassvirksomhet under sitt

lovgrunnlag (Pijnenburg Muller, Gjesvik og Friis 2018). Sammen med den nye sikkerhetsloven, følger også Forskrift om objektsikkerhet som pålegger virksomheter og departementer å utpeke objekter de mener kategoriseres som skjermingsverdige i henhold til sikkerhetsloven. Disse objektene vil da prioriteres av myndighetene i en eventuell krisesituasjon og i utformingen av sikkerhetspolitikken for øvrig. I påvente av den nye sikkerhetsloven, anbefaler utredningsutvalget at det igangsettes et arbeid innen verdivurdering og klassifikasjon av næringens anlegg og IKT-systemer (Digital sårbarhet - sikkert samfunn). Tilsynet har foreløpig ikke foretatt noen regelverksendringer ettersom den reviderte sikkerhetsloven fremdeles er under behandling (IKT-sikkerhet 2017). Effektene av olje- og gassanleggenes manglende definisjon som skjermingsverdige objekter vil bli utdypet ved en senere anledning.

Hvis sikkerhet betyr en verning om sentrale nasjonale verdier, er det høyst nødvendig å definere den norske petroleumssektoren som skjermingsverdig infrastruktur, spesielt på bakgrunn av tre årsaker: Cybersabotasje mot OT-en i petroleumssektoren vil i første omgang yte skade på kritiske nettverk og fysiske installasjoner. Dette vil ta lang tid å gjenopprette, og etter all sannsynlighet; medføre høye kostnader. Den andre årsaken er at som følge av at installasjonene slås ut av drift, må petroleumsproduksjonen stoppe i likhet med leveransene av olje og gass til Norges energikunder. Dette vil medføre betydelige økonomiske tap, og sette Norge i et dårlig lys på den internasjonale arena. En ytterligere, og kanskje den viktigste, årsaken for et ekstra høyt sikkerhetsnivå i petroleumsvirksomheten er risikoen for at mange mennesker kan omkomme – industriprosesser som spinner ut av kontroll på grunn av et datavirus eller andre former for materiell cybersabotasje vil ha enorme konsekvenser for liv og helse.

3.6.3 – Anbefaling på området: Håndtering av digitale angrep

Kapittel 21 i utredningen *Digital sårbarhet - sikkert samfunn* skisserer prosessene i tilknytning til avdekking og håndtering av IKT-kriminalitet, spionasje, sabotasje og terror. På grunn av den høye graden mistanke og usikkerhet cyberspace presenterer, er dette viktige og kompliserte emner i myndighetenes arbeid med digitale trusselaktører. Lysneutvalget skildrer de viktigste organene i forvaltningen av cyberdomenet i Norge, og greier ut om deres roller og ansvar. Det kommer frem at varslingen, rapporteringen, håndteringen og etterforskningen av cyberangrep involverer mange instanser på ulike samfunnsnivåer, noe som medfører vanskeligheter i tilknytning til arbeidet. Utvalget nevner blant annet: «Offentlige og private

virksomheter blir utsatt for alvorlige dataangrep og opplever usikkerhet og utilstrekkelig koordinering mellom myndighetsaktører som har ansvar for bekjempelsen av digitale angrep» (Digital sårbarhet - sikkert samfunn 2015:272).

Konkretisering av tiltak: *Etablere et helhetlig nasjonalt rammeverk for digital hendelseshåndtering*

Som et forebyggende sikkerhetstiltak på dette punktet, har utvalget foreslått etableringen av et helhetlig nasjonalt rammeverk for håndtering av digitale hendelser der innsatsen fra relevante aktører innenfor dette arbeidet er tydeliggjort (Digital sårbarhet - sikkert samfunn 2015, IKT-sikkerhet 2017). NSM fikk pålagt ansvaret for å utarbeide rammeverket, som per dags dato er ferdigstilt og lansert.[2] Tiltaket viser en konkret vilje til å simplifisere myndighetenes og sikkerhetsorganenes oppgaver innen cybersikkerhet. Ved uklare rammer, lange menneskelige verdikjeder og kompliserte krav og forventninger, er det av essensiell betydning for sikkerhetsarbeidet at samarbeidet disse instansene imellom er så sømløst og forståelig som mulig. Især ved et sabotasjeangrep på petroleumsvirksomheten, må nettverkene som har ansvaret for å ta hånd om situasjonen evne å samvirke og samhandle.

3.6.4 – Anbefaling på området: Etterretning

Aktørene som antas å ha de beste kapabilitetene og midlene for å være i stand til å gjennomføre store digitale sabotasjeangrep mot norske olje- og gassinstallasjoner, er fremmede stater. Statlig etterretning, sabotasje og spionasje er av like høy relevans i dag som det har vært gjennom hele sikkerhetspolitikkens historie. Med inntoget av digitale medier og internett, har slike operasjoner fått et cyberaspekt, og gjennomføres nå hyppigere og mer effektivt. Det er vanskelig å opprettholde den nødvendige mengden informasjon for å sikre seg mot slike operasjoner, og det er problematisk å definere gjerningspersonen etter et inntruffet angrep.

Norges Etterretningstjeneste (E-tjenesten) er det organet som har hovedansvaret for å underrette norske myndigheter om truende utenriks-, sikkerhets,- og forsvarspolitiske forhold. Trusler innen cyberdomenet er spesielt utfordrende, og utvalget av NOU-en skriver at «For å kunne oppdage, varsle og håndtere utenlandske trusler som terror, spionasje og digitale angrep trengs det ifølge Etterretningstjenesten å kunne følge med på relevant Internett-trafikk

[2] NSM, https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/rammeverk-hendelseshandtering/

som går via kabler (såkalt grenseforsvar)» (Digital sårbarhet - sikkert samfunn 2015:263). I dag har E-tjenesten «[…] liten eller ingen egen tilgang til informasjonen som flyter i kommunikasjonskablene» (IKT-sikkerhet 2017:31).

Konkretisering av tiltak: *Utrede innføringen av et digitalt grenseforsvar*

Som et tiltak til dette, ble det i 2016 satt ned et utvalg av Forsvarsdepartementet som utredet muligheten for å etablere et digitalt grenseforsvar (DGF) i Norge, på anmodning fra utredningsutvalget. En sentral problemstilling ved DGF er at kommunikasjonen mellom norske borgere som oppholder seg i Norge, også vil bli fanget opp av grenseforsvaret, i tillegg til informasjonen som krysser Norges landegrenser. Forslaget om innføringen av DGF er fremdeles under behandling (Regjeringen 2018), og det er per i dag uvisst hva resultatet av det vil bli.

Rapporten og den påfølgende behandlingsprosessen rundt DGF er et konkret resultat av *Digital sårbarhet - sikkert samfunn*, og belyser godt hvordan offentlige utredninger har en påvirkning på fremtidige beslutninger, og tilfanget av nye dokumenter. Slike organisatoriske nettverk er med på å utforme politikken rundt oss, og dersom DGF blir innført, vil det etter all sannsynlighet også har en viss innvirkning på våre liv og handlinger i cyberdomenet. E-tjenestens ønske om et DGF viser også hvordan sikkerhetspolitikken har utvidet seg til å omfatte andre sikkerhetsmetoder og -behov enn de som var relevant før cyberspace.

3.6.5 – Anbefaling på området: Deteksjon

Deteksjon er ofte altavgjørende ved alvorlige cybersabotasjer. Jo tidligere et forestående angrep er oppdaget, desto raskere kan det bli avverget. Nasjonal sikkerhetsmyndighet (NSM) drifter og videreutvikler varslingssystemet for digital infrastruktur (VDI) som er et inntrengningsdeteksjonssystem i form av sensornettverk, utplassert hos virksomheter som anses for å utgjøre den kritiske infrastrukturen i Norge (NSM 2014).

Konkretisering av tiltak: *Videreutvikle og oppgradere varslingssystemet for digital infrastruktur*

Lysneutvalget skriver at VDI-teknologien bør videreutvikles slik at tilstrekkelige deteksjonsmekanismer hos virksomhetene ivaretas (Digital sårbarhet - sikkert samfunn 2015). Justis- og beredskapsdepartementet skriver i sin stortingsmelding om IKT-sikkerhet at «Regjeringen ønsker å videreutvikle VDI for å styrke deteksjonsevnen i den enkelte sektor.

Sensorteknologien skal oppgraderes» (IKT-sikkerhet 2017:69). NSM fortsetter å være forvalter av varslingssystemet, og er sannsynligvis den instansen som er pålagt å implementere de nødvendige prosessene som regjeringen fremmer rundt VDI-nettverket. Antakelig er nettverket subjekt for både videreutvikling og oppgradering på en kontinuerlig basis. Hvilken rolle VDI spiller i den norske petroleumsnæringen vil bli omtalt i påfølgende kapittel.

3.6.6 – Anbefaling på området: Myndighetsansvar

Cyberspace er et ikke-territorielt domene, og brer seg utover hele samfunn og verden for øvrig. Derfor er også sikkerhetsarbeidet på dette området nødt til å være tverrsektorielt der samtlige enheter, næringer, tilsyn og virksomheter jobber sammen for å redusere den digitale sårbarheten på best mulig måte.

Konkretisering av tiltak: *Tydeliggjøre JDs rolle og ansvarsområde*

Utredningsutvalget av NOU-en påpeker at det er noen uklarheter rundt Justis- og beredskapsdepartementets rolle i sammenheng med IKT-sikkerhet i statsforvaltningen (Digital sårbarhet - sikkert samfunn 2015). JD har den generelle samordningsrollen for samfunnssikkerhet og beredskap, inkludert innen det digitale domenet. Utvalget foreslår å tydeliggjøre denne samordningsrollen ytterligere. I 2016 fremla JD stortingsmeldingen Meld. St. 10 (2016-2017) *Risiko i et trygt samfunn – Samfunnssikkerhet* der departementets roller og ansvar for samfunnssikkerhet i sivil sektor på nasjonalt nivå samt samordningsrollen innenfor samfunnssikkerhet og IKT-sikkerhet er presisert (IKT-sikkerhet 2017). Meld. St. 10 er en av de direkte følgene av den offentlige utredningen om digital sårbarhet i samfunnet, og markerer en nødvendighet for en avklaring av roller og myndighetsansvar for en effektiv håndtering av digitale angrep.

3.6.7 – Anbefaling på området: Digitale sårbarheter

Konkretisering av tiltak: *Utvikle en årlig helhetsoversikt over digitale sårbarheter*

Som et initiativ til å forbedre helhetsoversikten over samfunnets digitale sårbarheter, har NSM produsert risikorapporter som har blitt utgitt hvert år fra og med 2015. Lysneutvalget anbefalte i sin utredning om IKT-sikkerhet at JD ber NSM og Direktoratet for samfunnssikkerhet og beredskap (DSB), om å «[…] utarbeide et felles metodisk rammeverk i samarbeid som kan ligge til grunn for en helhetlig årlig oversikt over digital sårbarhet»

(Digital sårbarhet - sikkert samfunn 2015:292). Dette er et viktig arbeid i bekjempelsen av cybertrusler. Et tilstrekkelig kunnskapsgrunnlag om samfunnets tilstand, den geopolitiske konteksten, og medienes utviklingsmønster bidrar til å kartlegge de mest sannsynlige truslene som Norge står ovenfor. NSMs risikorapport for 2017 har for eksempel fremmet nyttig informasjon som har blitt lagt til grunn for denne avhandlingen. Lysneutvalgets anbefaling har dermed utvidet tilfanget av opplysninger og systematiserte oversikter over Norges helhetlige cybersikkerhet. DSB utvikler egne rapporter, i likhet med Politiets sikkerhetstjeneste (PST) og E-tjenesten.

3.6.8 – Anbefaling på området: Forebyggende sikkerhetsarbeid

«Utvalget anbefaler at Justis- og beredskapsdepartementet utarbeider et sett med minimumskrav til hvilke elementer som skal inkluderes i virksomhetsstyringssystemene, og det bør utarbeides veiledningsmateriell som kan øke kompetansen på området» (Digital sårbarhet - sikkert samfunn 2015:291). Anbefalingen er fremmet på bakgrunn av nødvendigheten for virksomhetene å integrere IKT-sikkerhet i sine styringssystemer, og å synliggjøre et sårbarhetsbilde av både tilsiktede og ikke-tilsiktede hendelser i disse systemene.

Konkretisering av tiltak: *Utarbeide veiledningsmateriell med spesifikasjoner rundt IKT-sikkerhet*

I løpet av 2017, har NSM arbeidet med en tiltakspakke som inneholder de viktigste minimumskravene for sikring av samfunnsviktige IKT-løsninger. Pakken heter *NSMs grunnprinsipper for IKT-sikkerhet*, og omhandler forebyggende sikkerhetstiltak for å beskytte private og offentlige virksomheters verdier og leveranser. Tiltakene er åpne for lesning på nett.[3] Det ser ut til at tiltakspakken kun er sentrert rundt IT- og IKT-sikkerhet, og omtaler ved flere anledninger aspekter knyttet til programvare, nettverk og informasjon. Av områdene virksomhetene skal sikre, nevnes kontoer, dataflyt, e-poster og nettlesere (NSMs grunnprinsipper for IKT-sikkerhet 2017). Det virker ikke som at OT er tatt like mye hensyn til som administrative nettverk.

IKT og informasjonssikkerhet er uten tvil viktige verdier som krever en høy beskyttelsesgrad, men OT og driftskontrollsystemer, ikke minst innen petroleumsnæringen, krever også robuste sikringsmekanismer da et angrep på disse systemene kan utøve større skade enn et angrep på

[3] NSM, https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

eksempelvis en nettside. DKS i olje- og gassindustrien og tilstanden på disse vil senere i avhandlingen bli omtalt ytterligere.

3.7 – Utredningens innflytelse på andre samfunnsinstanser

Som belyst i analysen over, har NOU 2015: 13 resultert i en rekke sikkerhetssentrerte dokumenter og initiativer tilknyttet IKT-sikkerheten i Norge. Blant disse er DNV GLs anbefalte praksis om standardiserte krav til IKT-sikkerhet i petroleumsnæringen, NSMs policydokument om grunnprinsipper for IKT-sikkerhet i virksomhetenes styringssystemer, Justis- og beredskapsdepartementets stortingsmelding *Risiko i et trygt samfunn* hvor departementets roller og ansvar blir presisert etter anmodning fra Lysneutvalget, fastsettelsen av rutinene for utarbeidelsen av årlige risikorapporter som NSM startet med i 2015, og den offentlige utredningen om innføring av digitalt grenseforsvar.

Utredningen har altså bidratt til at norske myndighetenes og andre sikkerhetsaktørers sikkerhetisering av cyberspace har fått et større omfang og et bredere nedslagsfelt. Tiltakene som har blitt analysert over er bare noen få av mange som har blitt presentert av utredningsutvalget, men de hjelper å danne et bilde av hvordan cybersikkerhet prioriteres i det norske samfunnet. Noen av anbefalingene er fremdeles under arbeid, blant annet i tilknytning til ny sikkerhetslov.

Digital sårbarhet - sikkert samfunn viser godt hvordan myndighetsprosesser fortoner seg i utarbeidelsen og implementeringen av digital sikkerhet, og belyser at sårbarheter i cyberspace kan inntreffe i så vel menneskelige verdikjeder som datanettverk. Hva angår fokuset på materialitet, kunne utredningsutvalget med fordel ha gått nærmere inn på dette temaet, og belyst flere sider av trusler som kan inntreffe i fysiske bestanddeler. Viktige momenter nevnes, ikke minst i tilknytning til driftskontrollsystemer, men andre aspekter ser ut til å være utelatt. En utdypelse av denne påstanden vil påfølge senere i oppgaven.

I tillegg til å iverksette nye sikkerhetstiltak i cyberdomenet, har Lysneutvalgets vurdering av tilstanden på IKT-sikkerhet i Norge vært medvirkende for utformingen av andre dokumenter og rapporter som omhandler samme viktige tema. Et av disse dokumentene er, som allerede vist, stortingsmeldingen *IKT-sikkerhet* fra Justis- og beredskapsdepartementet der anbefalingene fra utredningen *Digital sårbarhet - sikkert samfunn* blir fulgt opp. En annen stortingsmelding fra samme departement er *Risiko i et trygt samfunn* der blant annet departementets roller og ansvarsområde blir nærmere beskrevet. I tillegg tas det i meldingen

opp samfunnssikkerhet i helhet, og sentrale områder i arbeidet med samfunnssikkerhet blir gjennomgått, deriblant også digitale sårbarheter og IKT-sikkerhet. Meldingen skriver at den følger opp sentrale deler av NOU-en som er hovedfokuset i denne oppgaven, men poengterer at Justis- og beredskapsdepartementet vil i 2017 fremme en egen stortingsmelding om oppfølgingen av Lysneutvalgets anbefalinger (Risiko i et trygt samfunn 2016). Enkelte av de foreslåtte tiltakene som stortingsmeldingen fra 2017 gjennomgår har allerede blitt skissert her og trenger ikke å gjengis. *IKT-sikkerhet* er også den seneste (2017) stortingsmeldingen som tar opp Lysneutvalgets anbefalinger, og var derfor mer naturlig å holde et fokus på i stedet for meldingen fra 2016.

Andre dokumenter som benytter seg av informasjonen i NOU 2015: 13 er Utenriksdepartementets *Internasjonal cyberstrategi for Norge 2017* og forskningsrapporten fra NUPI (Norsk Utenrikspolitisk Institutt) *Cyber-weapons in International Politics – Possible sabotage against the Norwegian petroleum sector* fra 2018. Disse dokumentene bruker den offentlige utredningen hovedsakelig som et referansepunkt ved at de gjengir relevant informasjon fra utredningen i sine egne tekster. NOU-en fungerer altså som en kunnskapskilde for instanser som behandler samme tematikk, nemlig cybersikkerhet (eller IKT-sikkerhet, som dokumentene oftest benevner det som).

3.8 – Oppsummering

En kvalitativ analyses formål er å komme til bunns i spesifikke forhold og erverve en forståelse av disse. I dette arbeidet, kan vi benytte oss av en rekke tilnærminger, deriblant dokumentanalyse. Når vi analyserer dokumenter, må vi i første instans definere hvilken funksjon de skal ha i vår analyse. De kan enten være selve forskningsobjektet, eller de kan være ressurser for forskningen. I dokumentanalysen skissert ovenfor, har NOU-en fungert som en kilde til kunnskap om avhandlingens sakstema. Samme funksjon har også de øvrige dokumentene hatt (se vedlegg 1), men grunnet begrensninger på tid og oppgavens omfang, har ikke disse blitt analysert i like gjennomgående grad som dokumentet ovenfor. I stedet har dokumentene blitt tildelt konkrete opplysninger samt en kort oppsummering av overordnet tema.

Ved analysen av NOU-en, har jeg belyst konkrete deler og kapitler som har særlig relevans for avhandlingens *case*. Disse har blitt oppført i sine respektive tabeller i form av vedlegg. I tabell nummer én, «**Utredningens helhetlige komposisjon**», forsøker jeg å vise utredningens

overordnede tematikk, og hvilke aspekter innen digital sikkerhet utvalget har valgt å fokusere på. Tabell nummer to, «**Utredningens særlig relevante deler**», viser konkrete aspekter som kan knyttes tett opp mot oppgavens hovedtema. Denne tabellen viser tydelig hvorfor NOU-en har vært en sentral del i forståelsen av Norges digitale sikkerhet, og hvordan informasjonen her er fruktbar i avhandlingens gjennomgående røde tråd.

I analysen har jeg forsøkt å skape en delvis oversikt over hvilke tiltak utvalget av NOU-en har anbefalt, og status på gjennomføringen av disse per våren 2018. En oppsummering av alle anbefalte tiltak ville ha vært for omfattende, og jeg har dermed valgt ut ni av dem med utgangspunkt i de tre mest relevante kapitlene i utredningen: Kapittel 14 – **Olje og gass**, kapittel 21 – **Avdekke og håndtere digitale angrep**, og kapittel 23 – **Tverrsektorielle sårbarhetsreduserende tiltak**. Jeg har forsøkt å behandle de utvalgte anbefalingene i samsvar med Københavnerskolens begrep om utvidet sikkerhet og mediearkeologiens materialitetsaspekt samt nettverksarkeologiens konsept om nettverk for å poengtere hvordan dette henger sammen. Som et verktøy for analysen, har jeg også her brukt tabeller hvor anbefalingene innen hvert av kapitlene og status på dem er skildret. Disse ligger som vedlegg 3 sammen med de foregående tabellene.

Jeg har også pekt på hvilke andre dokumenter NOU-en har vært et grunnlag for. Ettersom saksgangen i myndighetsarbeidet med offentlige utredninger og følgene av dem, ofte er ganske omfattende, er det nærmest ikke mulig å få en fullstendig oversikt over hvilke andre aktører NOU-en har hatt innflytelse på, og hvilke andre dokumenter og eventuelle lovendringer den har resultert i.

Kartleggingen av de utvalgte tiltakene bidrar til å kaste lys over hvordan arbeidet med IKT-sikkerhet i det norske samfunn brer om seg, og om de ansvarlige som står bak implementeringen av denne sikkerheten tar Lysneutvalgets anbefalinger til etterretning. Dette er et viktig aspekt i forståelsen av myndighetenes arbeid innen sikring av petroleumsrelatert infrastruktur spesielt, og ikke minst viktighetsgraden en offentlig utredning har i relasjon til utviklingen og forbedringen av cybersikkerheten i Norge generelt.

Dokumentanalysen av NOU-en og de øvrige tekstene har tjent eksplisitte formål; den har vært en ressurs til kunnskap om forholdene i norsk cybersikkerhet i samfunnet, og petroleumsindustrien spesielt. Den har for det første vist hvilken prosess en offentlig utredning gjennomgår på myndighetsnivå, og hvilke andre arbeid og prosesser den

igangsetter, blant annet ved utarbeidelsen av stortingsmeldinger og proposisjoner. Mange medvirkende tar del i arbeidet, og også de som står utenfor regjering og Storting kan bli oppfordret eller inspirert til å skrive egne rapporter eller veiledninger innen temaet som utredningen tar opp. Det skapes med dette nettverk hvor aktører på tvers av samfunnssektorer bidrar til utviklingen av cybersikkerhet, og får dermed en innflytelse på Norges overordnede digitale hverdag i helhet.

For det andre, har dokumentanalysen bidratt til å konkretisere bestemt kunnskap slik at denne har kunnet brukes i resten av avhandlingen for øvrig. Analysen har gjort det mulig å skille opplysninger som er spesielt viktige for problemstillingen, og de opplysningene som ikke har vist seg å være like relevant. På grunn av dette har også det overordnede arbeidet med oppgaven blitt lettere og mer systematisert, og diskursen rundt materielle sider ved cyberdomenet innen den norske petroleumssektoren har kommet bedre frem i lyset.

4 – Norges petroleumsindustri i cyberspace

4.1 – Innledning

I arbeidet med å få et innblikk i myndighetenes forebyggende cybersikkerhetsarbeid i konteksten «norsk petroleumsrelatert infrastruktur», har det kommet frem mange interessante momenter. Hovedparten av datagrunnlaget har sin opprinnelse i utvalgte dokumenter. På grunn av tidsbegrensning i kombinasjon med et betydelig tilfelle av *the paradox of choice*, hvor store mengder informasjon har gjort det vanskelig å velge ut den viktigste, er naturligvis ikke all relevant litteratur lagt vekt på eller tatt i betraktning. Et ytterligere problemaspekt er at dokumenter og rapporter fra offentlig hold, især innad statsforvaltningen, genereres med høy frekvens, og revisjoner, avgjørelser og implementeringer foregår på en kontinuerlig basis. Cybersikkerhet i norsk petroleumsindustri er dessuten et meget ømfintlig tema, og dokumenter med eksplisitt og omfattende informasjon om dette må man være sikkerhetsklarert for å kunne få innsyn i.

Det overordnede målet med avhandlingen er å forsøke å holde et fokus på materialitet i henhold til mediearkeologien, og omtale cybersikkerhet på lik linje med andre former for sikkerhet som hører til i sine respektive sektorer fremsatt av Københavnerskolen. I samme instans, øker nettverk og sårbare digitale verdikjeder risikoen for tilsiktede angrep, noe som kan forbindes tett opp mot nettverksarkeologien og den omfattende sirkulasjonssamlingen av ulike samfunnsmessige aspekter, ikke minst tilknyttet myndigheter og beslutningstakere, som utformer hverdagen rundt oss. Materialitetsaspektet tilsier at jeg ikke greier ut om cyberhendelser som for eksempel spionasje og informasjonsinnhenting da dette ikke ligger på samme nivå som sabotasjeangrep mot fysisk infrastruktur. Etterretning kan riktignok være et ledd i gjennomføringen av slike angrep, men er ikke nevneverdig vektlagt i oppgaven som en cybertrussel i seg selv. Cyberspace er en grenseløs enhet, men for formålet med problemstillingen som har blitt satt, har denne enheten blitt snevret inn til å omfatte utelukkende angrep på materialitet.

Fakta som har vært sentrale for dette prosjektets problemstilling, og som blir utdypet i nåværende kapittel, er i hovedsak myndighetenes beslutninger, vedtak og helhetlige forebyggende sikkerhetsarbeid i det digitaliserte norske samfunn generelt samt den norske olje- og gassnæringen spesielt, den norske petroleumssektorens oppbygging og generelle

digitale sikkerhetsnivå, og konsekvensene av omfattende sabotasjeangrep fra cyberspace mot næringens fysiske infrastruktur.

Den generelle viktigheten og relevansen av cybersikkerhet i petroleumsvirksomheten har økt på bakgrunn av en rekke hendelser de siste årene. I 2012 ble oljeselskapet Saudi Aramco offer for et omfattende cyberangrep, utløst av en hackergruppe med politiske motiver. En skadelig programvare, *Shamoon*, infiserte 30 000 av selskapets datamaskiner, og slettet dokumenter, e-poster og andre filer. Skadevaren var målrettet mot raffineriene, og forårsaket systemene som styrer dem til å bli ustabile. Hovedmålet med angrepet var å stanse leveransene av olje og gass fullstendig, men Saudi Aramcos prosedyrer og sikkerhetsrutiner bidro til å forhindre dette (Stouffer mfl. 2015, Jørgenrud 2012, Helgesen 2013b, Perlroth 2012).

Også i Norge har man sett tendenser til økt fiendtlig cyberaktivitet i næringen. I 2011 ble norske olje-, gass- og forsvarsbedrifter angrepet av det som så ut til å være en APT – *advanced persistent threat* – det vil si meget sofistikerte cyberangrep. Nasjonal sikkerhetsmyndighet (NSM) sa den gang at minst 10 bedrifter var rammet av angrepene. Virusinfiserte e-poster, fordekt til å se ut som om de kom fra legitime kilder, ble sendt ut til spesielt utvalgt personell i de rammede virksomhetene. Brukernavn, passord, industritegninger og kontrakter var blant dataene som hadde blitt stjålet. NSM uttrykte at angrepet var første gang Norge hadde vært vitne til en så omfattende og vid form for digital spionasje (Greene 2011, Messmer 2011, BBC 2011).

Men denne påstanden ble overskygget i 2014 da NSM sendte ut en advarsel til så mange som 300 virksomheter i olje- og gassektoren, inkludert landets største oljeselskap, Statoil, om at de var et mål for et massivt cyberangrep. Også denne gangen var «legitime» e-poster med mistenkelige vedlegg opphavet til angrepet. NSM uttalte at hackerne hadde tilegnet seg nødvendig kunnskap på forhånd, og visste hvilke nøkkelpersoner de skulle gå etter (Munson 2014). Ifølge Norsk olje og gass (NOROG) var denne hendelsen av en særskilt karakter fordi 1: Angrepet hadde et massivt omfang, 2: Antall virksomheter som var angrepet var meget høyt, og 3: Det så ut til at det var en relativt avansert skadevare som var vedlagt e-postene (Digital sårbarhet - sikkert samfunn 2015), sannsynligvis ikke ulikt APT-en fra 2011.

Den overordnede diskursen rundt digital sikkerhet ser ut til å dreie seg i betydelig grad rundt «tradisjonelle» problemstillinger i en velkjent IKT-kontekst. Ikke ulikt de tradisjonelle tendensene innen medievitenskap, som i lang tid har sentrert rundt meningsinnhold, budskap

og retorikk, har diskusjonen omkring cybersikkerhet ofte fokus på informasjonssikkerhet, overvåkningsmekanismer og personvern. Dette er utvilsomt viktige emner ettersom informasjon og kunnskap er grunnlaget som hele vår verdensanskuelse er befestet i, men i konteksten av cyberspace, kan det være lett å glemme materialiteten som utgjør store deler av det femte krigføringsdomenet, og som dermed kan bli svekket, forpurret eller destruert.

På bakgrunn av dokumentanalysene i forbindelse med denne avhandlingen, virker det som at det er en mangel på en større vektlegging av operasjonsteknologi (OT), materialitet og industrielle kontrollsystemer (*industrial control systems* – ICS). Dessuten kan det se ut til at en inngående diskusjon rundt cybersikkerhet i Norge har brukt lang tid på å komme til overflaten hvis vi tar i betraktning at den første stortingsmeldingen som utelukkende omhandler IKT-sikkerhet ikke kom før 2017.[4] Meldingen har tittelen *IKT-sikkerhet – Et felles ansvar* og ble nærmere presentert i foregående kapittel. Den er utarbeidet av Justis- og beredskapsdepartementet (JD), og er tilgjengelig på regjeringens nettsider.[5]

Denne meldingen, sammen med flesteparten av dokumentene som har blitt lagt til grunn for dette prosjektet, skildrer Norges teknologiske hverdag på flere plan, det vil si; cybersikkerheten i samfunnet for øvrig. Ett kapittel i utredningen *Digital sårbarhet - sikkert samfunn* handler spesifikt om cybersikkerhet i olje- og gassnæringen. Kapittelet tar utgangspunkt i rapporten til DNV GL *Digitale Sårbarheter Olje & Gass.*

DNV GL er et selskap som arbeider med sikkerhet og rådgivning i en rekke industrisektorer, deriblant olje og gass. Rapporten som det her refereres til er utarbeidet av selskapet ved konsulent Pål Børre Kristoffersen spesielt for Lysneutvalgets utredning. Rapporten ble avgitt til utvalget 24.april 2015, og er fritt tilgjengelig på DNV GLs og regjeringens nettsider.[6] I den kartlegger DNV GL digitale sårbarheter, eksempelvis i form av angrep, sabotasje eller menneskelige feil samt utfordringer, blant andre manglende investeringsvilje i sikringstiltak og uklarheter i lovverk og tilsyn, som den norske olje- og gassektoren står ovenfor (Digitale Sårbarheter Olje & Gass 2015).

I løpet av min forskningsperiode ble det klart at opplysninger som omhandler min tematikk på et spesifikt plan ikke er offentlig tilgjengelige, noe som kan tilsi at informasjonen i DNV GLs

[4] Informasjonen er hentet fra et arrangement som presenterte funn fra forskningsprosjektet *Cybervåpen i internasjonal politikk.* NUPI, 27.februar 2018, Oslo
[5] Regjeringen, https://www.regjeringen.no/no/dokumenter/meld.-st.-38-20162017/id2555996/sec1?is=true&q=#match_0
[6] Regjeringen, https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

rapport ikke er fullstendig utfyllende. Gradert informasjon gjør at tilstanden på cybersikkerheten i norsk petroleumsnæring samt myndighetenes forebyggende arbeid på dette feltet ikke blir gjennomgående analysert i avhandlingen.

Dokumentene i forskningsmaterialet er grundige, men omhandler ikke cybersikkerhet på et inngående og dypere nivå. For eksempel sies det lite om den konkrete påvirkningen et cyberangrep kan ha på materialitet. Problematikken nevnes, blant annet i sammendraget av *Digital sårbarhet - sikkert samfunn*, ved at virksomhetenes utstyr, maskiner og infrastruktur kan angripes og bli delvis styrt av uvedkommende, men det sies ikke nok om utfallet av slike trusler og betydningen de kan ha for den overordnede samfunnssikkerheten. I utredningen blir SCADA-systemene og sårbarhetene ved dem påpekt, men ikke i like høy grad som sedvanemessig IKT-utstyr. Den største andelen av informasjonen rundt SCADA-nettverkene forekommer dessuten i kapitlene om vann- og energiforsyning, og ikke i tilstrekkelig grad i delen om olje og gass. En mulig grunn til det lavere fokuset på ICS, kan bunne i at angrep på internettilkoblede administrative nettverk har en høyere forekomst, og er lettere å gjennomføre enn cyberangrep på driftskontrollsystemer i industrien, noe som legitimerer en inngående og konkret debatt om slike nettverk.

Som en motvekt til et tilsynelatende høyt fokus på tradisjonell IKT-sikkerhet, ønsker jeg, ved hjelp av denne avhandlingen, å sette fokus på den manglende debatten omkring cyberangrep på materielle aspekter av samfunnet med utgangspunkt i Norges olje- og gassinstallasjoner. I det foregående har jeg presentert en dokumentanalyse av et av dokumentene som har stått sentralt i oppgaven; NOU 2015: 13 *Digital sårbarhet - sikkert samfunn*. I dette kapittelet, vil jeg gå nærmere inn på aspektene og innholdet av dokumentet, og drøfte disse i konteksten cyberangrep mot petroleumsrelatert infrastruktur og myndighetenes sikkerhetspolitikk som omfatter denne. Materielle sider av cyberdomenet vil bli belyst, i tillegg til hvordan konsekvensene av cybersabotasje mot disse kan påvirke petroleumsvirksomheten på norsk sokkel.

Dette kapittelet er strukturert som følger: I første omgang, vil jeg påminne om cyberdomenets militære karakter i henhold til Københavnerskolens sikkerhetiseringsteori. Deretter vil jeg gå nærmere inn på olje- og gassnæringens struktur og oppsett. Jeg vil så skissere en rekke aspekter i tilknytning til cyberdomenets materialitet og knyte disse opp mot hoveddokumentet som står sentralt i avhandlingen, NOU 2015: 13 *Digital sårbarhet - sikkert samfunn*. Jeg vil så drøfte petroleumsvirksomhetens status i henhold til to vesentlige momenter som ble presentert

i metodekapittelet; responsmiljø og sikkerhetsloven. Kapittelet konkluderes med noen siste resonnementer samt en kort oppsummering.

4.2 – Cyberspace i en sikkerhetisert kontekst: Et tilbakeblikk

Som det ble skissert innledningsvis i avhandlingen, karakteriseres cyberspace av tre lag: L3 – det kognitive, L2 – applikasjonslaget, og L1 – det materielle. Hvert av disse lagene kan bli offer for en tilsiktet uønsket hendelse, bedre kjent som *cyberangrep*. Disse angrepene utføres i sin tur av cyber*våpen*, som kan brukes til å *hacke*, trenge inn i, spionere på eller stjele konfidensiell informasjon fra ett eller flere systemer. Cybervåpen er i første omgang ondsinnet kode som bevisst blir spredt for å destruere eller forpurre konfidensialiteten, integriteten og tilgjengeligheten i bestemte datasystemer (Shackelford 2014). Tjenestenektangrep og løsepengevirus er to angrepsformer som har potensiale til å forårsake stor skade på kritisk infrastruktur og viktige samfunnsfunksjoner. Løsepengevirus kan sette hele virksomheter ut av drift i flere dager eller uker (Risiko 2017 2017). Kyndige aktører, især statlig støttede, har kompetanse til å utføre mange digitale angrep som kan få følger for et helt samfunn. Ikke minst gjelder dette angrep som har en direkte innflytelse på fysisk infrastruktur. Dette kan oppnås både ved hjelp av datavirus i kritiske industrielle prosesskontrollsystemer, men også som et *direkte* angrep på cyberdomenets materielle lag, for eksempel ved kutting av undersjøiske fiberoptiske kabler eller ødeleggelse av kommunikasjonsinfrastruktur og mobile lagringsenheter. Tap av liv, forpurring av produksjonsutstyr, og miljøødeleggelser er alle mulige utfall av cyberangrep.

Dette viser at cyberspace har mye til felles med den militære sektoren og tradisjonell sikkerhetspolitikk som bunner i grunntanken om å beskytte sentrale verdier. Som tidligere nevnt, har et eksplisitt fokus på cyberspace en bakgrunn i RMA (*revolution in military affairs*), som åpnet opp for å transformere både slagmarken og krigføringen for øvrig (Buzan og Hansen 2009). Fremskritt og forbedringer i teknologien bidro til å utvide den militære sektoren. Ikke minst, kan man trekke konnotasjoner fra cyberspace til atomvåpen som, i likhet med dagens digitale våpen, endret den sikkerhetspolitiske tankegangen. På samme måte som kjernefysiske våpen frembrakte et behov for nye, sikkerhetiserende grep, eksempelvis i form av traktaten for ikke-spredning av kjernefysiske våpen (*the Nuclear Non-Proliferation Treaty* – NPT) fra 1968 (Buzan og Hansen 2009), har cyberspace gjort det samme, som blant annet vist ved dokumentanalysen av NOU 2015: 13.

Nissenbaum fremstiller cybersikkerhet som noe som knyter «teknisk datasikkerhet», fra det vitenskapelig og tekniske feltet, sammen med tradisjonelle forestillinger om nasjonal sikkerhet fordi cybersikkerhet som oftest artikuleres av myndigheter, bedriftsledere og ledere av andre ikke-statlige sektorer (Nissenbaum 2005). Når myndigheter, sikkerhetseksperter, næringslivsledere og andre aktører utarbeider strategier, retningslinjer, handlingsplaner og *recommended practice*-dokumenter med et mål om å forebygge sabotasjeangrep fra det digitale rom, er dette tegn på en sikkerhetiseringsprosess på lik linje med for eksempel Utenriksdepartementets internasjonale cyberstrategi og Forsvarsdepartementets cyberretningslinjer fra norsk kontekst.

Slike institusjonelle grep kan minne om prosedyrene rundt konvensjonelle militære krigstrusler, og statenes opprustning og strategiutforming som et motsvar til slike trusler. Det som særlig under den kalde krigen var anerkjent som de mest presserende truslene mot en stat, har i dag fått en annen form, men krever fortsatt den samme graden beskyttelsesmekanismer. Og de sentrale verdiene er likeledes uendret. Slik har teknologinettverkene blitt bevart gjennom historien – hver «nyvinning» har egentlig vært en avart av det som kom før den. Mediearkeologien sier at det ikke finnes «nye» og «gamle» medier i deres historiske utvikling; de får bare nye bruksområder. Disse bruksområdene blir så omfattet av allerede etablerte rammer og betingelser, slik tilfellet er med institusjonaliseringen av sikkerhetiseringsteorien tilknyttet cyberspace.

Blant annet er NATOs anerkjennelse fra 2016 av cyberspace som det fjerde (eller femte, hvis verdensrommet blir tatt med i betraktningen) operative krigføringsdomenet (NATO Cyber Defence 2017), et tydelig tegn på hvor stor alvorlighetsgrad cybervåpen har fått for den overordnede sikkerhetspolitikken på den internasjonale arena. Konvensjonell krigføring er ikke lenger det eneste bekymringsmomentet, og i kombinasjon med våpen i det digitale rom, utvides trusselnivået og risikobildet: «Hybride trusler visker ut det tradisjonelle skillet mellom fred og krig […]» (IKT-sikkerhet 2017:11). Dette krever mer koordinasjon, samarbeid, og nytenkning, noe som ofte kan medføre vanskeligheter ettersom det som må prioriteres er «[…] usynlig, komplekst, grenseoverskridende, tverrsektorielt og som krever mye penger» (Nystrøm 2016). En prioritering av cybersikkerhet på lik linje med prioriteringen av tradisjonelle militærvåpen kan være et problematisk anliggende ettersom det alltid vil kretse usikkerheter rundt hvorvidt forebyggende sikkerhetstiltak i det digitale rom faktisk tjente sitt formål, eller om angrepet ville ha vært uunngåelig eller ikke-eksisterende uansett.

Ved vurderingen av slike problemstillinger, kan en trekke linjer til andre sikkerhetstrusler som debatteres i sikkerhetspolitikken, for eksempel terroranslag. Slike trusler kan få direkte konsekvenser for bebyggelse og infrastruktur, ikke ulikt følgene et massivt cyberangrep kan ha, og det er aldri fullverdig sikkert når og hvorvidt et slikt cyberangrep i det hele tatt vil inntreffe. Likevel bruker myndigheter og sikkerhetsaktører ressurser og midler på å sikre samfunnet mot slike trusler fordi – hvis et samfunn først står ovenfor den type konflikt – kan det ha fundamentale konsekvenser for menneskeliv, institusjoner, og samfunnets ideologiske verdier (Risiko i et trygt samfunn 2016). Samme mentalitet er også nødt til å være til stede i cyberdomenet.

4.3 – Petroleumssektorens struktur og virke

I den norske olje- og gassnæringen finnes det gode tegn på sikkerhetisering av cyberdomenet, eksempelvis med utviklingen av anbefalte retningslinjer for integrerte operasjoner med fokus på informasjonssikkerhet i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer, utgitt av interesse- og arbeidsgiverorganisasjonen Norsk olje og gass (NOROG).[7] NOROG arbeider også med standardisering for å forbedre teknologien, spare kostnader, og øke HMS-nivået i hele petroleumssektoren. Organisasjonen jobber i tillegg tett med andre kyndige instanser, deriblant den operative delen av Nasjonal sikkerhetsmyndighet (NSM); NorCERT og det statlige tilsynsorganet Petroleumstilsynet (Ptil). Andre sikkerhetiserende tiltak har også blitt iverksatt og gjennomført, som påvist i analysen av NOU 2015: 13 sammen med Meld. St. 38.

Allerede har tre viktige sikkerhetsorganer blitt nevnt; NOROG, NSM og Ptil. I tillegg til disse, består det norske samfunn generelt og den norske petroleumsnæringen spesielt av ytterligere nettverk i form av mennesker, beslutningstakere og statsforvaltere. Mange av disse spiller en vesentlig rolle i utformingen av sikkerhetspolitikken ved å fatte vedtak, utarbeide rapporter, skrive analyser, fastsette nødvendige rammer, og anbefale retningslinjer som virksomhetene i Norge må ta stilling til.

Slike omfattende verdikjeder kan være vanskelige å forholde seg til både når det gjelder å implementere riktige forebyggende sikkerhetstiltak på IKT, og når det står om håndteringen av et sabotasjeangrep mot viktig nasjonal infrastruktur, ikke minst i olje- og gassektoren der konsekvensene, i verste fall, kan være av eksistensiell art og spre seg til både miljøsektoren,

[7] Norsk olje og gass, https://www.norskoljeoggass.no/arbeidsliv/retningslinjer/integrerte-operasjoner/104-anbefalte-retningslinjer-krav-til-informasjonssikkerhetsniva-i-ikt-baserte-prosesskontroll--sikkerhets--og-stottesystemer-ny-revisjon-pr-05.12.2016/

økonomisektoren og den politiske sektoren. I en slik krisesituasjon må rollene og ansvarsfordelingen mellom de forskjellige sikkerhetsinstansene være avklart. Ikke minst må de berørte virksomhetene selv vite hvilke prosedyrer de skal iverksette for å kunne håndtere angrepet i henhold til krav, lovverk og kapasitet, og være i stand til å samvirke med hverandre. Utredningsutvalget av *Digital sårbarhet - sikkert samfunn* fremhever at det ligger hindringer for slike sømløse og åpne prosesser ved at det finnes «[…] uklarheter knyttet til roller og ansvar, en utilstrekkelig samarbeids- og delingskultur, manglende verktøy for utveksling av sensitiv og gradert informasjon» (Digital sårbarhet - sikkert samfunn 2015:261). Virksomhetene er ofte forvirrede rundt hvem de skal forholde seg til på myndighetssiden, og hvem de skal henvende seg til når de skal anmelde en uønsket tilsiktet cyberhendelse: «For virksomheter og leverandører er det ofte uklart hvem de skal forholde seg til på myndighetssiden. Utvalget er kjent med flere hendelser der det har vært usikkerhet knyttet til hvor man skal anmelde forholdet» (Digital sårbarhet - sikkert samfunn 2015:261).

Den norske petroleumsvirksomheten er statlig organisert med mange departementer, direktorater og tilsyn på ulike fagområder som til sammen utgjør politikken i og utviklingen av næringen. En presentasjon av noen av de viktigste kan være hensiktsmessig.

4.3.1 – Olje- og energidepartementet

Olje- og energidepartementet (OED) har det overordnede ansvaret for forvaltningen av petroleumsressursene på norsk sokkel, og forsikrer at petroleumsvirksomheten drives i henhold til de retningslinjene som Stortinget og regjeringen pålegger virksomheten. OED skal ha oversikt over risiko og sårbarhet innen sektoren. Dette gjelder også cybersikkerhet (Digital sårbarhet - sikkert samfunn 2015). I kraft av at OED har hovedansvaret for norsk petroleumsforvaltning, har departementet en del organer under seg, blant annet selskapene Petoro AS, Gassco AS, Statoil ASA, og forvaltningsorganet Oljedirektoratet (OD).

4.3.2 – Petroleumstilsynet

Petroleumstilsynet (Ptil) er et selvstendig, statlig tilsynsorgan underlagt Arbeids- og sosialdepartementet med myndighetsansvar for beredskap, sikkerhet og arbeidsmiljø i norsk petroleumsvirksomhet (Petroleumstilsynet, årstall ikke angitt). Tilsynet utvikler regelverk og fører tilsyn med selskapene som opererer på norsk kontinentalsokkel samt med åtte landanlegg og tilhørende rørledningssystem (Petroleumstilsynet, årstall ikke angitt). På bakgrunn av dette, skal Ptil være en vesentlig sikkerhetsaktør i den norske olje- og

gassnæringen. Dette utelukker ikke sikkerhet i cyberspace. I tilknytning problematikken nevnt ovenfor angående uklarheter og komplikasjoner rundt varsling og håndtering av digitale hendelser, er Ptil en av instansene som har opplevd å bli kritisert på bakgrunn av en slik hendelse i 2014. NSM sendte ut varsel til Ptil, som i sin tur formidlet meldingen om angrepet til de berørte bedriftene. I ettertid har tilsynet blitt kritisert for å ha gitt meldingen til feil personer, og at personer som burde ha blitt informert om den aktuelle hendelsen, ikke ble det (Digital sårbarhet - sikkert samfunn 2015). Dette tydeliggjør en uklarhet i varslingsprosedyrene innad petroleumsnæringen, noe som kan forverre en situasjon hvor infrastrukturen har blitt utsatt for cybersabotasje.

4.3.3 – Nasjonal sikkerhetsmyndighet

Ptil fikk varsel fra Nasjonal sikkerhetsmyndighet (NSM), som har det overordnede ansvaret for deteksjon, varsling og avverging av digitale hendelser i samtlige virksomheter og næringer. NSM er underlagt Forsvarsdepartementet (FD), og er det nasjonale fagmiljøet innen IKT-sikkerhet med særlig ansvar for varsling og koordinering ved alvorlige cyberangrep mot samfunnskritisk infrastruktur eller andre vesentlige samfunnsfunksjoner (Risiko i et trygt samfunn 2016). Fagmyndigheten gir råd og fører tilsyn, blant annet med sikring av nasjonalt viktig infrastruktur (Risiko 2017 2017). NSM har også ansvaret for VDI; et sensornettverk som fanger opp mulige datainnbrudd hos den aktuelle virksomheten, og sender så et varsel til NSM NorCERT. NorCERT koordinerer i sin tur responsen på det digitale innbruddet (NSM 2014). VDI ble første gang omtalt i analysen av NOU 2015: 13 under punktet «*3.6.5 – Anbefaling på området: Deteksjon*» (s.41). Dette nettverket er av stor relevans når truende cyberhendelser skal avdekkes og avverges. I petroleumsnæringen er dette av særskill betydning, noe jeg kommer tilbake til senere.

4.3.4 – Justis- og beredskapsdepartementet

Den hovedsakelige andelen av ansvaret for generell samfunnssikkerhet ligger hos Justis- og beredskapsdepartementet (JD). JD har en samordningsrolle for samfunnssikkerhet og beredskap i sivil sektor samt et samordningsansvar på IKT-sikkerhetsområdet. Departementet har også et overordnet ansvar for bekjempelsen av IKT-kriminalitet (Digital sårbarhet - sikkert samfunn 2015). JD fastsetter krav og anbefalinger på sikkerhetsområdet for de øvrige departementene som «[…] skal involvere Justis- og beredskapsdepartementet i prosesser hvor IKT-sikkerhetshensyn er av nasjonal betydning […]» (IKT-sikkerhet 2017:62).

Som nevnt i analysen av *Digital sårbarhet - sikkert samfunn* forelå det, på tidspunktet utredningen ble skrevet, noen uklarheter rundt JDs rolle i sammenheng med IKT-sikkerhet. Som et svar på dette, ble rollen presisert i stortingsmeldingen fra 2016 *Risiko i et trygt samfunn – Samfunnssikkerhet*. Meldingen er skrevet av Justis- og beredskapsdepartementet selv, og omhandler regjeringens arbeid og politikkutforming innen samfunnssikkerhet. Funksjoner, roller og ansvar i enheter som brann- og redningsetatene, Sivilforsvaret, politiet og kommunene er noen av emnene som blir belyst. Blant sentrale områder i arbeidet med samfunnssikkerhet er digitale sårbarheter og IKT-sikkerhet omtalt i et eget kapittel. *Risiko i et trygt samfunn* følger også opp deler av Lysneutvalgets anbefalinger fra NOU 2015: 13. I tilknytning til denne avhandlingen, ble meldingen tidligere nevnt i kapittelet om analysen av *Digital sårbarhet - sikkert samfunn.*

4.4 – Sårbarheter og trusler i cyberdomenets materielle lag

Den materielle dimensjonen av teknologiutviklingen og cyberspace for øvrig har ført med seg en rekke trusler som ikke var tilstedeværende før medienes tid. Disse truslene er i høy grad befestet i bruken av internett. Internett sammenkobler samtlige viktige samfunnsfunksjoner og gir større spillerom for sårbarheter og kriminelle cyberaktører som ønsker å utnytte dem.

Internett har blant annet blitt integrert i prosesskontrollsystemer som brukes i industrien, og har dermed økt risikoen for at systemene kan bli infisert av et datavirus via et åpent nettverk. Dette viruset kan i sin tur ødelegge fysisk produksjonsutstyr. Mulige angrep mot ICS kan involvere uautoriserte endringer i kommandoer, instruksjoner eller alarmer, som kan føre til at essensielt utstyr skades, deaktiveres eller slås av, miljøet blir negativt påvirket eller at menneskeliv havner i fare (Stouffer mfl. 2015).

4.4.1 – SCADA

I petroleumsnæringen brukes et system som heter SCADA. SCADA står for *Supervisory Control and Data Acquisition*, og er et nettverk som brukes til å styre og overvåke industrielle prosesser ved hjelp av elektriske, mekaniske eller hydrauliske funksjoner for å oppnå et resultat i tilknytning til blant annet produksjon og transport (Stouffer mfl. 2015). I tillegg til samfunnsfunksjonen olje og gass, benyttes SCADA på mange andre viktige områder som energi- og vannforsyning samt kontroll av tog- og flytrafikk, og er dermed en del av nasjonens kritiske infrastruktur som må bli beskyttet mot de mange truslene i cyberspace, ifølge et dokument utarbeidet av det amerikanske *President's Critical Infrastructure*

Protection Board og Energidepartementet (21 Steps to Improve Cyber Security of SCADA Networks 2002). Colin Williams går et steg videre, og hevder at slike former for industrielle kontrollsystemer kobler sammen alle verdens nasjoner i helhet: «[…] the great interconnectedness of everything encompasses ICS and SCADA systems and, therefore, the totality of the critical infrastructure of every nation on earth» (Williams 2014:382).

Mange vesentlige goder og funksjoner som samfunnet og menneskene i det er avhengig av, styres altså av vitale systemer som kan være sårbare for digitale angrep, og dermed føre til ødeleggelser i samfunnskritisk eller annen vesentlig infrastruktur. Stuxnet-angrepet fra 2010 er et direkte eksempel på et cyberangrep som forpurret betydningsfulle driftskontrollsystemer som deretter ga utslag på de fysiske bestanddelene i det iranske atomanlegget. Digital sabotasje mot petroleumsrelatert infrastruktur kan være en like stor trussel, men den har i stor grad vært oversett av politikere og næringslivsledere i Norge (NUPI, årstall ikke angitt). Den offentlige utredningen som er lagt til grunn for oppgaven skisserer en del vesentlige mangler og bekymringsmomenter ved SCADA-systemene som brukes i petroleumsnæringen, og som bør utforskes nærmere.

I utgangspunktet ble SCADA utarbeidet med en vektlegging på funksjonalitet og tilgjengelighet. Sikkerhetsaspektet ble ikke viet nevneverdig oppmerksomhet ettersom SCADA fungerte uavhengig av andre IKT-systemer, og hadde dermed ikke kontakt med omverdenen (Digital sårbarhet - sikkert samfunn 2015). Ytelsen og reliabiliteten i disse systemene er derfor relativt robust, men det svake sikkerhetsnivået gjør at nettverkene i høyere grad kan bli sårbare for forstyrrelser, prosessomdirigering, og manipulasjon av operasjonelle data (21 Steps to Improve Cyber Security of SCADA Networks). Når SCADA-systemene kobles opp mot administrative IKT-systemer samt internett, øker dette de digitale sårbarhetene, både i form av systemfeil, men også tilsiktet *hacking* (Digital sårbarhet - sikkert samfunn 2015). Andre utfordringer i SCADA-systemene er bruken av antivirusprogramvare eller systemer for overvåkning av datatrafikk da en slik bruk øker risikoen for at disse systemene forstyrrer, forsinker eller stopper lovlig og nødvendig datatrafikk. Et ytterligere svakt punkt med SCADA, er at det er kostbart, arbeids- og tidkrevende å oppgradere, noe som resulterer i at det fortsatt finnes sårbart utstyr i kritiske samfunnsfunksjoner (Digital sårbarhet - sikkert samfunn).

I petroleumsnæringen gjelder dette spesielt de eldre anleggene, der de industrielle kontrollsystemene som først ble anskaffet ikke var ment oppkoblet nettverk og integrert i

andre IT-systemer. «*Disse kontrollsystemene inneholder ikke det samme nivå av feiltoleranse og innebygget sikkerhet som nyere systemer*» (Digitale Sårbarheter Olje & Gass 2015:10). Dersom en utenforstående lykkes i å ta kontroll over vitalt produksjonsutstyr, kan dette resultere i miljøødeleggelse og i verste fall; tap av menneskeliv. Grunnet store mengder brann- og eksplosjonsfarlig materiale, et høyt antall personell på installasjonene, og store avstander fra land, gjør at olje- og gassektoren er spesielt utsatt for slike konsekvenser. Ikke minst, vil et cyberangrep på fysisk infrastruktur får negative følger for den økonomiske sektoren ettersom produksjonen må stoppes. Hvis produksjonen er ute av drift i lange tidsperioder, vil dette bety vesentlig tapte inntekter for næringslivet. Norges omdømme som en stabil produsent og transportør av energi vil også bli svekket (Digitale Sårbarheter Olje & Gass 2015). Samme problematikk påpekes i prosessene med elektrifisering, hvor petroleumsfeltene på sokkelen får sin kraftforsyning fra land. I tilfelle brudd på denne kraftforsyningen, må de fleste installasjoner stenge produksjonen. Distribusjonssystemene for elektrisk kraft er i høy grad åpne for cyberangrep ved at de er «[…] komplekse nettstrukturer med stor avhengighet til styring og kontrollsystemer» (Digitale Sårbarheter Olje & Gass 2015:1).

Også lange *cyber supply chains* medfører trusler når virksomhetene får sine digitale varer levert av utenlandske leverandører. Uoversiktlige verdikjeder som består av mange ledd, kan skape risikoer for de virksomhetene som er avhengige av digitale tjenester ved at sårbarhetene arves fra det ene leddet til det andre. For brukerne av disse tjenestene er det dermed vanskelig å holde oversikt over egne sårbarheter: «NSM mener det er en stor svakhet at IKT-løsningene i offentlig forvaltning er fragmenterte og at ansvaret er fordelt på mange aktører. […] Fragmenterte drifts- og forvaltningsmiljøer medfører økt kompleksitet og bidrar til unødige variasjoner på nettverk, systemer og tjenester» (Risiko 2017 2017:25-26). Vurderingen som sikkerhetsmyndigheten presenterer her, tilsier at verdikjedene, både de menneskelige og i cyberspace, øker risikoen for at en tilsiktet uønsket hendelse kan inntreffe, enten i produksjons- eller leveringsfasen av verdikjeden, eller når det ferdige produktet allerede har blitt tatt i bruk.

For kritisk infrastruktur som opererer med tungt maskineri tilkoblet internett og digitale løsninger, kan en slik hendelse få fatale følger. Ikke minst gjelder dette petroleumsindustrien, der norske olje- og gassinstallasjoner benytter underleverandører som har sitt utstyr og systemer i komplette pakker eller *moduler*. Slike moduler kan skape en sikkerhetstrussel ved at potensielle sårbarheter ikke er tilstrekkelig kartlagt på grunn av manglende dokumentasjon

(Digitale Sårbarheter Olje & Gass 2015). Dette kan medføre høye risikoer, ikke bare for industriens systemer og infrastruktur, men også for menneskeliv og samfunnet for øvrig.

Sikkerhetsmyndighetens sitat er hentet fra deres sårbarhetsanalyse *Risiko 2017: Risiko og sårbarheter i en ny tid – En vurdering av sårbarheter og risiko i Norge* som ble utgitt i 2017. Rapporten inngår i NSMs og en rekke andre sikkerhetsorganers praksis med å sette sammen årlige risikobilder. NSM har utgitt slike rapporter siden 2015, og fokuserer på risiko knyttet til cyberspace. Rapporten fra 2017 som det refereres til i denne avhandlingen kartlegger sannsynlige trusler mot Norge, blant andre spionasje, sabotasje og kriminalitet med økonomisk vinning som formål samt utfordringer som det norske samfunn møter i samsvar med den økte graden av digitalisering. Analysen er offentlig tilgjengelig på NSMs nettsider.[8] Ved begynnelsen på arbeidet med denne avhandlingen, var NSMs risikorapport fra 2017 den seneste rapporten tilgjengelig. Derfor er det også den som blir benyttet som kunnskapsgrunnlag. NSM utga en rapport for 2018 i mars.

For at et cyberangrep på kritiske nettverk og vitalt produksjonsutstyr faktisk blir igangsatt og uforstyrret gjennomført, må det kraftige midler til. Slike midler er i stor grad begrenset til fremmede stater eller statlig støttede aktører. For å kunne utnytte kjente sårbarheter i driftskontrollsystemene, er det en selvfølge å inneha nødvendig kunnskap om hvordan disse systemene opererer, hvilke funksjoner de er satt til å utføre, og eventuelt hvilke IKT-systemer og nettverk de er koblet opp mot. Innsikt i mediets funksjon blir dermed en vesentlig faktor her, og resonerer en velkjent mediearkeologisk tankegang. Lilly Pijnenburg Muller, Lars Gjesvik og Karsten Friis ved Norsk Utenrikspolitisk Institutt (NUPI) er inne på samme tankegang når de skriver i sin rapport *Cyber-weapons in International Politics* at det kreves inngående og omfattende kunnskap om både IT generelt, og de spesifikke industrielle prosessene og konfigurasjonene som styrer teknologien spesielt, for å kunne igangsette samt gjennomføre et digitalt angrep: «While an effective tool of sabotage, digital weapons also necessitate significant knowledge about industrial processes to be effective» (Pijnenburg Muller, Gjesvik og Friis 2018:23).

Det høye nivået av slik ekspertise gjør at muligheten for å kunne lansere et alvorlig cyberangrep, foreløpig, stort sett ligger hos et begrenset antall stater med «[…] expansive capabilities» (Pijnenburg Muller, Gjesvik og Friis 2018:19). Massive cyberangrep, særlig rettet mot kritisk nasjonal infrastruktur, utføres dermed som oftest av statlige aktører, i en

[8] NSM, https://nsm.stat.no/publikasjoner/rapporter/rapport-om-sikkerhetstilstanden/

geopolitisk kontekst. NSM skriver i sin risikorapport for 2017 at de mest alvorlige truslene mot digitale systemer i Norge sannsynligvis fremdeles vil komme fra Kina og Russland (Risiko 2017 2017). Russland er en særlig aktuell cyberaktør på grunn av landets historiske forhold til vesten. Som nevnt tidligere, kan Russlands posisjon, både geografisk og i verdenspolitikken, utrette trusler mot Norge, også i cyberdomenet. Nøyaktig hva disse truslene vil bestå i, kan en aldri vite med full sikkerhet, men at den norske petroleumsnæringen kan tjene som et ettertraktet mål virker å være et faktum.

NUPIs rapport *Cyber-weapons in International Politics – Possible sabotage against the Norwegian petroleum sector* har vært av essensiell betydning for innblikket i hvordan petroleumsvirksomheten i Norge kan bli berørt av alvorlige cyberangrep. Rapporten kom ut i 2018, og presenterer funn fra forskningsprosjektet *Digitale Sabotasjeangrep mot Norsk Petroleumssektor*. Rapporten kartlegger blant annet myndighetenes roller og ansvar, utfordringer i informasjonsdelingen mellom instanser, og drøfter aspektene rundt olje- og gassinstallasjonenes definisjon som CNI (*critical national infrastructure* – kritisk nasjonal infrastruktur). Dokumentet er en offentlig tilgjengelig publikasjon, og kan finnes på nettsidene til NUPI for dem som ikke har en papirutgave.[9]

Selv om eksepsjonelt teknisk kompetente, statlige aktører er de det knyttes mest bekymring til i sammenheng med alvorlig cybersabotasje, kan man ikke utelukke at digitale angrep også blir igangsatt av aktører uten noen tilknytning til statlige myndigheter eller omfattende kunnskap om de tekniske bestanddelene og funksjonene i innretningen som skal angripes. Muller, Gjesvik og Friis skriver i ovennevnte rapport at en rekke selskaper i Ukraina, inkludert kraftselskaper, ble gjenstand for flere cyberangrep i 2015. Aktørene bak angrepene kunne «[…] shut down production without having any specialized competencies as to the layout of the industrial systems» (Pijnenburg Muller, Gjesvik og Friis 2018:22). I NOU 2015: 13 *Digital sårbarhet - sikkert samfunn* kan man lese at informasjon om kritiske deler av et driftskontrollsystem finnes på internett, og at manualer og videoer om hvordan de ulike DKS-ene virker kan oppsøkes og lastes ned (Digital sårbarhet - sikkert samfunn 2015). Dette muliggjør at også ikke-eksperter kan påføre kritiske samfunnsfunksjoner store skader ved et potensielt digitalt angrep.

[9] NUPI, http://www.nupi.no/Publikasjoner/CRIStin-Pub/Cyber-weapons-in-International-Politics-Possible-sabotage-against-the-Norwegian-petroleum-sector

Til tross for at et cyberangrep mot Norges petroleumsrelaterte infrastruktur, i teorien, kan utføres av hvem som helst, er nok terskelen likevel lavest for statlige aktører med nødvendige kapabiliteter og kompetanse. Dessuten må den geopolitiske konteksten være av en slik art at norsk petroleumssektor er et legitimt og attraktivt mål for et digitalt sabotasjeangrep fra for eksempel russisk hold. Store sabotasjeangrep fra cyberspace mot materielle samfunnsaspekter er i stor grad avhengige av historiske og politiske forhold innad det internasjonale samfunnet, ikke ulikt tradisjonelle angrep innen militærsektoren.

Utgreiingen om SCADA i NOU 2015: 13 har en betydelig høyere tilstedeværelse i kapitlene om energi- og vannforsyning. Her skisseres både sårbarhetene i systemet og mulige utnyttelser av disse på en mer inngående måte enn tilfellet er i delen om olje og gass. Mesteparten av informasjonen om SCADA skissert ovenfor er tatt fra disse to kapitlene. Hva angår anbefalte tiltak, blir systemet indirekte nevnt i henhold til energiforsyning, for eksempel ved at koblinger mellom driftskontrollsystemer (DKS) og forretningssystemer blir stadig tettere og vanligere, og at det ikke lønner seg å jobbe imot denne utviklingen ettersom de forretnings- og styringsmessige gevinstene er for store (Digital sårbarhet - sikkert samfunn 2015). I stedet, foreslår utvalget at «[…] NVE bør kunne spille en viktig rolle i å formidle beste praksis og for øvrig veilede berørte virksomheter i sikker implementering» (Digital sårbarhet - sikkert samfunn 2015:144).

Innen vannforsyning, nevner Lysneutvalget at det bør «[…] utvikles kurs og studieretninger innenfor prosesstyring, systemintegrasjon og IKT […]» (Digital sårbarhet - sikkert samfunn 2015:166) for å bedre kompetansen på disse systemene.

Utvalget presenterer ingen tiltak i tilknytning til systemet i olje- og gassektoren. Anbefalingene omhandler en styrket kompetanse, responsmiljø for sektoren, bedre sikkerhetstradisjon innen IKT, regelverk samt en verdivurdering av IKT-systemer og anlegg (Digital sårbarhet - sikkert samfunn 2015), men direkte forbedringer i form av oppdatering og oppgradering av selve SCADA-systemet blir ikke anbefalt. Sannsynligvis blir ikke slike endringer ansett som gunstige på bakgrunn av de tidligere nevnte høye kostnadene og det lange tidsaspektet de vil medføre. Det er forståelig at myndighetene ikke ønsker å legge ned omfattende tid og ressurser på å videreutvikle driftskontrollsystemet, men heller øke sikkerhetsnivået på andre måter, eksempelvis med tilsyn og bredere kompetanse på systemstyring. Det er likevel interessant å bemerke at på tross av samtlige mangler i SCADA som utvalget selv nevner i utredningen, er det ingen anbefalinger på området i henhold til

petroleumsvirksomheten. Gamle anlegg er fremdeles i drift, og DKS-ene der har et lavere sikkerhetsnivå enn nyere systemer. Potensiell cybersabotasje mot et av disse anleggene kan dermed tenkes å utgjøre mer skade enn mot andre: «De eldste anlegg representerer en større digital trussel enn de nye» (Digitale Sårbarheter Olje & Gass 2015:10)

4.4.2 – Undersjøiske fiberoptiske kabler og rørledningssystemer

Sårbarheter i ICS er indirekte tilknyttet materialitet – et system blir infisert av et *malware* som i sin tur forpurrer fysiske prosesser. I det materielle laget av cyberspace, kan trusler forekomme i mer direkte forstand, for eksempel ved destruksjon av undersjøiske fiberoptiske kabler. Slike kabler er kritisk infrastruktur som muliggjør hele det globale nettverkssamfunnet som vi mennesker er omringet av (Starosielski 2015), og gir oss goder som internett, fjernsyn og telekommunikasjonssystemer.

Ved hjelp av kablene, knyttes land og kontinenter fysisk sammen, og ødeleggelse av disse kan potensielt ramme flerfoldige stater, og føre til konsekvenser innad store deler av det internasjonale samfunnet (Threats to Undersea Cable Communications 2017). I dag finnes det omtrent 16 transatlantiske kabelsystemer og 18 kabelsystemer som krysser Stillehavet, som alle enten er operasjonelle eller under utvikling. I alt finnes det over 250 separate undersjøiske kabelnettverk som allerede er funksjonelle eller under konstruksjon (Threats to Undersea Cable Communications 2017). Sendere og mottakere av informasjonen som flyter i disse nettverkene, vier ofte lite oppmerksomhet til hvordan informasjonen utveksles dem imellom – som regel er de bare opptatte av at informasjonen kommer uavbrutt frem, og til rett instans. Og dersom frykten for cybertrusler dukker opp, er det sjeldent det tas høyde for at fysiske ødeleggelser av kabelnettverket, har et mye større skadepotensial enn *hacking* og innhenting av konfidensiell og/eller privat informasjon: «Fortunately for actors wishing to disrupt cable systems, the public has a general lack of awareness of the scope and criticality of the vast array of submarine cable systems» (Threats to Undersea Cable Communications 2017:14).

Ødeleggelse av undersjøiske fiberoptiske kabler kan føre til utbredte konsekvenser, især hvis angrepet inntreffer ved et strategisk område, for eksempel Egypt, der et av verdens mest konsentrerte landepunkt for kabelnettverk befinner seg (Saffo 2013). Destruksjon av fiberoptiske kabelnettverk har allerede tatt sted, blant annet da en dykker skal ha kuttet en undersjøisk fiberoptisk kabel ved kysten av Alexandria i Egypt i 2013. Hendelsen førte til en 60% nedgang i internetthastigheten, og en 20 timer lang gjenoppretting av tjenestetilbydernes

nett (Threats to Undersea Cable Communications 2017, Al-Youm 2013). I dette tilfellet, var konsekvensene minimale, og i likhet med annen cybersabotasje – som blir utført nærmest utelukkende av statlige aktører med tilstrekkelige midler og politiske motiver – er sannsynligheten relativt liten for at sabotasje av undersjøiske kabelnettverk med et formål om å destruere flere lands kommunikasjons- og informasjonstilgang vil forekomme i nærmeste fremtid: «This is not an imminent possibility, as it would cause extraordinary economic harm that would outweigh any political benefits» (Starosielski 2015:13).

Norsk petroleumsindustri benytter i stor grad integrerte operasjoner (IO). IO handler om å integrere mennesker, organisasjoner, arbeidsprosesser og teknologi (IO Center, årstall ikke angitt) med et formål om å effektivisere og optimalisere produksjonen innad næringen. Et eksempel på integrerte operasjoner i olje- og gassindustrien er sanntidsoverføring av data fra brønn til land og sanntidsdeling av informasjon mellom personell offshore og personell onshore (Digital sårbarhet - sikkert samfunn 2015).

Datakommunikasjonen til oljeinstallasjonene som opererer på norsk kontinentalsokkel er primært basert på fiberoptisk kabling på havbunnen, og IO krever at kommunikasjonsnettene er oppe til enhver tid (Digital sårbarhet - sikkert samfunn 2015). Dersom et alvorlig angrep – digitalt eller annet – inntreffer på en plattform, er det av essensiell betydning at denne hendelsen blir kommunisert til relevante aktører uten forsinkelser eller komplikasjoner. I tillegg kan manglende kommunikasjon bety en nedstengning av produksjon på plattformer som opereres fra land eller fra naboplattformer (Digital sårbarhet - sikkert samfunn 2015).

NOU 2015: 13 skisserer ikke eksplisitt følgene det kan ha at de fiberoptiske kommunikasjons- og datanettene blir fysisk destruert. Utvalget skriver at for en bruk av felles kommunikasjonsløsninger, benyttes det ofte felles, delte datanett. Aspektene som presiseres i sammenheng med disse er følgende: «Slike nett kan være sårbare for avlytting, inntrenging og manglende tilgjengelighet, og kommunikasjonsenheter har operatørgrensesnitt som er sårbare. Et tjenestenektangrep på et lite ubeskyttet segment […] i et delt nettverk kan medføre at kritiske segmenter blir berørt» (Digital sårbarhet - sikkert samfunn 2015:152). Tjenestenektangrep (*denial of service* – DoS) igangsettes av cyberaktører for å begrense eller stanse normale og nødvendige tjenester. DoS-angrep kan dermed få konsekvenser for petroleumsvirksomheten, men har ikke relasjon til en direkte ødeleggelse av undersjøiske fiberoptiske kabler.

Angående dem, skriver Lysneutvalget: «Det har vært få skader på denne infrastrukturen, men i områder med grunt vann (15-20 meter) og mye havstrøm har det oppstått 5-6 skader i løpet av de siste 15 årene» (Digital sårbarhet - sikkert samfunn 2015:152) og: «Fiberoptiske kabler på havbunnen kan være utsatt for skade fra byggevirksomhet, fiskeriaktivitet og erosjon» (Digital sårbarhet - sikkert samfunn 2015:153). Utredningen peker dermed ut spionasje, datavirus og miljø- og samfunnsmessige konsekvenser som de truslene som kan ha en innvirkning på kabelnettverkene i Nordsjøen. Lysneutvalget skisserer kritiske konsekvenser som følge av slike trusler, blant annet produksjonsstopp og tap av konfidensiell informasjon, men kutting eller annen form for ødeleggelse av kablene i form av et tilsiktet angrep er ikke åpenlyst eksemplifisert som truende.

Tilfellet med dykkeren som kuttet en fiberoptisk kabel i Egypt tilsier at slik form for sabotasje verken krever den konkrete kompetansen om teknologien eller de omfattende midlene som er nødvendige for et angrep på ICS. På den ene siden, kan dette faktumet øke frykten for at fysisk destruksjon av fiberoptisk kabling kan inntreffe i den norske petroleumsvirksomheten, for eksempel fra en «miljøhacktivist». På den andre siden, har slike sabotasjeangrep en lav forekomst, som nevnt tidligere, og den norske petroleumssektoren har så langt heller ikke opplevd noe lignende. Dette kan være en mulig argumentasjon for at denne typen trussel ikke er tatt med i betraktningen når digitalisering og IO i olje- og gassindustrien blir analysert. På den annen side, er det viktig å være klar over alle sårbarheter, også dem som tilsynelatende er ikke-eksisterende i nåværende stund. Utredningen har pekt på noen betydningsfulle mangler og sårbarheter, men det materielle laget av cyberspace i form av undersjøisk fiberoptisk kabling kunne med fordel ha vært omtalt på en mer inngående måte for å vise alle sidene av potensiell cybersabotasje mot petroleumssektoren.

Infrastrukturen i petroleumsnæringen er omfattende, og består av mange fysiske bestanddeler. Blant disse er rørledningssystemene som transporterer olje og gass til Norges europeiske energikunder. Disse systemene inkluderer stigerør, prosessanlegg og mottaksterminaler. Utredningsutvalget skriver at: «Rørledninger er eksponert for sabotasje og ulykker, siden de i store områder ligger ubeskyttet. I tillegg påvirker automatiserings-, kontroll-, og sikkerhetssystemer selve flyten av hydrokarboner i rørene. Disse systemene kan også være sårbare» (Digital sårbarhet - sikkert samfunn 2015:153). I likhet med de fiberoptiske kablene, kan også rørene bli fysisk destruert ved et tilsiktet cyberangrep. Utredningen eksemplifiserer et slikt tilfelle med en eksplosjon i en rørledning i Tyrkia i 2008 der hackere utnyttet styringssystemet for ledningen, og forårsaket at trykket i ledningen økte uten at noen alarmer

detekterte dette eller at noen feilsignaler ble sendt til kontrollrommet (Digital sårbarhet - sikkert samfunn 2015). Igjen er denne typen angrep, i likhet med angrep på SCADA-nettverk, indirekte knyttet til materialitet, men det er ikke utenkelig at en ødeleggelse av rørledningene i seg selv også er mulig, på samme måte som en direkte ødeleggelse av undersjøiske fiberoptiske kabler.

4.4.3 – BYOD

Trusler i materialitetslaget til cyberspace forekommer ikke nødvendigvis utelukkende via sammensatt infrastruktur, nettverk og systemer. De materielle sidene av cyberspace inkluderer i minst like stor grad eksterne, bærbare enheter i form av mobiltelefoner, PC-er, nettbrett, USB-pinner, harddisker, ledninger og mye annet. Denne typen utstyr kan være åpen for en rekke sårbarheter som kan få konsekvenser for en hel virksomhet.

Mange sektorer opererer med begrepet *bring your own device*, forkortet BYOD. BYOD involverer de ansattes rett til å bruke sitt privateide utstyr i jobbsammenheng. Via dette, kan de ansatte få tilgang til sine daglige tjenester som e-post, kalenderfunksjoner og IP-telefoni (Digital sårbarhet - sikkert samfunn 2015). De kan også laste ned applikasjoner og spill og besøke ønskede nettsider. I utgangspunktet er konseptet rundt BYOD positivt for virksomhetene; de bruker en mindre andel av budsjettet på *hardware* og *software* samt vedlikeholdelsen av disse; produksjonseffektiviteten øker som følge av at de ansatte jobber raskere på sitt eget utstyr som de kjenner godt; og den overordnede tilfredsheten hos de ansatte blir større ved at de føler seg mer komfortable med å bruke private enheter (Evans 2015).

BYOD øker kraftig i omfang, og ifølge mørketallsundersøkelsen fra 2014 brukte ansatte i nesten 50% av virksomhetene privateide mobiltelefoner (Digital sårbarhet - sikkert samfunn 2015). Denne bruken av egne enheter på arbeidsplassen øker risikoene for at en uønsket hendelse inntreffer. Ondsinnet kode i et e-postvedlegg, modifiserte applikasjoner og utdatert *software* er alle trusler som BYOD presenterer brukerne og virksomheten. DNV GLs rapport *Digitale Sårbarheter Olje & Gass* poengterer at en av de 10 mest fremtredende truslene i olje- og gassektoren er mobile lagringsenheter (Digitale Sårbarheter Olje & Gass 2015). NOU 2015: 13, som har basert sitt kapittel om olje og gass på rapporten fra DNV GL, skriver: «Det åpnes vedlegg i e-post, det settes inn minnepinner, det lades mobiltelefoner, bærbare datamaskiner kobles til kritiske nett, og så videre. Mobiltelefoner kan også lett etablere

Internett-forbindelser. Brukere lures til å oppgi passord, med mer» (Digital sårbarhet - sikkert samfunn 2015:152). I tillegg nevnes risikoen for at utro tjenere med omfattende rettigheter og tilgang til betydningsfulle nettverk og prosesser kan påføre virksomheten stor skade.

Virksomhetenes sikkerhetspolicyer inkluderer i liten grad privat utstyr og er i stedet rettet mot utstyr som virksomhetene selv eier eller har kontroll over. En del av virksomhetene har utarbeidet policyer som omtaler privat utstyr tilknyttet virksomhetens IKT-systemer og nettverk (Digital sårbarhet - sikkert samfunn 2015). Hvordan tilstanden på dette området er i den norske petroleumssektoren er ikke presentert av utredningsutvalget, derfor er det vanskelig å få et bilde av hvilket sikkerhetsnivå selskapene har hva angår BYOD. En privat PC, infisert av et *malware*, tilkoblet arbeidsplassens nett kan potensielt få følger for hele virksomheten dersom konfidensiell informasjon, som for eksempel finansielle data, brukernavn, koder eller passord som gir tilgang til driftskontrollsystemene, blir stjålet. Sistnevnte aspekt kan få følger for produksjonsutstyret i virksomheten dersom cyberaktøren velger å utnytte dette. Lav regulering av eller utilstrekkelig oversikt over medbrakte bærbare innretninger gir cyberaktøren større spillerom. For eksempel ble Stuxnet i 2010 muliggjort ved hjelp av én enkel USB-pinne. «If not fully understood and regulated, it [BYOD] can threaten IT security and put a company's sensitive business systems at risk» (Evans 2015).

Utredningen har kartlagt truslene som i størst grad sentrerer rundt manipulasjon av *software* eller infiserte e-postvedlegg. Det som ser ut til å ha blitt utelatt, er risikoen for at en enhets *hardware* i seg selv blir negativt modifisert.

Hardware hacking kan gjøres for å få en enhet til å gjøre andre ting enn de den er ment for, det være seg å endre informasjonen som vises på skjermen eller få enheten til å sende signaler til en annen, med mer. Enhver aktør med fysisk tilgang til en virksomhetsansatts private PC kan få adgang til dataene i den, og infisere PC-en med en skadevare for å bedrive spionasje. En fullstendig kryptering av harddisken kan motvirke dette, men om krypteringen ikke er til stede, har «hardware hackeren» åpent spillerom for å modifisere PC-en: «It doesn't matter how good your password is because without encryption, the attacker can simply unscrew the case on your laptop, remove your hard disk, and access it from another computer» (Lee 2018).

Hackeren kan også modifisere dataene på selve harddisken og erstatte vesentlige programmer og funksjoner for så å sette disken tilbake på plass. Aktøren kan installere en

hardware keylogger for å holde oversikt over brukerens passord og andre tastetrykk. Ved å få tilgang til PC-en på et senere tidspunkt (eller ved å direkte stjele den), kan den ondsinnede aktøren finne informasjonen fra *keylogger*-en i maskinens internminne. Vedkommende kan også skifte ut vitale komponenter i PC-en, eksempelvis prosessoren, skjermkortet, nettverkskortet eller selve harddisken. Hackeren kan erstatte selve enheten med en annen som ser helt lik ut, men som har blitt modifisert uten brukerens viten (Lee 2018). Til slutt kan utstyr regelrett ødelegges slik at det ikke lenger er operativt.

Hardware hacking trenger selvsagt ikke utelukkende å gjelde BYOD; virksomhetenes eget utstyr og enheter kan også bli utsatt for fysiske destruksjoner, for eksempel av en utro tjener som allerede har et innpass i og adgang til virksomheten og dens innretninger. Men ettersom mange virksomheter ikke har policydokumenter som skisserer den nødvendige sikkerheten i de ansattes utstyr, er det større risiko for at det nettopp er dette utstyret som medfører flest sikkerhetshull og sårbarheter. For eksempel kan en ansatts PC være installert med en *hardware keylogger* som overvåker hvilke passord den ansatte skriver inn mens PC-en er tilkoblet virksomhetens nett.

Utredningen *Digital sårbarhet - sikkert samfunn* omtaler BYOD eksplisitt én gang, i et lite avsnitt tilknyttet «trender som påvirker sårbarhetsbildet» (punkt 6.4.3, s.49). Nøyaktig hvordan denne praksisen kan være truende for en virksomhet, blir ikke kartlagt. I kapittelet med fokus på olje og gass, blir praksisen indirekte omtalt ved at «[…] det settes inn minnepinner, det lades mobiltelefoner, bærbare datamaskiner kobles til kritiske nett […]» (Digital sårbarhet - sikkert samfunn 2015:152), som nevnt tidligere. Det materielle aspektet av cyberspace virker, i denne sammenhengen, ikke nevneverdig til stede i utredningens uttalelser. En mer konkretisert og utdypende analyse av hvilke konsekvenser materielle skader ved BYOD kan påvirke den norske olje- og gassektoren hadde vært et nyttig supplement til utredningens helhetlige oversikt over digitale sårbarheter.

4.4.4 – Satellittbasert navigasjon

Olje- og gassvirksomheten er i høy grad avhengig av satellittbaserte tjenester. «Satellittbaserte navigasjons- og posisjoneringstjenester er kritiske innsatsfaktorer for utvinning av olje og gass på norsk sokkel» står det i sårbarhetsrapporten til Norsk Romsenter fra 2013 (Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur 2013:18).

Satellittbasert navigasjon benyttes i sikkerhetssystemer for forebygging av ulykker og miljøskader samt for dynamisk posisjonering (DP) av fartøyer og produksjonsinnretninger. DP-systemer brukes for å holde skip i én bestemt posisjon eller på en programmert rute i en konstant retning. Systemene anvender satellittnavigasjon via GPS og GLONASS som et referansesystem for nøyaktig dynamisk posisjonering. Andre verktøy som blant andre vind-, strøm-, og bølgesensorer, treghetsnavigasjon og laser benyttes som støtte- og reservesystemer. Informasjonen fra disse sensorsystemene blir kontinuerlig overført til datamaskiner som i sin tur beregner nødvendig ytelse for å posisjonere fartøyet med tilstrekkelig nøyaktighet og i henhold til kravene for spesifikke operasjoner (Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur 2013).

DP gjør mange operasjoner på norsk sokkel mulig, deriblant kartlegging av energiressurser, nedlegging av oljerørledninger, boring av produksjonsbrønner, vedlikeholdsdrift, og selve olje- og gassproduksjonen. Borerigger og -skip, forsyningsfartøyer og spesialfartøyer for seismiske undersøkelser er blant anvendelsesområdene som DP inngår i (Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur 2013).

Utredningsutvalgets omtale av satellittbaserte tjenester blir presentert i et eget kapittel i *Digital sårbarhet - sikkert samfunn*. Her blir også mulige trusler og sårbarheter belyst. På bakgrunn av at satellittsystemer får en stadig større betydning for kritiske samfunnsområder som luftfart, sivil beredskap, og Forsvarsaktiviteter, poengterer utvalget at det er naturlig at «[…] disse systemene vil kunne være et mål for fiendtlige angrep, både i form av angrep mot fysisk infrastruktur og i form av cyberangrep mot styrings- og driftssystemer» (Digital sårbarhet - sikkert samfunn 2015:123).

Her kan det argumenteres for at utvalgets bruk av ordet «cyberangrep» også kunne ha stått i sammenheng med angrep mot fysisk infrastruktur, og ikke utelukkende i tilknytning til styrings- og driftssystemer. Signaler fra de tidligere nevnte GPS og GLONASS mottas av bakkestasjoner – eller GNSS-stasjoner (Global Navigation Satellite System) – som bruker data fra satellittene til blant annet jordobservasjon, bestemmelse av landheving, oppmåling av eiendom, anleggsdrift, værvarsling, overvåking av romvær, og ikke minst; overvåking av oljeplattformer (Kartverket 2017). Fysiske installasjoner, som disse GNSS-stasjonene, knyttet til romvirksomhet som leverer digitale satellittbaserte tjenester til samfunnet og verden for øvrig inngår i den omfattende infrastrukturen av cyberspace. I likhet med fiberoptiske kabler,

PC-er, mobiltelefoner og andre håndgripelige enheter, kan nettverket av basestasjoner som mottar GPS-signaler inkluderes i cyberdomenets materielle lag.

Det kan være komplisert å forholde seg til terminologien rundt cyberspace, og måten vi omtaler ulike angrep eller hendelser på avhenger av hvilken diskurs vi fører. I Forsvarsdepartementets dokument *FDs cyberretningslinjer*, blir cyberangrep definert slik: «Handlinger i eller gjennom cyberdomenet med hensikt å skade eller påvirke personell, materiell eller konfidensialiteten, integriteten, tilgjengeligheten eller autentisiteten til et informasjonssystem» (2014:21). Her har departementet med rette inkludert handlinger som kan gjennomføres enten i selve cyberdomenet eller ved hjelp av det, og være rettet mot materielle bestanddeler. Dersom Lysneutvalget hadde omtalt angrep på romrelatert infrastruktur i en lukket cyberkontekst, hadde det vært hensiktsmessig å endre ordlyden i avsnittet om cyberangrep mot satellittsystemer slik at materialitetsaspektet ved slike angrep kom tydeligere frem. Dersom konteksten er væpnede militære handlinger i en tradisjonell forståelse av sikkerhets- og forsvarspolitikk, er det etter all sannsynlighet ikke like relevant å benytte seg av prefikset «cyber», selv om cyberspace og militærmakt henger nært sammen. Det kan antas at utredningsutvalget støtter seg mer mot det siste alternativet.

Utvalget nevner andre tilsiktede hendelser i form av signalblokkering som eksempelvis kan forårsakes av støysending, utsending av falske signaler og retransmisjon av forsinket signal, og poengterer at satellittnavigasjonssignaler i utgangspunktet lett kan bli forstyrret av en sterkere støysending (Digital sårbarhet - sikkert samfunn 2015). Ved et plutselig tap av GPS-signaler i petroleumssektoren, kan det oppstå en kompleks situasjon som vil kreve at navigatøren skaffer seg en oversikt over hvordan de ulike typene av navigasjonsutstyr er påvirket, og hva som kan gjøres for å styre den videre navigasjonen (Digital sårbarhet - sikkert samfunn 2015). Av mulige utfall som følge av en uønsket hendelse i DP-systemet nevnes dette: «En kollisjon mellom en plattform og for eksempel et forsyningsfartøy eller en flytende boligplattform kan få alvorlige konsekvenser» (Digital sårbarhet - sikkert samfunn 2015:155). Det er med dette åpenlyst at forstyrrelser av satellittbaserte tjenester i petroleumsvirksomheten kan ha alvorlige konsekvenser for fysisk infrastruktur, men utvalget går ikke nærmere inn på dette emnet i sammenheng med materielle hendelser og utfall.

4.5 – Petroleumssektorens digitale sikkerhetsnivå

4.5.1 – Sektorens kritikalitet

DNV GLs rapport om digitale sårbarheter i petroleumsvirksomheten sier at norske etterretningsmyndigheter advarer om en økning i cyberangrep mot Norges industri, og at en rekke hendelser har vist at energi- og petroleumssektoren er blant de mest utsatte (Digitale Sårbarheter Olje & Gass 2015). Den norske petroleumsnæringen består av lange verdikjeder; fra utvinning av hydrokarboner og omdannelsen av disse til olje- og gassprodukter, til aspekter som salg, markedsføring, foredling, transport, forskning, myndighetsrapportering, og annet (Digitale Sårbarheter Olje & Gass 2015). På den materielle siden, står det en omfattende infrastruktur hvorav produksjonsplattformer, raffinerier, rørledninger og skipningsterminaler er de mest kritiske (Digital sårbarhet - sikkert samfunn 2015).

Disse bestanddelene kan alle bli påvirket i en eller annen form grunnet digitale sårbarheter i olje- og gassektoren. Blant de mest sentrale sårbarhetene som blir presentert i rapporten til DNV GL er utdaterte styresystemer på installasjonene, mangelen på separasjon av datanett, datanett mellom landinstallasjoner og oljefelt samt de tidligere nevnte mobile lagringsenhetene (Digitale Sårbarheter Olje & Gass 2015). Blant de fire leddene leting, feltutvikling, produksjon og transport (Digitale Sårbarheter Olje & Gass 2015), er det sannsynligvis spesielt i produksjonsfasen at konsekvensene av et sabotasjeangrep fra cyberdomenet potensielt kan få flest kritiske ringvirkninger, ikke bare for de resterende leddene i verdikjeden, men også for andre aspekter av industrien og det øvrige samfunnet. Alle de ovennevnte formene for trusler og sikkerhetshull knyttet til SCADA-systemer, fiberoptiske undersjøiske kabler, BYOD og satellittbaserte navigasjonssystemer er til stede i produksjonsleddet.

I de nasjonale myndighetenes sikkerhetiseringsarbeid av cyberspace innen olje og gass er det uten tvil tatt mange steg i riktig retning, ikke minst ved satsingen på å styrke Petroleumstilsynets kompetanse på digital sikkerhet samt tilsynets finansiering av rapporten *Digitalisering i petroleumsnæringen: Utviklingstrender, kunnskap og forslag til tiltak*,[11] der hovedfokuset er effektene av digitalisering for helse, miljø og sikkerhet i petroleumssektoren. Til tross for dette, fremhever utredningsutvalget av *Digital sårbarhet - sikkert samfunn* en

[11] IRIS, http://www.ptil.no/getfile.php/1348080/Tilsyn%20p%C3%A5%20nettet/tilsynrapporter%20pdf/Rapport%20IRIS%202018-001_Digitalisering%20i%20petroleumsn%C3%A6ringen_final.pdf

oppfatning om at «[…] dagens sikkerhets- og tilsynsregime gitt med hjemmel i petroleumsloven er for svakt med tanke på den viktigheten anlegg på norsk sokkel har for norsk økonomisk bæreevne og for Norges internasjonale betydning og omdømme som olje- og gassleverandør» (Digital sårbarhet - sikkert samfunn 2015:156). Petroleumsvirksomheten i Norge må kunne regnes som en av landets viktigste verdier, og den komplekse infrastrukturen som næringen består av bør kreve et like høyt sikkerhetsnivå som for eksempel finans- eller helsesektoren. «Utvalget mener at anlegg på norsk sokkel har betydning for vitale samfunnsinteresser og rikets sikkerhet» (Digital sårbarhet - sikkert samfunn 2015:157), og utelukker ikke risikoen for at alvorlige hendelser kan inntreffe. «Alvorlige hendelser» må også kunne inkludere tilfeller i form av cyberangrep på eller via materielle installasjoner relatert til petroleumssektorens funksjonalitet.

4.5.2 – CERT

Det fremstår derfor som noe unaturlig at petroleumssektoren verken har en fastsatt prosedyre for varsling om digitale trusler eller sin egen responsfunksjon i form av et CERT (Computer Emergency Response Team) (Digital sårbarhet - sikkert samfunn 2015), som påpekt i forrige kapittel. CERT er en beredskapsgruppe med ekspertkompetanse på håndteringen av cybertrusler i alle former, og arbeider med å forhindre og minske cyberangrep der de inntreffer ved å gjenopprette normalsituasjonen så effektivt som mulig samt forebygge fremtidige angrep (Technopedia, årstall ikke angitt). I motsetning til andre samfunnssektorer, eksempelvis kraftsektoren og de allerede nevnte finans- og helsesektoren, har ikke olje- og gassindustrien i Norge sin egen CERT-funksjon. Sektorvise CERT-er konsentrerer sitt arbeid innenfor sin respektive sektor. En slik ordning er hensiktsmessig ved at en potensiell krisesituasjon med opphav i cyberdomenet kan håndteres av en ekspertgruppe med den nødvendige innsikten i problematikken som har oppstått, kombinert med kunnskap om sitt sektorsentrerte fagområde. På denne måten kan cyberangrepet løses på et mer målrettet og konsentrert vis.

Stortingsmeldingen *IKT-sikkerhet – Et felles ansvar* poengterer at petroleumsnæringen har varslingssystemet PISAS (Petroleum Industry Security Alert System) som eies av NOROG, men det fremgår ikke videre hvilke hendelser dette systemet er innrettet mot. I *Retningslinjer for samarbeid ved fare- og ulykkessituasjoner i petroleumsvirksomheten* skrevet av den norske redningstjenesten blir varslingssystemet nevnt én gang under «særskilte varslingsprosedyrer» i forbindelse med beredskapssituasjoner som involverer bombetrusler,

terror eller annen alvorlig kriminalitet (2013). Det kommer ikke tydelig frem hva som menes med «annen alvorlig kriminalitet», og om cybertrusler alternativt inngår her. Mer omfattende og konkretiserte opplysninger om PISAS har vært vanskelig å oppdrive i løpet av forskningsperioden.

De store selskapene på norsk sokkel har etablert en egen dialog med sikkerhetsmyndighetene, og blir løpende oppdatert om trusselbildet gjennom denne (Digitale Sårbarheter Olje & Gass 2015), og kun noen få av dem er tilknyttet varslingssystemet for digital infrastruktur (VDI) (Digital sårbarhet - sikkert samfunn 2015). Systemets funksjon og rolle i den norske olje- og gassnæringen vil bli utdypet om litt.

Mens den helhetlige petroleumssektoren ikke har et CERT, har for eksempel Statoil sitt eget CSIRT (Computer Security Incident Response Team). Fordelene med disse ordningene tilflyter utelukkende de enkelte selskapene. De andre, som ikke har lignende prosedyrer, har større utfordringer med å detektere nye digitale trusler i form av at 1: *Deteksjonskapasiteten av digitale angrep blir betydelig mindre*, og 2: *Utveksling av informasjon samt hendelseskoordinering blir vesentlig svekket* (Pijnenburg Muller, Gjesvik og Friis 2018). Dette kan medføre konsekvenser utover selskapene selv hvis et cyberangrep med følger for infrastruktur, miljø, økonomi og menneskeliv inntreffer. Som et alternativ til petroleumsindustriens eget CERT, har kraftbransjens KraftCERT ønsket petroleumssektoren velkommen som medlem i forebyggingen og håndteringen av cyberhendelser (IKT-sikkerhet 2017). Som det fremkom av analysen av Lysneutvalgets anbefalinger per våren 2018, har petroleumssektoren tilsynelatende fortsatt ikke inngått et medlemskap på bakgrunn av at sektoren synes å ha behovet sitt dekket via avtalene med NSM, og det utenlandske moderselskapets avtaler med sitt nasjonale CERT-miljø (IKT-sikkerhet 2017).

4.5.3 – CNI

I myndighetenes sikring av petroleumsrelatert infrastruktur mot digitale angrep ble det i analysen av NOU 2015: 13 presentert et annet særegent moment i form av at ingen av Norges olje- og gassinstallasjoner er per i dag definert som CNI – *critical national infrastructure* eller kritisk nasjonal infrastruktur. Andre betegnelser er «skjermingsverdig infrastruktur» eller «skjermingsverdig objekt». Uansett benevnelse, handler problematikken rundt petroleumsrelatert CNI om at sektoren ikke er underlagt sikkerhetsloven, og dermed heller ikke Forskrift om objektsikkerhet.

Sikkerhetsloven (formalisert; Lov om forebyggende sikkerhetstjeneste) omhandler arbeid med forebyggende sikkerhetstiltak for å effektivt «[…] kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser […]» (Sikkerhetsloven 1998, § 1) ved å planlegge, tilrettelegge, kontrollere og gjennomføre nevnte sikkerhetstiltak. Sikkerhetstruende momenter kan være spionasje, sabotasje og terrorhandlinger. Hjemlet i sikkerhetsloven er Forskrift om objektsikkerhet som pålegger virksomheter og departementer å utpeke objekter de mener kategoriseres som skjermingsverdige i henhold til sikkerhetsloven. Departementene utpeker slike objekter innen sitt myndighetsområde. Virksomheter, NSM og tilsynsorganer, som for eksempel Petroleumstilsynet, kan også foreslå skjermingsverdige objekter som, etter deres syn, egner seg for kategorien (Helgesen 2013a, Forskrift om objektsikkerhet 2010).

Et skjermingsverdig objekt er etter sikkerhetsloven definert som «[…] eiendom som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser» (Sikkerhetsloven 1998, § 3). Ingen av petroleumssektorens installasjoner er per dags dato underlagt sikkerhetsloven og definert som skjermingsverdig infrastruktur. Forskningsrapporten *Cyber-weapons in International Politics* fremhever at en ny sikkerhetslov er under arbeid, og at dette har ført til oppfatningen om at petroleumssektoren delvis vil bli inkorporert i den (Pijnenburg Muller, Gjesvik og Friis 2018). Hvilke objekter og installasjoner som eventuelt vil bli utpekt som skjermingsverdige er i skrivende stund uvisst, og den nye sikkerhetsloven vil sannsynligvis ikke tre fullverdig i kraft før 01.januar 2019.[12]

Dette er utvilsomt et positivt tiltak, men det kommer påfallende sent med tanke på at petroleumsvirksomheten har eksistert i nærmere 50 år, og at digitaliseringen og den teknologiske utviklingen opptrer hyppigere for hver dag som går. Petroleumsindustrien har gitt Norge store verdier helt fra starten av, ikke minst hva angår økonomisk vekst og velferd. På bakgrunn av det som har blitt nevnt om cybersabotasje på materielle dimensjoner, er det ikke usannsynlig at slik sabotasje mot den norske petroleumsindustrien kan få konsekvenser for «vitale nasjonale sikkerhetsinteresser». I 2013 påstod Olje- og energidepartementet (OED) at ingen olje- og gassinstallasjoner krever ekstra terrorbeskyttelse, noe som frembrakte skarp kritikk fra NSM som mente at installasjonene helt klart regnes som vital nasjonal infrastruktur

[12] Informasjonen er hentet fra et arrangement som presenterte funn fra forskningsprosjektet *Cybervåpen i internasjonal politikk.* NUPI, 27.februar 2018, Oslo

som bør sikres: «'Det er en rekke aspekter innen sikkerhetspolitikk, utenriksrelasjoner, liv og helse, miljøforhold og økonomiske forhold som til sammen gjør at flere olje- og gassinstallasjoner bør sikres'» (Helgesen 2013a). OED har også blitt anklaget for å ikke ha tilstrekkelig intern kompetanse til å kunne utføre jobben med å utpeke skjermingsverdige objekter innen sitt fagområde (Helgesen 2013a).

I det pågående arbeidet med ny Lov om forebyggende sikkerhetstjeneste er det fremdeles OED som vil ha siste ord i behovet for utvelgelsen av skjermingsverdige objekter i olje- og gassnæringen (Pijnenburg Muller, Gjesvik og Friis 2018). Dersom departementet opprettholder synet fra 2013, vil det bety et mindre robust sikkerhetsnivå enn det den norske petroleumsindustrien fortjener med bakgrunn i cybertrusler.

Parallelt med diskusjonen om olje- og gassinstallasjoner som skjermingsverdige objekter, kommer også de kompliserte omstendighetene rundt varslingssystem for digital infrastruktur (VDI) inn. Sensornettverket drives og videreutvikles av NSM, og fungerer på den måten at det fanger opp mulige datainnbrudd hos den aktuelle virksomheten (NSM 2014). VDI er i prinsippet et nyttig verktøy for avdekking av digitale angrep, men medfører en ulempe i sin utplasseringsstruktur ved at tilknytning til nettverket er basert på frivillighet samt en vurdering av virksomhetens egnethet til statusen «kritisk infrastruktur». For medlemmer av VDI-nettverket, påfølger det også en kostnad for selve sensoren som skal utplasseres (Digital sårbarhet - sikkert samfunn 2015). På grunn av dette, er det ikke en selvfølge at sensorene er utplassert akkurat der det nødvendigvis er størst behov. Utredningsutvalget av NOU 2015: 13 konkluderer VDI-praksisen med at: «Andelen virksomheter som inngår i nettverket […], gjør at VDI-sensornettverket ikke dekker behovet for å avdekke digitale angrep mot kritisk infrastruktur og informasjon i Norge i dag» (Digital sårbarhet - sikkert samfunn 2015:263).

Som nevnt, er det ikke regulert ved lov eller annet pålegg for virksomheter å delta i VDI. Derfor er det ikke gitt at systemet er utplassert der det er mest hensiktsmessig. I petroleumsindustrien kan dette være nokså problematisk, ettersom selskapene opererer med massive installasjoner, materiale og infrastruktur, som aller helst bør være kontinuerlig overvåket. NOU 2015: 13 fastslår: «*Varslingssystem for digital infrastruktur (VDI)* i NSM har til hensikt å gi myndighetene varsel om koordinerte og alvorlige dataangrep mot samfunnskritisk infrastruktur eller andre viktige samfunnsfunksjoner» (Digital sårbarhet - sikkert samfunn 2015:259). Likevel er det ikke et krav for virksomheter som er tilknyttet nettopp samfunnskritisk infrastruktur eller viktige samfunnsfunksjoner å ta del i VDI-

samarbeidet. Det foreligger heller ingen føringer for at virksomheter må være tilknyttet sikkerhetsloven for å kunne få utplassert en VDI-sensor. At ingen olje- og gassinstallasjoner på norsk kontinentalsokkel er definert som skjermingsverdig objekt bør derfor ikke være til hinder for å pålegge at operatørselskapene går inn for å tilknytte seg varslingssystemet. Det finnes gode argumenter for å anse installasjonene i petroleumsindustrien og tilhørende infrastruktur som, i minste grad, «viktige samfunnsfunksjoner». Især når industrien verken har sin egen CERT-funksjon eller er medlem i for eksempel KraftCERT, kan et utvidet VDI-nettverk bistå i en mer effektivisert avdekking og håndtering av store cyberhendelser som kan ødelegge fysiske andeler av installasjonene.

4.6 – Oppsummering

Cybersabotasje mot den norske petroleumsindustriens infrastruktur har, i nåværende sikkerhetskontekst, lav sannsynlighet. Dette følger av at slike former for cyberangrep krever ekspertkompetanse, kraftige gjennomføringsmidler, og et nærmest garantert vinningsutfall. Sikkerheten rundt industrien involverer mange tiltak, fra mange ulike samfunnsaktører. Disse bidrar til å minske de digitale truslene og sårbarhetene som finnes i sektoren. Men det tverrsektorielle arbeidet, med sine lange verdikjeder og nettverk, øker i sin tur andelen uklarheter og misforståelser i avdekkingen, håndteringen og etterforskningen av digitale hendelser. Også verdikjeder i systemer og nettverk bidrar til at nødvendige sikkerhetsbehov, krav og praksiser ikke alltid sammenfaller.

På bakgrunn av det som har blitt skissert her og i de foregående kapitlene, fremstår det nærmest et misforhold i måten petroleumssektoren blir omtalt på av sikkerhetsmyndigheter, og lovverket som sektoren faktisk er omfattet av. I sammenheng med OEDs motvilje til å utpeke infrastruktur på norsk sokkel som kritisk og skjermingsverdig, sa NSM: «Etter vår mening er landets olje- og gassinstallasjoner helt klart vital nasjonal infrastruktur som bør sikres» (Helgesen 2013a). Et så høyt nivå av uenighet mellom en nasjonal sikkerhetsinstans og instansen som innehar hovedansvaret for all norsk petroleumsvirksomhet, kan bidra til en stagnering i effektiviseringen av gode og nyttige forebyggende sikkerhetstiltak som næringen, etter alt å dømme, har krav på.

Ifølge utredningen *Digital sårbarhet - sikkert samfunn,* blir olje- og gassinstallasjonenes materialitet skissert som tilstedeværende og essensiell, men oftest i relasjon til SCADA. Sårbarheter i andre materielle instanser blir, ifølge forskningsdataene som har blitt lagt til

grunn, ikke like høyt prioritert. Sannsynligheten er stor for at disse elementene blir kartlagt i andre, mer temaspesifiserte dokumenter.

De siste års risikoanalyser har pekt på at etterretning og informasjonsinnhenting i det digitale rom fremdeles er de mest utbredte formene for cyberaktivitet. Statlige og andre internasjonale aktører er de det særlig knyttes en bekymring til i denne konteksten. NSM skriver i sin risikorapport for 2017 at statlige aktører antakelig kan kartlegge sårbarheter i den digitale infrastrukturen for så å utnytte disse til sabotasjehandlinger (Risiko 2017 2017). Også tilgang til vital informasjon, slik som brukernavn og passord, kan tjene som et forberedende steg mot å utføre cybersabotasje ved en senere anledning. I denne sammenheng kan det avslutningsvis være verdt å nevne misnøyen som har vært rettet mot Oljedirektoratet (OD) og deres forvaltning av verdifull informasjon som kan være ettertraktet av utenforstående.

Direktoratet drifter databasen *Diskos* der lete- og utvinningsrelatert informasjon – hovedsakelig brønn- og seismikkdata for norsk sokkel – er lagret. Informasjonen er delvis konfidensiell, og oljeselskapene har ikke tilgang til hverandres data. Ansatte i offentlig virksomhet, derimot, har fått innvilget slik tilgang (Digitale Sårbarheter Olje & Gass 2015). OD har ved flere anledninger blitt kritisert for å ikke ha gode nok sikkerhetsrutiner for lagring av sine data. Riksrevisjonen har anklaget direktoratet for å ikke ha «[…] et tilfredsstillende styringssystem for informasjonssikkerhet når de behandler informasjon fra oljesektoren, som er viktig å beskytte» (Wernersen 2017). I 2014 varslet Riksrevisjonen om alvorlige mangler i datasikkerheten hos OD, og påpekte at direktoratet ikke hadde noen kontroll over om dataene var forsvarlig sikret. Ifølge Riksrevisjonen, hadde ikke OD fulgt sikkerhetskravene stilt av staten, blant annet knyttet til de ansattes bruk av og tilgang til databasen, hvor vital informasjon om nærmest all norsk oljevirksomhet og kartdata ligger (Block Vagle 2014). Slike opplysninger representerer store verdier for olje- og gasselskapene, og har stor påvirkningskraft på børsverdien (Digitale Sårbarheter Olje & Gass 2015). Uautorisert tilgang til disse dataene, enten fra selskapenes side eller fra en fiendtlig hacker, kan forårsake store økonomiske tap hvis dataene blir manipulert, slettet eller brukt til eget vinningsformål.

Spionasje og etterretningsoperasjoner fra fremmede aktører eller stater i cyberdomenet er ofte den formen for cyberhendelser som oppstår hyppigst, og tilgang til vital informasjon samt passord, numre og koder er alltid attraktive gevinster ved slike hendelser. Ikke minst er cyberkriminalitet med økonomisk vinning som formål særlig utbredt. Dette, sammen med Riksrevisjonens kritikk av Oljedirektoratet, kan forklare det store fokuset på konvensjonell

IKT-sikkerhet til fordel for sikkerhetsrutiner knyttet til konkrete digitale sabotasjeangrep mot materielle samfunnsaspekter. I norsk petroleumssektor har det hittil heller ikke blitt avdekket alvorlige cyberangrep mot infrastrukturen, noe som muligens har bremset debatten omkring denne problematikken. I fremtidige utredninger og diskusjoner bør det likevel legges mer vekt på dette slik at Norge erverver et bredere kunnskapsgrunnlag på området, og ikke henger igjen i det forebyggende teknologiske sikkerhetsarbeidet. Som kjent, vokser digitaliseringen raskt, nye cybervåpen utvikles og forbedres i takt med teknologien, og de politiske situasjonene på det internasjonale plan endres kontinuerlig.

5 – Konklusjon

Denne avhandlingen har tatt for seg den norske petroleumssektorens infrastruktur tilknyttet cyberspace. Målet har vært å belyse hvordan nasjonalt myndighetspersonell og sikkerhetsaktører prioriterer, sikrer og omtaler denne infrastrukturen med bakgrunn i digitale trusler og sårbarheter. To teoriretninger har stått sentralt i dette formålet. Den første har utgangspunkt i Københavnerskolens utvidede sikkerhetsbegrep og *securitization theory* eller sikkerhetiseringsteorien. Den andre har opphav i mediearkeologien, og sentrerer rundt et fokus på materialitet og nettverksarkeologi.

Det utvidede sikkerhetsbegrepet taler for at tradisjonell sikkerhetspolitikk ikke lenger er tilstrekkelig for en debatt rundt sikkerhet i dagens trusselbilde. Siden slutten av den kalde krigen, har tradisjonell sikkerhetstenkning, som lenge var sentrert rundt stat og militærmakt, hatt en markant endring i retning av flere referanseobjekter og flere eksistensielle trusler. Spekteret av verdier som måtte beskyttes ble utvidet til å inkludere sektorer som økonomi, miljø, politikk og samfunn. Innen hvert av disse, kunne man finne karakteristiske trusler som på lik linje med konvensjonell krigføring kunne ramme hele eller deler av den bestemte sektoren. Dersom et cyberangrep forårsaker store og varige strømavbrudd, eksplosjoner i gassrørledninger, togavsporing, flykrasj, fundamentale finansielle tap, og liknende, kan det bli ansett som et terroranslag (Denning 2012). Brukernes utforming av domenet i en mer militært orientert retning ved for eksempel ulovlig og anonymisert våpenhandel, modifikasjoner av programvare, utvikling av ulike typer skadevare, publisering av desinformasjon, med mer legitimerer domenets plass på den utvidede sikkerhetsagendaen.

Mediearkeologien har hjulpet å snevre inn det grenseoverskridende cyberspace innen konteksten av denne avhandlingen ved at én sentral dimensjon har stått i fokus; nemlig materialiteten. Materialitet er det aspektet som mediearkeologer oftest beskjeftiger seg med, og kan nærmest anses som et motsvar til den sedvanemessige vektleggingen av hermeneutikk og retorikk i tradisjonell mediehistorie. Mediearkeologien fordrer et nytt og friskt syn på teknologien som omgir oss, og krever at uutforskede innretninger og deres forsømte elementer blir dratt frem i lyset. Ved å velge den norske petroleumssektoren og den materielle teknologien den omfatter som mitt utgangspunkt for avhandlingen, har jeg forsøkt å nærme meg en slik mediearkeologisk tankegang.

Det er ikke bare de usynlige sidene av teknologien og mediene som er allestedsnærværende; vi er også konstant omringet av de fysiske, og i likhet med at en internettside kan bli manipulert eller stengt ved hjelp av et datavirus, kan et datavirus også infisere fysiske bestanddeler i en eller flere samfunnssektorer. Dersom den påfølgende skaden er kritisk nok, kan hele sektoren rammes, noe som i sin tur kan få konsekvenser for andre avhengige sektorer. Slike massive angrep forekommer heldigvis ikke ofte, og mye av grunnen kan være at de må utføres av kyndige aktører, i en gitt kontekst. Aktørene er gjerne fremmede stater, mens konteksten er forholdene på den internasjonale arena der og da. Historiske faktorer kan også spille sin rolle her i henhold til konstruktivistisk sikkerhetsteori.

En underkategori innen mediearkeologien har bidratt til en belysning av hvordan både samfunnsmessige og teknologiske nettverk, prosesser og verdikjeder former og muliggjør vår mediehverdag. Nettverksarkeologien fordrer et fokus på de omkringliggende aspektene som er til stede når teknologien og sikringen av den implementeres i samfunnet. Slike omstendigheter karakteriseres gjerne av økonomi, arbeid, kultur og politikk. Hvilke teknologier et samfunn tar i bruk, og *hvordan* disse brukes, betinges ofte av myndighetenes og andre forvalternes ønsker, avveiinger og føringer, og ikke minst; av teknologien selv og dens overordnede formål. I tillegg til de strukturelle samfunnsmessige nettverkene i form av beslutningstakere, statlige aktører og sikkerhetseksperter, er mediene også omfattet av lange verdikjeder i form av *cyber supply chains* som involverer mange ledd i tilegnelsen av digitale tjenester. Disse leddene kan være sårbare for trusler fra cyberspace ved at det ofte er usikkert hvor høy grad av sikkerhet leverandøren av tjenestene har tilegnet dem. Manglende dokumentasjon eller en manipulasjon av for eksempel programvare, kan medføre risikoer som virksomheter sjeldent er klar over. Lange *cyber supply chains* kan gjøre det vanskelig å holde oversikt over hvor sårbarhetene ligger, og resultere i at et sikkerhetshull i det ene leddet kan overføres til de resterende. En defekt digital tjeneste, kan potensielt sette vitalt produksjonsutstyr ut av drift.

Nettverk og verdikjeder i form av både mennesker og teknologi gjør en helhetlig risikoforståelse vanskelig. Det kan ha grunnlag i uklarheter knyttet til ansvarsfordeling og myndighetsroller eller i en utilstrekkelig kvalitet på viktige digitale tjenester. Ved hjelp av dokumentanalysene som har blitt lagt til grunn for denne avhandlingen, har jeg forsøkt å belyse disse sidene ved å kartlegge innholdet i et bestemt utvalg rapporter, retningslinjer, stortingsmeldinger, med mer. Hovedfokuset har ligget på NOU 2015: 13 *Digital - sårbarhet sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden,* utredet av et

utvalg ledet av Olav Lysne. I den har utvalget greid ut om digitale sårbarheter i ulike sektorer, inkludert åtte kritiske samfunnsfunksjoner, deriblant olje og gass.

De anbefalte tiltakene innen disse områdene har senere blitt fulgt opp av Justis- og beredskapsdepartementet i deres stortingsmelding Meld. St. 38 *IKT-sikkerhet – Et felles ansvar*. Ved å ta denne meldingen til hjelp, har jeg valgt ut ni av tiltakene som skisseres, og diskutert disse for å peke på hvordan prosessen rundt implementeringen av dem har fortonet seg. Noen av tiltakene har blitt hørt og besvart, mens andre, for eksempel Lysneutvalgets oppfordring om petroleumssektorens tilslutning til KraftCERT, har ikke hatt en like effektiv progresjon. Kartleggingen av tiltakene i kombinasjon med et bilde av hvilke andre dokumenter NOU-en har hatt en innflytelse på og et opphav til, har bidratt til en belysning av Norges offentlige utredningers institusjonelle rolle i samfunnet og samfunnets politikkutforming.

I tråd med fokuset på materialitet, har *Digital sårbarhet - sikkert samfunn* bistått med å legge grunnlaget for en diskurs rundt hvordan trusler mot cyberdomenets materielle lag blir omtalt i statsforvaltningen. Det helhetlige bildet av utredningen viser at tradisjonell IKT-sikkerhet fortsatt blir lagt mest vekt på, men materielle aspekter kommer også frem i lyset til en viss grad. Det kan være mange grunner for hvorfor utvalget ikke greier eksplisitt ut om materielle sider ved cyberspace og sårbarhetene i dem, ikke minst fordi alvorlige sabotasjeangrep mot fysisk infrastruktur hittil ikke har tatt sted på norsk jord, noe som gjør relevansen av slike angrep mindre fremtredende. På den annen side, og som skissert tidligere, kan sabotasjeangrep fra cyberspace ha samme karakteristikker som konvensjonelle terroranslag ved at det er uvisst når og hvorvidt de finner sted. Cybersikkerhet fordrer et samfunn som er godt rustet mot digitale trusler uavhengig av hvor usannsynlige de virker i nåværende stund. I dagens sikkerhetspolitiske bilde skjer endringene raskt, og medfører en kontinuerlig nødvendighet for oppdaterte og effektive forebyggende sikkerhetstiltak.

I forskningsarbeidet har særlig to momenter vist seg å være interessante for oppgavens fokus: Den norske olje- og gassektoren har ikke et eget responsmiljø for varsling om digitale trusler i form av verken et CERT/CSIRT eller et heldekkende VDI-system, og ingen av olje- og gassinstallasjonene på norsk kontinentalsokkel er definert som skjermingsverdig infrastruktur. På bakgrunn av det som har blitt sagt i denne avhandlingen, er jeg tilbøyelig til å bemerke at petroleumsindustriens tilknytning til et responsmiljø samt en definisjon som CNI hadde vært et viktig steg i retning av en mer robust beskyttelse av et av landets største verdier. Særlig i

henhold til den fysiske infrastrukturen som hele industrien er befestet i, er det av essensiell betydning at denne infrastrukturen er godt beskyttet mot trusler fra det digitale rom som kan ha utslag på materialitet.

Nasjonale myndighetsaktører omfatter et vidt spekter av departementer, tilsyn, sikkerhetsorganer, direktorater, med mer. Alle har erkjent cyberspace som et fremtredende aspekt av menneskenes liv, fra underholdningsformål til hybrid krigføring. Cybersikkerhet spiller en betydningsfull rolle i myndighetenes politikk og samfunnsutforming. Det skal ikke undergraves at petroleumssektoren har gagnet Norge på mange måter siden funnet av Ekofiskfeltet i 1969. Høye økonomiske forekomster og en posisjon som verdens 2. ledende gasseksportør har gjort Norge til en markant velferdsstat. Infrastrukturen som petroleumsindustrien er omfattet av krever en høy beskyttelsesgrad, også i cyberspace. Utro tjenere med tilgang til kritiske nettverk og systemer, hacktivister og statlige aktører kan alle ha noe å tjene på å forpurre den nasjonale petroleumsvirksomheten. Dersom betydningsfulle driftskontrollsystemer blir manipulert, skadet eller satt ut av drift, kan de negative konsekvensene inntreffe i både politisk, økonomisk og miljømessig sektor. I verste instans, kan forpurret produksjonsutstyr sette menneskeliv i fare. *Hardware hacking* av maskineri, PC-er, USB-pinner eller annet lett tilgjengelig utstyr kan forårsake at vesentlige systemer og funksjoner slutter å virke. Og kutting av undersjøiske fiberoptiske kabler kan medføre total produksjonsstopp som følge av manglende nettforbindelse og kommunikasjonsmuligheter.

I dette forskningsprosjektet har det vært problematisk å få tilgang til korrekt informasjon som omhandler cybersikkerheten innen norsk olje- og gassektor eksplisitt, derfor er det ikke gitt at de viktigste faktorene og sikkerhetstiltakene har blitt viet tilstrekkelig oppmerksomhet. Det er stor sannsynlighet for at cyberdomenets materielle lag innen petroleumsvirksomheten er mer utdypende omtalt i andre dokumenter enn de som har blitt lagt til grunn for denne oppgaven, især NOU 2015: 13. Faktagrunnlaget som har blitt benyttet i oppgaven tilsier at den norske petroleumsvirksomheten både har igangsatt og gjennomført viktige sikkerhetiserende grep med sikte på å heve sikkerhetsnivået i sektoren i lys av den hyppige digitaliseringen og den stadige avhengigheten av digitale løsninger. For fremtidens oppfølginger vil det bli særlig spennende å følge med på hva utfallet av den reviderte Lov om forebyggende sikkerhetstjeneste vil bli. Uavhengig av resultatet, er det mye som tyder på at Norges petroleumsrelaterte infrastruktur har krav på en solid sikkerhet i cyberspace.

Litteraturliste

21 Steps to Improve Cyber Security of SCADA Networks (2002). President's Critical Infrastructure Protection Board og Energidepartementet (Veiledning). https://www.hsdl.org/?abstract&did=1826 [Lest: 26.januar 2018].

Al-Youm, Al-Masry (2013): «Internet saboteur caught, says Telecom Egypt CEO». *Egypt Independent*, egyptindependent.com. http://www.egyptindependent.com/internet-saboteur-caught-says-telecom-egypt-ceo/ [Lest: 03.mai 2018].

BBC: «Hackers attack Norway's oil, gas and defence businesses» (2011). http://www.bbc.com/news/technology-15790082 [Lest: 20.april 2018].

Block Vagle, Håkon (2014): «Manglet kontroll med hemmelige oljedata». *Bergens Tidene*, bt.no. https://www.bt.no/nyheter/lokalt/i/k8nkk/Manglet-kontroll-med-hemmelige-oljedata [Lest: 19.april 2018].

Buzan, Barry (1995): «Security, the State, the «New World Order», and Beyond». I: Ronnie D. Lipschutz (red.): *On security*. New York og Chichester: Columbia University Press.

Buzan, Barry og Lene Hansen (2009): *The Evolution of International Security Studies*. Cambridge: Cambridge University Press.

Buzan, Barry, Ole Wæver og Jaap de Wilde (1998): *Security – A New Framework For Analysis*. Boulder og London: Lynne Rienner Publishers, Inc.

Denning, Dorothy E. (2012): «Stuxnet: What Has Changed?». *Future Internet* 4(3):672-687. DOI: 10.3390/fi4030672

Digital sårbarhet - sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden (2015). Oslo: Justis- og beredskapsdepartementet (NOU 2015: 13).

Digitale Sårbarheter Olje & Gass (2015). Stavanger: DNV GL (Rapport).

Elsaesser, Thomas (2004): «The New Film History as Media Archaeology». *Cinémas: Revue d'études cinématographiques* 14(2-3):75-117.

Eun, Yong-Soo og Judith Sita Aßmann (2016): «Cyberwar: Taking Stock of Security and Warfare in the Digital Age». *International Studies Perspectives* 17:343-360. DOI: http://dx.doi.org/10.1111/insp.12073

Evans, Dean (2015): «What is BYOD and why is it important?». *Techradar*, techradar.com. https://www.techradar.com/news/computing/what-is-byod-and-why-is-it-important-1175088 [Lest: 03.mai 2018].

Fermann, Gunnar (2011): «Utenrikspolitikk som begrep, intensjon og atferd». I: Jon Hovi og Raino Malnes (red.): *Anarki, makt og normer – Innføring i internasjonal politikk*. Oslo: Abstrakt forlag AS.

Forskrift om objektsikkerhet (2010). *Forskrift om objektsikkerhet*. Fastsatt ved kgl.res. 22. oktober 2010 med hjemmel i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven) § 17 andre ledd. https://lovdata.no/dokument/SF/forskrift/2010-10-22-1362

Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren – «FDs cyberretningslinjer» (2014). Oslo: Forsvarsdepartementet (Retningslinjer).

Galloway, Alexander (2004): *Protocol: How Control Exists After Decentralization.* Cambridge: MIT Press.

Goldstein, Joshua S. og Jon C. Pevehouse (2014): *International Relations.* 6.utg. Boston: Pearson.

Greene, Tim (2011): «Hackers hit oil, gas, defense companies in Norway». *NetworkWorld*, networkworld.com. https://www.networkworld.com/article/2183366/malware-cybercrime/hackers-hit-oil--gas--defense-companies-in-norway.html [Lest: 20.april 2018].

Hamnes, Leif (2012): «16 spektakulære cyberangrep». *E24*, e24.no. https://e24.no/digital/16-spektakulaere-cyberangrep/20237501 [Lest: 26.februar 2018].

Hansen, Lene og Helen Nissenbaum (2009): «Digital Disaster, Cyber Security, and the Copenhagen School». *International Studies Quarterly* 53(4):1155-1175. DOI: 10.1111/j.1468-2478.2009.00572.x

Hansen, Tore (2017): «Norges offentlige utredninger (NOU)». *Store norske leksikon*, snl.no. https://snl.no/Norges_offentlige_utredninger_(NOU) [Lest: 15.mars 2018].

Helgesen, Ole Ketil (2013a): «'Ingen olje- og gassinstallasjoner trenger ekstra terrorbeskyttelse'». *Teknisk Ukeblad*, tu.no. https://www.tu.no/artikler/ingen-olje-og-gassinstallasjoner-trenger-ekstra-terrorbeskyttelse/275375 [Lest: 22.mars 2018].

Helgesen, Ole Ketil (2013b): «Prøver å lamme oljeproduksjon med cyberangrep». *Teknisk Ukeblad*, tu.no. https://www.tu.no/artikler/prover-a-lamme-oljeproduksjon-med-cyberangrep/232713 [Lest: 11.april 2018].

Hovi, Jon og Raino Malnes (red.) (2011): *Anarki, makt og normer – Innføring i internasjonal politikk.* 2.utg. Oslo: Abstrakt forlag AS.

Huhtamo, Erkki og Jussi Parikka (red.) (2011): *Media Archaeology: Approaches, Applications, Implications*. Berkeley: University of California Press.

IKT-sikkerhet – Et felles ansvar (2017). Oslo: Justis- og beredskapsdepartementet (Meld. St. 38).

Internasjonal cyberstrategi for Norge (2017). Oslo: Utenriksdepartementet (Strategi).

IO Center: «What is integrated operations?» (årstall ikke angitt). http://www.iocenter.no/info/what-integrated-operations [Lest: 03.mai 2018].

ISO – International Organization for Standardizaton: «We're ISO: we develop and publish International Standards» (årstall ikke angitt). https://www.iso.org/standards.html [Lest: 20.april 2018].

Iversen, Gunnar (2016): «Mediearkeologi som alternative historiefortellinger om film». I: Jan Anders Diesen, Tore Helseth og Gunnar Iversen (red.): *Den levende fortiden: Filmhistorie og filmhistoriografi*. Oslo: Universitetsforlaget.

Jørgenrud, Marius (2012): «Angrep slo ut 30.000 pc-er». *Digi*, digi.no. https://www.digi.no/artikler/angrep-slo-ut-30-000-pc-er/204822 [Lest: 11.april 2018].

Kartverket: «GPS og GNSS» (2017). https://www.kartverket.no/kunnskap/posisjon-og-navigasjon/GPS-og-GNSS/ [Lest: 04.mai 2018].

Kittler, Friedrich A. (1999): *Gramophone, film, typewriter*. Stanford: Stanford University Press.

Lee, Micah (2018): «IT'S IMPOSSIBLE TO PROVE YOUR LAPTOP HASN'T BEEN HACKED. I SPENT TWO YEARS FINDING OUT.» *The Intercept*, theintercept.com. https://theintercept.com/2018/04/28/computer-malware-tampering/ [Lest: 01.mai 2018].

Lipschutz, Ronnie D. (red.) (1995): *On security*. New York og Chichester: Columbia University Press.

Melito, Steve (årstall ikke angitt): «Cyber War and the Siberian Pipeline Explosion». *DSA – Defence and Security Alert*, dsalert.org. http://www.dsalert.org/int-experts-opinion/cyber-warfare/508-cyber-war-and-the-siberian-pipeline-explosion [Lest: 25.januar 2018].

Messmer, Ellen (2011): «Security roundup for week ending Nov.18: Facebook, Norway oil-industry cyberattacks, and why virtualization and mobile devices mean security stress». *NetworkWorld*, networkworld.com. https://www.networkworld.com/article/2183349/security/security-roundup-for-week-ending-nov--18--facebook--norway-oil-industry-cyberattacks--and-w.html [Lest: 20.april 2018].

Mitchell, W.J.T. og Mark B.N. Hansen (red.) (2010): *Critical terms for media studies*. Chicago og London: The University of Chicago Press.

Munson, Lee (2014): «Massive cyber attack on oil and energy industry in Norway». *Naked Security*, nakedsecurity.sophos.com. https://nakedsecurity.sophos.com/2014/08/28/massive-cyber-attack-on-oil-and-energy-industry-in-norway/ [Lest: 15.mars 2018].

NATO Cyber Defence (2017). NATO (Faktaark). https://www.nato.int/cps/en/natohq/144032.htm [Lest: 11.april].

Nissenbaum, Helen (2005): «Where computer security meets national security». *Ethics and Information Technology* 7(2):61-73. DOI: 10.1007/s10676-005-4582-3

Norsk olje og gass: «Standardisering» (årstall ikke angitt). https://www.norskoljeoggass.no/drift/standardisering/ [Lest: 20.april 2018].

NSM: «Varslingssystem for digital infrastruktur (VDI)» (2014). https://nsm.stat.no/norcert/varslingssystem-for-digital-infrastruktur-vdi/ [Lest: 21.mars 2018].

NSMs grunnprinsipper for IKT-sikkerhet (2017). Sandvika: Nasjonal sikkerhetsmyndighet (Grunnprinsipper). https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/ [Lest: 29.april 2018].

NTNU CCIS: «Center for Cyber and Information Security» (årstall ikke angitt). https://www.ntnu.edu/web/ccis/center-for-cyber-and-information-security [Lest: 12.april 2018].

NUPI: «Digitale Sabotasjeangrep mot Norsk Petroleumssektor (DISP)» (årstall ikke angitt). http://www.nupi.no/Om-NUPI/Prosjekter-og-sentre/Digitale-Sabotasjeangrep-mot-Norsk-Petroleumssektor [Lest: 14.februar 2018].

Nystrøm, Sofie (2016): «Er vi rigget for å motstå en hybrid krise eller krig?». *Den Norske Atlanterhavskomité*, atlanterhavskomiteen.no. http://www.atlanterhavskomiteen.no/post/8097694/Er%20vi%20rigget%20for%20%C3%A5%20motst%C3%A5%20en%20hybrid%20krise%20eller%20krig [Lest: 11.april 2018].

Parikka, Jussi (2012): *What is Media Archaeology?* Cambridge og Malden: Polity Press.

Parikka, Jussi (2015): *A Geology of Media*. Minneapolis: University of Minnesota Press.

Peoples, Columba og Nick Vaughan-Williams (2015): *Critical Security Studies – An introduction*. 2.utg. London og New York: Routledge.

Perlroth, Nicole (2012): «In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back». *The New York Times*, nytimes.com. https://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html [Lest: 11.april 2018].

Petroleumstilsynet: «Om oss» (årstall ikke angitt). http://www.ptil.no/om-oss/category701.html [Lest: 05.april 2018].

Petroleumstilsynet: «Rolle og ansvarsområde» (årstall ikke angitt). http://www.ptil.no/rolle-og-ansvarsomrade/category725.html [Lest: 05.april 2018].

Pijnenburg Muller, Lilly, Lars Gjesvik og Karsten Friis (2018): *Cyber-weapons in International Politics – Possible sabotage against the Norwegian petroleum sector*. http://hdl.handle.net/11250/2486814 [Lest: 01.mars 2018].

Regjeringen: «Fokus 2018: E-tjenestens åpne vurdering» (2018). https://www.regjeringen.no/no/aktuelt/fokus-2018-e-tjenestens-apne-vurdering/id2592753/ [Lest: 13.april 2018].

Regjeringen: «NOU-ar» (årstall ikke angitt). https://www.regjeringen.no/no/dokument/nou-ar/id1767/ [Lest: 15.mars 2018].

Regjeringen: «Proposisjonar til Stortinget» (årstall ikke angitt). https://www.regjeringen.no/no/dokument/prop/id1753/ [Lest: 22.mars 2018].

Retningslinjer for samarbeid ved fare- og ulykkessituasjoner i petroleumsvirksomheten (2013). Den offentlige redningstjenesten (Retningslinjer). https://www.hovedredningssentralen.no/dokumenter/ [Lest: 25.april 2018].

Risiko 2017 - Risiko og sårbarheter i en ny tid – En vurdering av sårbarheter og risiko i Norge (2017). Sandvika: Nasjonal sikkerhetsmyndighet (Risikorapport).

Risiko i et trygt samfunn – Samfunnssikkerhet (2016). Oslo: Justis- og beredskapsdepartementet (Meld. St. 10).

Saffo, Paul (2013): «Disrupting Undersea Cables: Cyberspace's Hidden Vulnerability». *Atlantic Council*, atlanticcouncil.org. http://www.atlanticcouncil.org/blogs/new-atlanticist/disrupting-undersea-cables-cyberspaces-hidden-vulnerability [Lest: 03.mai 2018].

Shackelford, Scott J. (2014): *Managing Cyber Attacks in International Law, Business, and Relations – In Search of Cyber Peace*. New York: Cambridge University Press.

Sikkerhetsloven (1998). *Lov om forebyggende sikkerhetstjeneste av 20.mars 1998 nr.10.* https://lovdata.no/dokument/NL/lov/1998-03-20-10

Starosielski, Nicole (2015): *The Undersea Network*. Durham: Duke University Press.

Starosielski, Nicole, Braxton Soderman og Cris Cheek (2013): «AMODERN 2: NETWORK ARCHAEOLOGY». *Amodern*, amodern.net. http://amodern.net/article/network-archaeology/ [Lest: 29.november 2017].

Stouffer, Keith mfl. (2015): *Guide to Industrial Control Systems (ICS) Security.* http://dx.doi.org/10.6028/NIST.SP.800-82r2 [Lest: 26.januar 2018].

Syvertsen, Trine (1998): *Dokumentanalyse i medievitenskapen: Tilgang, kildekritikk, problemstillinger – Med oversikt over offentlige dokumenter og dokumenter fra medieinstitusjoner (papir- og webkilder).* Notat. Oslo: Institutt for medier og kommunikasjon. https://www.academia.edu/5410482/Dokumentanalyse_i_medievitenskapen_Tilgang_kildekritikk_problemstillinger_1998_ [Lest: 14.mai 2018].

Technopedia: «Computer Emergency Response Team (CERT)» (årstall ikke angitt). https://www.techopedia.com/definition/31003/computer-emergency-response-team-cert [Lest: 25.april 2018].

Threats to Undersea Cable Communications (2017). The Public-Private Analytic Exchange Program (AEP). https://www.dni.gov/files/PE/Documents/1---2017-AEP-Threats-to-Undersea-Cable-Communications.pdf [Lest: 08.mai 2018].

Ventre, Daniel (2013): «Conclusion». I: *Cyber Conflict.* https://doi.org/10.1002/9781118562666.ch10 [Lest: 23.mai 2017].

Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur (2013). Oslo: Norsk Romsenter. https://www.romsenter.no/no/Aktuelt/Publikasjoner/Rapport-om-saarbarhet-ved-bruk-av-satellittnavigasjon [Lest: 04.mai 2018].

Wendt, Alexander (1995): «Constructing International Politics». *International Security* 20(1):71-81. https://muse.jhu.edu/article/447390/summary [Lest: 04.desember 2017].

Wernersen, Camilla (2017): «Riksrevisjonen: – Oljedirektoratet sikrer sensitiv informasjon for dårlig». *NRK*, nrk.no. https://www.nrk.no/norge/riksrevisjonen_-_-oljedirektoratet-sikrer-sensitiv-informasjon-for-darlig-1.13777395 [Lest: 19.april 2018].

Williams, Colin (2014): «Security in the cyber supply chain: Is it achievable in a complex, interconnected world?». *Technovation* 34(7):382-384. DOI: 10.1016/j.technovation.2014.02.003

Williams, Paul D. (red.) (2013): *Security Studies – An Introduction.* 2.utg. Abingdon og New York: Routledge.

Windelberg, Marjorie (2015): «Objectives for managing cyber supply chain risk». *International Journal of Critical Infrastructure Protection* 12:4-11. DOI: http://dx.doi.org/10.1016/j.ijcip.2015.11.003

Windfeld Lund, Niels (2010): «Document, text and medium: concepts, theories and disciplines». *Journal of Documentation* 66(5):734-749. DOI: 10.1108/00220411011066817

Østbye, Helge mfl. (2007): *Metodebok for mediefag*. 3.utg. Bergen: Fagbokforlaget Vigmostad & Bjørke AS.

Vedlegg 1 – Dokumentoversikt

Dokument: *Digitale Sårbarheter Olje & Gass* (2015). Stavanger: DNV GL (Rapport)

Dokumentopplysninger:

- Hva: Rapport.
- Utarbeidet av: DNV GL v/Pål Børre Kristoffersen.
- Avgitt til: Lysneutvalget (digitalt sårbarhetsutvalg, nedsatt av regjeringen 20.juni 2014), 24.april 2015.
- Tilgjengelig her.

Overordnet tema/innhold: Digitale sårbarheter og utfordringer i norsk olje- og gassektor. Spesielt fokus på fire ledd i virksomhetens verdikjede; leting, feltutvikling, produksjon og transport.

-

Dokument: *Risiko 2017: Risiko og sårbarheter i en ny tid – En vurdering av sårbarheter og risiko i Norge* (2017). Sandvika: NSM (Rapport)

Dokumentopplysninger:

- Hva: Rapport/risikovurdering.
- Utarbeidet av: NSM (Nasjonal Sikkerhetsmyndighet).
- Avgitt til: Offentlig tilgjengelig risikorapport på NSM sine nettsider. Årlig utgivelse. Denne er fra 2017.
- Tilgjengelig her.

Overordnet tema/innhold: Sannsynlige trusler mot Norge samt skildring av sårbarheter.

-

Dokument: *Digital sårbarhet - sikkert samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden* (2015). Oslo: Utvalg v/Olav Lysne (NOU 2015: 13)

Dokumentopplysninger:

- Hva: Offentlig utredning.
- Utarbeidet av: Utvalg oppnevnt ved kongelig resolusjon 20.juni 2014. Leder: Olav Lysne.
- Avgitt til: Justis- og beredskapsdepartementet 30.november 2015.
- Tilgjengelig her.

Overordnet tema/innhold: IKT-sikkerhet innen samtlige av Norges samfunnssektorer. Sårbarheter i kritiske samfunnsfunksjoner. Forslag til forebyggende sikkerhetstiltak i tilknytning til arbeid med forebyggende IKT-sikkerhet samt nasjonal evne til avdekking og håndtering av digitale angrep.

-

Dokument: *IKT-sikkerhet: Et felles ansvar* (2016-2017). Oslo: Justis- og beredskapsdepartementet (Meld. St. 38)

Dokumentopplysninger:

- Hva: Melding til Stortinget.
- Utarbeidet av: Justis- og beredskapsdepartementet, 09.juni 2017.
- Avgitt til: Stortinget ved regjeringen Solberg (godkjent i statsråd 09.juni 2017).
- Tilgjengelig her.

Overordnet tema/innhold: IKT er til stede i mange deler av samfunnet og fører både til fordeler og ulemper. Meldingen fremmer status på anbefalingene gjort av Lysneutvalget i NOU 2015: 13 i sammenheng med tiltak for arbeid med forebyggende IKT-sikkerhet samt nasjonal evne til avdekking og håndtering av digitale angrep.

-

Dokument: *Risiko i et trygt samfunn: Samfunnssikkerhet* (2016-2017). Oslo: Justis- og beredskapsdepartementet (Meld. St. 10)

Dokumentopplysninger:

- Hva: Melding til Stortinget.
- Utarbeidet av: Justis- og beredskapsdepartementet, 09.desember 2016.
- Avgitt til: Stortinget ved regjeringen Solberg (godkjent i statsråd 09.desember 2016).
- Tilgjengelig her.

Overordnet tema/innhold: Regjeringens ønsker for arbeidet og politikkutformingen innen samfunnssikkerhet. Utgreiing av og tiltak innen brann- og redningsetatene, politi, ambulanse, Sivilforsvaret, kommunene osv. Samarbeid og kommunikasjon.

-

Dokument: *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren – «FDs cyberretningslinjer»* (2014). Oslo: Forsvarsdepartementet (Retningslinjer)

Dokumentopplysninger:

- Hva: Retningslinjer.
- Utarbeidet av: Forsvarsdepartementet v/departementsråd Erik Lund-Isaksen.
- Avgitt til: Ugradert og offentlig tilgjengelig, men gjelder for Forsvarsdepartementet og underlagte etater, 01.mars 2014.
- Tilgjengelig her.

Overordnet tema/innhold: Utlegging om retningslinjer, roller og ansvar, arbeidsoppgaver og praktisk utførelse av disse innad forsvarssektoren ved digitale angrep. Begrepsdefinisjoner.

-

Dokument: *Cyber-weapons in International Politics – Possible sabotage against the Norwegian petroleum sector* (2018). Oslo: NUPI (Forskningsrapport)

Dokumentopplysninger:

- Hva: Forskningsrapport.
- Utarbeidet av: NUPI (Norsk Utenrikspolitisk Institutt) v/Lilly Pijnenburg Muller, Lars Gjesvik og Karsten Friis.
- Avgitt til: Offentlig publikasjon tilgjengelig på NUPI sine nettsider, 2018.
- Tilgjengelig her.

Overordnet tema/innhold: Utlegging om funn fra forskningsprosjektet *Digitale Sabotasjeangrep mot Norsk Petroleumssektor*. Ansvar, roller, myndighet, informasjonsdeling.

Vedlegg 2 – Oversikt over *Digital sårbarhet - sikkert samfunn* – *Beskytte enkeltmennesker og samfunn i en digitalisert verden* (2015). Oslo: Utvalg v/Olav Lysne (NOU 2015: 13) i tabell én og tabell to

Tabell én - Utredningens helhetlige komposisjon:

Kapittel	Overordnet tema/innhold	Merknader
1 – Sammendrag	Norges avhengighet av internett og sårbarhetene dette fører med seg i sektorer og virksomheter. Liste over utvalgets viktigste anbefalinger	
2 – Mandat, utvalgets sammensetning og arbeid	Presentasjon av utvalgets medlemmer og deres formål. Utvalgets mandat var hovedsakelig å utrede Norges digitale sårbarheter, sikkerhetsutfordringene på IKT-området, håndtering av disse med mer samt foreslå nødvendige tiltak for å styrke Norges IKT-sikkerhet	
3 – Rettsstatsprinsipper og grunnleggende samfunnsverdier	Utredning av problemstillingene som kan oppstå mellom høy grad av sikkerhet og grunnleggende menneskerettigheter slike som personvern, ytringsfrihet, privatliv og forsamlingsfrihet	
4 – Hva er digitale sårbarheter?	Skildring av begrepene «sårbarhet», «verdivurdering», «trussel og fare» og «risikovurdering»	
5 – Sikring av IKT og digital informasjon		Kapittelet er omtalt i tabellen «**Utredningens særlig relevante deler**»
6 – Trender som påvirker sårbarhetsbildet		Kapittelet er omtalt i tabellen «**Utredningens særlig relevante deler**»

7 – Utilsiktede og tilsiktede IKT-hendelser	Eksempler på ulike typer tilsiktede og utilsiktede IKT-hendelser og bakgrunnen for disse. For eksempel kan en utilsiktet hendelse være resultatet av naturhendelser, menneskelig eller organisatorisk svikt	Delkapitlene som omhandler tilsiktede hendelser (7.2) er omtalt i tabellen «**Utredningens særlig relevante deler**»
8 – Organisering av roller og ansvar		Kapittelet er omtalt i tabellen «**Utredningens særlig relevante deler**»
9 – IKT-sikkerhetsarbeid i andre land	Skildring av utvalgte andre lands arbeid på cybersikkerhetsområdet; USA, Canada, Tyskland, Nederland, Storbritannia, Sverige, Finland og Estland. Kartlegging av strategier og tiltak som kan overføres til Norge	
10 – Folkerett og internasjonalt samarbeid	Utredning om cyberdomenets grenseoverskridende karakter og behov for internasjonalt samarbeid. Noen viktige organisasjoner blir nevnt, bl.a. FN, EU, Europarådet, NATO og OECD. Norges rolle og forpliktelser	
11 – Elektronisk kommunikasjon	Kapittelet omhandler digitale sårbarheter i denne samfunnsfunksjonen samt utvalgets anbefalinger, vurderinger og tiltak knyttet til disse	Avhandlingens hovedfokus er Norges petroleumsnæring, dermed er ikke sårbarhetene og anbefalingene som er omtalt i denne samfunnsfunksjonen relevant
12 – Satellittbaserte tjenester	Kapittelet omhandler digitale sårbarheter i denne samfunnsfunksjonen samt utvalgets anbefalinger, vurderinger og tiltak knyttet til disse	Avhandlingens hovedfokus er Norges petroleumsnæring, dermed er ikke sårbarhetene og anbefalingene som er omtalt i denne samfunnsfunksjonen relevant
13 – Energiforsyning	Kapittelet omhandler digitale sårbarheter i denne samfunnsfunksjonen samt utvalgets anbefalinger, vurderinger og tiltak knyttet til disse	Avhandlingens hovedfokus er Norges petroleumsnæring, dermed er ikke sårbarhetene og anbefalingene som er omtalt i denne samfunnsfunksjonen relevant
14 – Olje og gass		Kapittelet er omtalt i tabellen «**Utredningens særlig relevante deler**»

15 – Vannforsyning	Kapittelet omhandler digitale sårbarheter i denne samfunnsfunksjonen samt utvalgets anbefalinger, vurderinger og tiltak knyttet til disse	Avhandlingens hovedfokus er Norges petroleumsnæring, dermed er ikke sårbarhetene og anbefalingene som er omtalt i denne samfunnsfunksjonen relevant
16 – Finansielle tjenester	Kapittelet omhandler digitale sårbarheter i denne samfunnsfunksjonen samt utvalgets anbefalinger, vurderinger og tiltak knyttet til disse	Avhandlingens hovedfokus er Norges petroleumsnæring, dermed er ikke sårbarhetene og anbefalingene som er omtalt i denne samfunnsfunksjonen relevant
17 – Helse og omsorg	Kapittelet omhandler digitale sårbarheter i denne samfunnsfunksjonen samt utvalgets anbefalinger, vurderinger og tiltak knyttet til disse	Avhandlingens hovedfokus er Norges petroleumsnæring, dermed er ikke sårbarhetene og anbefalingene som er omtalt i denne samfunnsfunksjonen relevant
18 – Transport	Kapittelet omhandler digitale sårbarheter i denne samfunnsfunksjonen samt utvalgets anbefalinger, vurderinger og tiltak knyttet til disse	Avhandlingens hovedfokus er Norges petroleumsnæring, dermed er ikke sårbarhetene og anbefalingene som er omtalt i denne samfunnsfunksjonen relevant
19 – Kompetanse	«Dette kapittelet omhandler kunnskap og ferdigheter som må utvikles, videreformidles og fordeles i samfunnet for å sikre tryggest mulig bruk av IKT» (Digital sårbarhet - sikkert samfunn 2015, s.221)	
20 – Styring og kriseledelse	Skildring av styring og kriseledelse på sentralt, regionalt og lokalt nivå. Utvalgets anbefalinger, vurderinger og tiltak	Delkapitlene 20.1.1, 20.1.2 og 20.2.6 omhandler emner som er særs viktige for avhandlingen, og er beskrevet i tabellen «**Utredningens særlig relevante deler**»
21 – Avdekke og håndtere digitale angrep		Kapittelet er omtalt i tabellen «**Utredningens særlig relevante deler**»

22 - Felleskomponenter	Kartlegging av sårbarheter og utfordringer i samfunnets digitale fellesfunksjoner; Brønnøysundregistrene, Skatteetaten, Kartverket, Altinn og e-ID/Difi. Vektlegging av informasjonssikkerhet. Utvalgets anbefalinger, vurderinger og tiltak	
23 – Tverrsektorielle sårbarhetsreduserende tiltak		Kapittelet er omtalt i tabellen «**Utredningens særlig relevante deler**»
24 – Økonomiske og administrative konsekvenser	Utvalgets forslag til konkrete tiltak som reduserer og/eller forebygger digitale sårbarheter. Bl.a. nevnes det en styrking av Justis- og beredskapsdepartementets samordningsrolle, en reduksjon av kritikaliteten av Telenors kjernenett og en videreutvikling av varslingssystem for digital infrastruktur	
25 – Vedlegg	Oversikt over bidragsytere, anvendte rapporter, departementsansvar og tidligere sentrale utvalg	

Tabell to - Utredningens særlig relevante deler:

(basert på egen definisjon av viktighetsgrad i sammenheng med avhandlingens hovedtema og problemstilling)

Kapittel	Overordnet tema/innhold	Merknader	Begrunnelse
Kapittel 5 – Sikring av IKT og digital informasjon	Utgreiing om hva som definerer IKT-sikkerhet samt konkrete preventive tiltak (antivirus, «patching», brannmur). Digitale utfordringer i samfunnet		Gir et overblikk over hva som involverer IKT-sikkerhet, og ikke minst; hvordan norske fagpersoner definerer dette samt hvilke samfunnsutfordringer som blir lagt vekt på
Kapittel 6 – Trender som påvirker sårbarhetsbildet	Samfunnets økende digitalisering, internettilkobling i alt fra klær til hjem, og sikkerhetsutfordringene dette medfører. Utvikling i noen teknologiske felt (biometri og kryptografi)		Gir et inntrykk av hvor det digitaliserte samfunnet er på vei, inkludert det norske, og skaper med dette et generelt helhetsbilde av hvilken innvirkning cyberspace har på våre liv
Delkapittel 7.2 – Tilsiktede IKT-hendelser	Definisjon av tilsiktede IKT-hendelser: Digital kriminalitet, digitale angrep, spionasje, sabotasje, terror. Definisjon av hvem som utfører slike hendelser: Fra «script kiddies» til sofistikerte angripere/APT-er, avhengig av motiv for angrepet		Fokuset for avhandlingens problemstilling er tilsiktede IKT-hendelser, mer konkret; sabotasjehandlinger, altså *ikke* naturhendelser, systemsvikt, manglende kompetanse o.l.

Kapittel 8 – Organisering av ansvar og roller	Utgreiing av sentrale aktørers ansvar og myndighet innen IKT-sikkerhet. Justis- og beredskapsdepartementet er en av hovedbestanddelene i arbeidet med sikkerhet og beredskap, også innen cyberdomenet. Andre relevante aktører: FD, UD, NSM, DSB. Øvrige instanser: Responsmiljøer, interesseorganisasjoner, foreninger og koordineringsarenaer		Viktig kapittel som kartlegger myndighetenes og andre aktørers rolle i tilknytning til cybersikkerhet i Norge (og internasjonalt). Hjelper godt å få et bilde av samhandlingen og ansvarsfordelingen på IKT-sikkerhetsområdet
Kapittel 14 – Olje og gass	Aspekter knyttet til petroleumsvirksomheten i Norge: Roller og myndighetsansvar, petroleumsnæringens verdikjede, utvalgets vurderinger og anbefalte tiltak rundt digitale trusler i norsk olje- og gassvirksomhet	Kapittelet er betydelig basert på rapporten *Digitale Sårbarheter Olje & Gass* av DNV GL (2015), noe utvalget også gjør eksplisitt	Naturlig kapittel å fokusere på ettersom det overordnete hovedfokuset i avhandlingen er norsk petroleumsnæring
Delkapittel 20.1.1 – Hva er en krise?	En krise er noe som truer viktige verdier og svekker en organisasjons evne til å utføre nødvendige funksjoner. En krise kan få konsekvenser for samfunn, næringsliv og individer samt en stats integritet og suverenitet, avhengig av motiv og omfang (og aktør, hvis dette er kjent)		Gir noen definisjoner på hva som karakteriseres som en krise, noe som ofte er resultatet av en tilsiktet uønsket IKT-hendelse eller *cyberangrep*, noe som igjen er en del av avhandlingens hovedfokus

Delkapittel 20.1.2 – Sentral kriseledelse	Utgreiing om kriseledelse på sentralt nivå, som er et departementsansvar, og deres funksjoner på dette området. Tiltak for håndtering av kritiske IKT-hendelser		Først og fremst er det myndighetenes roller og ansvar som er av interesse for avhandlingen, dette defineres gjerne som det «sentrale nivået». Delkapittelet gir noen verdifulle utgreiinger om dette
Delkapittel 20.2.6 – Målrettede IKT-angrep	Norge må være forberedt på en rekke former for irregulær krig. Digitale angrep kan ha konsekvenser vi aldri før har sett, og kreve samordning på tvers av styringsnivåer og ansvarsområder		Målrettede digitale angrep henger tett sammen med det som ble omtalt i delkapittel 7.2, og er dermed av særs relevans for oppgaven
Kapittel 21 – Avdekke og håndtere digitale angrep	Roller og ansvar. Informasjonsdeling. Varsling, rapportering og håndtering skjer via flere samfunnsnivåer – dette medfører usikkerheter og uklarheter. Utvalgets vurderinger og anbefalinger rundt digital risikohåndtering i Norge		Kapittelet henger tett sammen med det som blir omtalt i kapittel 8 og delkapittel 20.1.2, og er dermed av vesentlig betydning for oppgaven

Kapittel 23 – Tverrsektorielle sårbarhetsreduserende tiltak	Utvalgets anbefalinger og forslag til tiltak innen ulike samfunnsenheter rundt reduksjon og håndtering av uønskede IKT-hendelser. Problematisering av utkontraktering og skytjenester. Meget negativ til en regulering av eller et forbud mot kryptografi		Kapittelet kan bli sett på som en oppsummering av utvalgets utredning hvor utvalget presenterer flere konkrete tiltak på tvers av forvaltning, næring, og virksomhet i Norge. Viktig kapittel ettersom utvalgte tiltak kan følges opp i avhandlingen for å vise progresjonen på disse og med det; det helhetlige forebyggende sikkerhetsarbeidet innen IKT

Vedlegg 3 – Oppfølging av Lysneutvalgets anbefalinger per vår 2018

Kapittel 14 – **Olje og gass**

(i Meld. St. 38: Kapittel 13 – **Olje og gass**)

Konkretisering av tiltak	Status
I november 2015 tok DNV GL initiativ til å utarbeide standardiserte krav til IKT-sikkerhet for olje- og gassnæringen med utgangspunkt i ISA/IEC-standardene. I dette arbeidet deltok blant andre en representant for Ptil. Arbeidet skulle resultere i en anbefalt praksis, og være ferdigstilt sommeren 2017.	Den anbefalte praksisen er ferdigstilt og lansert, og finnes på DNV GLs nettsider mot registrering.
HMS-forskriftene for petroleumsaktiviteten omtaler ikke konkret digitale trusler. Ptil har utarbeidet og hatt på høring et forslag til presisering av forskriftene. Ptil avventer oppfølgingen av forslag til ny sikkerhetslov (NOU 2016: 19 *Samhandling for sikkerhet – Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*) før de fastsetter regelverksendringer basert på denne.	Lovforslaget til ny sikkerhetslov er fortsatt under behandling. Resultatet av det er per dags dato uvisst, men det er stor sannsynlighet for at olje- og gassinstallasjonene vil bli omfattet av den nye sikkerhetsloven.
Vurdere tilknytning til et responsmiljø for IKT-hendelser, noe olje- og gassektoren ikke har i dag. KraftCERT ønsker petroleumssektoren velkommen til et samarbeid og medlemskap.	Det er ingenting som per i dag tilsier at petroleumssektoren har blitt medlem i KraftCERT.

Kapittel 21 – **Avdekke og håndtere digitale angrep**

(i Meld. St. 38: Kapittel 20 – **Digitale angrep**)

Konkretisering av tiltak	Status
I 2016 fikk NSM i oppdrag å utarbeide et utkast til helhetlig rammeverk for digital hendelseshåndtering. Utkastet skulle ferdigstilles i løpet av 2017.	Rammeverket er lansert og åpent for nedlasting på NSMs nettsider.
Regjeringen ønsker å videreutvikle og oppgradere sensorteknologien i VDI (varslingssystem for digital infrastruktur).	Noe vanskelig å finne konkret status på dette, men det er ikke utenkelig at systemet både utvikles og oppgraderes kontinuerlig.
Utrede innføringen av digital grenseovervåkning.	FD satte ned et utvalg for dette formålet (Lysne II-utvalget) som avga sin rapport 25.august 2016.

Kapittel 23 – **Tverrsektorielle sårbarhetsreduserende tiltak**

(i Meld. St. 38: Kapittel 22 – **Tverrsektorielle tiltak**)

Konkretisering av tiltak	Status
NSM jobber med å etablere et helhetlig og systematisk sett med de viktigste minimumskrav og tiltak for å sikre samfunnsviktige IKT-løsninger gjennom grunnprinsipper for IKT-sikkerhet. Den første tiltakspakken skal være publisert i løpet av 2017 med påfølgende revisjoner.	Pakken er ferdigstilt og kan hentes på NSMs nettsider.

Tydeliggjøre Justis- og beredskapsdepartementets rolle og ansvarsområde.	Utarbeidelsen av Meld. St. 10 (2016-2017) *Risiko i et trygt samfunn* presiserer JDs roller og ansvar. Dette kan karakteriseres som et konkret resultat av Lysneutvalgets anbefaling.
Utarbeide et felles metodisk rammeverk for, og en årlig helhetsoversikt over, digitale sårbarheter.	NSM har, fom. 2015, årlig gitt ut risikobilder som kartlegger de mest presserende truslene i cyberdomenet. NSM har også fått i oppdrag å videreutvikle rapportene i samarbeid med andre relevante virksomheter, deriblant DSB.