POLITIHØGSKOLEN

SIKKERHETSRÅDGIVNING

NORSKE MYNDIGHETERS SIKKERHETSRÅDGIVNING OVERFOR STORE NORSKE BEDRIFTER MED VIRKSOMHET I UTLANDET

Lars Lindén

MASTER I POLITIVITENSKAP 2015

Forord

Det har vært en spennende og svært lærerik prosess å arbeide med oppgaven. Det ville ikke latt seg gjennomføre uten tålmodighet og støtte på hjemmebane. Jeg er takknemlig for at informantene har tatt seg tid til intervjuene og etterfølgende oppfølgingsspørsmål. Gode råd og fokus på den «røde tråden» fra veileder Cato Hemmingby har vært uvurderlig og biveileder Gunnar Thomassen har bidratt ved den metodiske delen av oppgaven. Tord Skogedal Lindén har gitt mange gode og konstruktive innspill underveis. Jeg vil også benytte muligheten til å berømme biblioteket på PHS som alltid tar seg tid til å hjelpe.

Tromsø, 22. april 2015

Abstract

The subject of this thesis is security consulting. Security consulting is a topic that is little discussed in academical literature, and is a term without a precise definition. I have therefore developed the following definition for this thesis: Security consulting is advice and/or information provided with the intension to improve companies` (continuous) security work in order to prevent and/or handle intended undesirable incidents carried out by individuals or groups in the best possibly way. This security advisory can be said to have two tracks: 1) preventive advice, and 2) specific advice relating to an issue or an event. Security advisory is a part of what you would call the field of social security. It`s an interdisciplinary field, which use various methods. The counselling I examine are oriented towards security[1] – intentional undesirable incidents – what we in Norwegian can call *sikring*.

I have used a qualitative approach with semi structured interviews. The thesis is built up as a case study of security advice exerted by Norwegian authorities with major Norwegian companies with operations abroad. I have interviewed a total of eleven informants from five different Norwegian authorities, an advisory body established by the business sector (Næringslivets sikkerhetsråd), and two major Norwegian companies which operates abroad (Statoil and Telenor).

The thesis is based on four issues and the first question of my research is how does Norwegian authorities work concerning security advising to large Norwegian companies with operations abroad, and in which areas are such advice given? My study shows that Norwegian authorities conducts security consulting to large Norwegian companies with operations abroad. I find that Norwegian authorities carry out security consulting in their field of work, but this advice is of different nature and are perceived as non-regular. The second question is: to what extent is the contact between the participants and why do they cooperate, what type of contact do they have, and how frequent is this contact? My research shows that participants have varying contact, but due to the limitation of my data it`s not possible to estimate the frequency of this contact any closer. The contact varies from being directly to different types of open and impersonal information, as well as various

[1] In the Norwegian language security includes both safety and security. Security is used regarding intended undesirable incidents, and the concept safety is used regarding undesirable incidents.

forums with several present. What and with whom one can share information is a challenge for authorities. The third question is whether some actors collaborate more than others, and if yes why is it so? It appears that Politiets sikkerhetstjeneste (Police Security Service), Etterretningstjenesten (Norwegian Intelligence Service), Utenriksdepartementet (The Ministry of Foreign Affairs) and Nasjonal sikkerhetsmyndighet (National Security Authority) has a well function cooperation, and the use of liaisons at Utenriksdepartementet emerges to be positive for cooperation. The fourth question is the following: is it, on the basis of five serious incidents (including terrorist attacks), possible to see changes in security advice and dialogue between the authorities and companies? The terrorist attacks on 22. July 2011 was highlighted by several of my informants, and the hostage operation at In Amenas 2013 had accompanied a majority of informants to have increased focus on security consulting and use of this type of counseling.

The thesis provides a picture of how security consulting is exercised from Norwegian authorities with major Norwegian companies with operations abroad. This is a topic that does not at least have been highlighted in the aftermath of the terrorist attack on the oil and gas plant in In Amenas. What Norwegian authorities had of relevant information and whether this was passed on became a theme. The host country is responsible for security on its territory, while enterprises are responsible for their employees in accordance with Norwegian law. Through well-functioning security consulting, which is an appropriate method for exchanging information, the Norwegian authorities provide security advice and share information, and contribute to the companies' safety work. A coordinated security consulting, with one responsible and/or a coordinating authority, would be able to capture more of the challenges that have emerged in my data. As an example exchange of information between authorities. Importance of and challenges related to cooperation and coordination is pointed out in several public documents (Official Norwegian Reports, White papers), evaluation reports, and is also pointed out within the civil preparedness.

Sammendrag

Tittel: Sikkerhetsrådgivning - Norske myndigheters sikkerhetsrådgivning overfor store norske bedrifter med virksomhet i utlandet.

Student: Lars Lindén

Veileder: Cato Hemmingby

Biveileder: Gunnar Thomassen

Årstall: 2015

Oppgavens tema er sikkerhetsrådgivning. Sikkerhetsrådgivning er et tema som er lite behandlet i faglitteraturen, og et begrep som ikke har en bestemt definisjon. Jeg har derfor utviklet følgende definisjon for denne oppgaven: Sikkerhetsrådgivning er råd og/eller informasjon som gis i den hensikt å bedre virksomheters (kontinuerlige) sikringsarbeid for slik og best mulig å kunne forebygge og/eller håndtere tilsiktede uønskede hendelser fra personer eller grupper. Denne sikkerhetsrådgivningen kan sies å ha to spor: 1) forebyggende råd, og 2) spesifikke råd knyttet mot sak eller hendelser. Sikkerhetsrådgivning er en del av det en kan kalle *samfunnssikkerhetsfeltet*. Det er et tverrfaglig felt og det benyttes ulike metoder. Rådgivningen jeg undersøker er security-rettet[2] - tilsiktede uønskede hendelser - det som på norsk kan kalles sikring.

Jeg har benyttet en kvalitativ tilnærming med semistrukturerte intervjuer. Oppgaven er bygget opp som en casestudie av sikkerhetsrådgivningen som utøves av norske myndigheter overfor store norske bedrifter med virksomhet i utlandet. Jeg har intervjuet totalt elleve informanter fra fem ulike norske myndigheter, et rådgivende organ stiftet av næringslivet (Næringslivets sikkerhetsråd), og to store norske bedrifter med virksomhet i utlandet (Statoil og Telenor).

Oppgaven tar utgangspunktet i fire problemstillinger. Den første problemstillingen er hvordan bedriver norske myndigheter sikkerhetsrådgivning overfor store norske bedrifter

[2] Sikkerhet kan deles i security (sikring) og safety (trygghet). Safety er uønskede hendelser, mens security er tilsiktede uønskede hendelser.

med virksomhet i utlandet, og på hvilke områder gis det slik rådgivning? Mine data viser at norske myndigheter bedriver sikkerhetsrådgivning overfor store norske bedrifter med virksomhet i utlandet. Jeg finner at myndighetene driver sikkerhetsrådgivning innen sine arbeidsfelt, men denne rådgivningen er av ulik karakter og fremstår som ikke-regulær. Den andre problemstillingen er: i hvilken grad er det kontakt mellom aktørene og hvorfor samarbeider de, hvilken type kontakt har de, og hvor hyppig er denne kontakten? Oppgaven viser at aktørene har varierende kontakt, uten at det på bakgrunn av mine data lar seg gjøre å anslå hyppigheten på denne kontakten nærmere. Kontakten mellom aktørene varierer fra å være direkte til ulike typer åpen og upersonlig informasjon, samt ulike fora med flere tilstede. Hva en kan dele av informasjon og med hvem er en utfordring for myndighetene. Den tredje problemstillingen er hvorvidt noen aktører samarbeider mer enn andre, og hvorfor er det eventuelt slik? Det fremstår som at PST (Politiets sikkerhetstjeneste), E (Etterretningstjenesten), UD (Utenriksdepartementet) og NSM (Nasjonal sikkerhetsmyndighet) har et velfungerende samarbeid, og bruk av liaisoner i UD fremstår som å være positivt for samarbeidet. Den fjerde problemstillingen er: er det, på bakgrunn av fem alvorlige hendelser (blant annet terrorangrep), mulig å se endringer i sikkerhetsrådgivningen og dialogen mellom myndighetene og bedrifter? Terrorangrepet 22. juli 2011 ble trukket frem av flere av mine informanter, og gisselaksjonen i In Amenas 2013 hadde i følge et flertall av informantene økt fokuset på sikkerhetsrådgivning og bruken av denne type rådgivning.

Oppgaven gir et bilde av hvordan sikkerhetsrådgivning utøves fra norske myndigheter overfor store norske bedrifter med virksomhet i utlandet. Dette er et tema som ikke minst har blitt aktualisert i etterkant av terrorangrepet mot olje- og gassanlegget i In Amenas. Hva norske myndigheter hadde av aktuell informasjon og om dette ble formidlet videre ble da et tema. Vertslandet har ansvaret for sikkerheten på sitt territorium, mens bedriftene har ansvar for sine ansatte i henhold til norsk lovgivning. Gjennom velfungerende sikkerhetsrådgivning, som er en hensiktsmessig metode for informasjonsutveksling, kan norske myndigheter gi sikkerhetsråd og dele informasjon, og slik bidra til bedriftenes sikringsarbeid. En *samordnet* sikkerhetsrådgivning, med én ansvarlig og/eller koordinerende myndighet, kunne fange opp flere av utfordringene som er fremkommet i mitt datamateriale. Eksempelvis informasjonsutveksling mellom myndighetene. Viktigheten av og

utfordringer knyttet til samarbeid og samordning er påpekt i flere offentlige dokumenter (NOU, St.meld.), evalueringsrapporter, samt påpekt innen den sivile beredskapen.

Innholdsliste

Tabell- og figuroversikt

1. Innledning

I denne delen ser jeg nærmere på oppbygging av oppgaven, oppgavens tema og problemstillinger. Hva er sikkerhetsrådgivning og hvorfor dette er et aktuelt tema å undersøke nærmere? Oppgaven tar utgangspunkt i fire problemstillinger som her blir presentert. Begrepet sikkerhetsrådgivning blir diskutert og jeg presenterer oppgavens definisjon av dette begrepet. Caset blir deretter kort beskrevet.

1.1 Tema og problemstilling for studien

Sikkerhetsrådgivning er et tema som er lite behandlet i faglitteraturen[3] og det finnes ingen entydig definisjon på begrepet sikkerhetsrådgivning. I andre sammenhenger har begreper gjerne flere definisjoner, der ulike momenter vektlegges. Terrorisme og organisert kriminalitet er to eksempler på slike begreper. Dette er ikke tilfelle ved sikkerhetsrådgivning. I mangel på en definisjon av begrepet har jeg utviklet en definisjon av sikkerhetsrådgivning:

> Råd og/eller informasjon som gis i den hensikt å bedre virksomheters (kontinuerlige) sikringsarbeid for slik og best mulig å kunne forebygge og/eller håndtere tilsiktede uønskede hendelser fra personer eller grupper.
>
> Sikkerhetsrådgivningen kan sies å ha to spor: 1) forebyggende råd, og 2) spesifikke råd knyttet mot sak eller hendelser.

Samfunnssikkerhet[4] og organisering av denne har hatt stort fokus det siste tiåret og det er produsert flere NOU-er (Norges offentlige utredninger) i denne sammenheng (Meld. St. 29 (2011-2012), 2012; NOU 2012:14, 2012). Terrorangrepet mot regjeringskvartalet og Utøya 22. juli 2011 og terroranslaget mot oljeraffineriet i In Amenas 16. januar 2013 har medvirket til opprettholdelse av denne oppmerksomheten. Angrep mot Telenors butikker i Pakistan i

[3] Utover egne søk har jeg fått søkehjelp på biblioteket ved Politihøgskolen og kontaktet flere eksperter.
[4] Kan på engelsk oversettes til *social security* (Forskningsrådet, 2011).

2006[5] som følge av Muhammed-karikaturene er et annet eksempel som har fått medieomtale (Ellingsen & Zaman, 2006; Iversen, 2006). «Samfunnssikkerhet er et tvetydig og omdiskutert begrep både i norsk politisk sammenheng og i internasjonal akademisk kontekst» (Fimreite, Langlo, Lægreid, & Rykkja, 2014, s. 17). Begrepet som mangler en omforent definisjon, handler om risiko i samfunnet og samfunnets sårbarhet (Fimreite et al., 2014, s. 17). Sikkerhetsrådgivning som er et av flere tiltak som kan medvirke til en bedre forståelse og håndtering av risiko og sårbarheter kan slik plasseres innen *samfunnssikkerhetsfeltet*. Ansvaret for samfunnssikkerheten er tillagt flere departement, offentlige instanser og ulike private eller offentlige aktører. Det er krevende å håndtere det differensierte ansvaret på en slik måte at det ikke forringer sikkerheten. Ved virksomhet i andre land er dette landets myndigheter en av aktørene. Kombinasjonen av uklarhet i begrepsbruk og ansvarsforhold er en utfordring både med tanke på sikkerhetsrådgivning som jeg undersøker nærmere i denne oppgaven, forebygging og operativ innsats.

Sikkerhetsarbeid (security og safety) er blitt en del av norske bedrifters virksomhet, også ved deres virksomhet i andre land. Eksempelvis virksomhet innen teknologi-, og olje- og gassnæring. Dette er også et samfunnsansvar som påligger myndighetene i landet en opererer i og er slik et samarbeid mellom offentlige myndigheter og private aktører. Jeg ser nærmere på hvordan norske myndigheter bedriver sikkerhetsrådgivning (formidler sikkerhetsråd) med utgangspunkt i fire problemstillinger:

1. Hvordan bedriver norske myndigheter sikkerhetsrådgivning overfor store norske bedrifter med virksomhet i utlandet, og på hvilke områder gis det slik rådgivning?
2. I hvilken grad er det kontakt mellom aktørene og hvorfor samarbeider de, hvilken type kontakt har de, og hvor hyppig er denne kontakten?
3. Er det noen aktører som samarbeider mer enn andre, og hvorfor er det eventuelt slik?

[5] Jyllandsposten (Danmark) publiserte Muhammed-karikaturene 30. september 2005, i Norge ble karikaturene publisert i Magazinet 10. jan 2006 (Tønnesen, 2008, s. 1). Urolighetene i etterkant av publiseringen av karikaturene kan ses på som en lengre periode med uroligheter fra slutten av 2005 og utover 2006. Det var en alvorlig situasjon i slutten av 2005 og anslag mot Telenors butikker fant sted i februar 2006. Muhammed-karikaturer har også vært aktuelle gjentatte ganger etter dette, den siste tiden i forbindelse med terrorangrepet mot Charlie Hebdo januar 2015.

4. Er det, på bakgrunn av de fem referansehendelsene, mulig å se endringer i sikkerhetsrådgivningen og dialogen mellom myndighetene og bedrifter?

Terrorangrepet mot In Amenas har aktualisert sikkerhetsrådgivning og det er stilt spørsmål ved hvordan norske myndigheter kan bistå norsk virksomhet i utlandet på en best mulig måte. En av anbefalingene i In Amenas-rapporten belyser dette ved å ta for seg samarbeid og nettverk:

> Utvide og styrke samarbeidet med relevante myndigheter og organisasjoner. Styrke eksterne nettverk og relasjoner. Etablere standarder for innsyn og innflytelse på sikkerhetsområdet i joint venture-selskaper og partnersamarbeid (Statoil ASA, 2013a, s. 6; 2013b).

Videre har Utenriksdepartementet (UD) i sin evaluering av norske myndigheters krisehåndtering ved In Amenas-angrepet funnet fire områder som må undersøkes nærmere. Punkt fire er *Sikkerhetsinformasjon til norske virksomheter i utlandet*. Under dette punktet kan vi lese at: «Som ledd i oppfølgingen av statsministerens redegjørelse i Stortinget 23. januar, vil Justis og beredskapsdepartementet lede et arbeid for å vurdere hvorvidt norske myndigheter ytterligere kan bistå norske virksomheter i utlandet i spørsmål av sikkerhetsmessig karakter» (Utenriksdepartementet, 2013, s. 37). Vi har flere norske selskaper med virksomhet i utlandet, hvorav Statoil, Yara, Jotun og Telenor er noen av dem. Sikkerhetsrådgivningen selskapene kan motta eller mottar er en del av deres sikkerhetsarbeid. Dette bør inngå i selskapenes risikovurderinger[6]. Dersom aktøren deltar i et joint venture-samarbeid, slik tilfelle er ved In Amenas-anlegget, kan det gjøre samarbeidsrelasjoner ytterligere utfordrende ved at det er flere interessenter samlokalisert.

Intervjuer med flere myndigheter og store norske bedrifter med virksomhet i utlandet (nærmere beskrevet i punkt 1.3) gjør at jeg kan gi et bilde av hvordan sikkerhetsrådgivningen fungerer. Sikkerhetsrådgivning er lite omtalt i faglitteraturen. Dette til tross for at det er et betydningsfullt område der bedriftene kan få nyttig informasjon, samtidig som

[6] Når jeg i oppgaven bruker risiko-, verdi- og trusselvurdering inngår sårbarhetsanalyse som en del av dette.

myndighetene kan ivareta sine oppgaver overfor norske interesser i utlandet. Oppgaven bidrar med kunnskap om dette viktige *sikkerhetsfeltet*. Det at informantene var så positive til oppgavens tema og ønsket mer kunnskap om dette feltet, viser at det er behov for mer kunnskap og forskning om sikkerhetsrådgivningen som bedrives av myndighetene overfor bedriftene. Det er motiverende at de som bedriver og mottar slik sikkerhetsrådgivning ønsker oppgavens tema belyst og undersøkt.

Forskningsprogrammet SAMRISK[7] (2006-2011) «…frembrakte mye ny kunnskap, men avdekket også betydelige behov for ny forskning innen feltet samfunnssikkerhet» (Programplanutvalget, 2013, s. 3). Det nye programmet for samfunnssikkerhet, SAMRISK II (2013-), skal imøtekomme dette behovet (Programplanutvalget, 2013). Internasjonalisering trekkes frem og det er ønskelig at programmets forskningsprosjekter har et internasjonalt preg (Programplanutvalget, 2013, s. 4). Privat norsk virksomhet i utlandet nevnes ikke eksplisitt i programmet, men sikkerhetsrådgivningen norske myndigheter bedriver overfor norske bedrifter i utlandet har en internasjonal dimensjon. Sikkerhetsrådgivningen jeg vil undersøke har internasjonale forgreininger ved at trusler en ønsker å gardere seg mot i større og større grad er globale trusler uten landegrenser. Norske myndigheters sikkerhetsrådgivning vil kunne ses opp mot andre lands utførelse av sikkerhetsrådgivning. Norske virksomhet i utlandet har vært og vil i fremtiden eksponeres for globale trusler som etterretningsvirksomhet, spionasje, organisert kriminalitet og terrorisme. Globalisering påvirker norsk virksomhet i utlandet og kan sies å være «the intensification of economic , political, social and cultural relations across borders» *(Lia, 2005, s. 18)*. En av følgene av at verden i stadig økende grad globaliseres er at ikke-statlige aktører, herunder store multinasjonale selskaper, får større innflytelse på bekostning av statlige myndigheter. Dette kan gjøre virksomhetene til interessante mål for å oppnå oppmerksomhet. I Trusler og sårbarheter 2013 kan vi lese at globaliseringen krever samarbeid og informasjonsutveksling mellom Politiets sikkerhetstjeneste, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet (Etterretningstjenesten, Nasjonal sikkerhetsmyndighet, & Politiets sikkerhetstjeneste, 2013). *Forebygging av terrorisme og andre tilsiktede handlinger med stort skadepotensiale* er et av SAMRISK II sine prioriterte forskningstemaer (Programplanutvalget, 2013, s. 5).

[7] Forkortelse for Samfunnssikkerhet og risiko.

Sikkerhetsrådgivning kan være et av flere tiltak for å forebygge slike tilsiktede handlinger, og ytterligere kunnskap om dette temaet kan slik være et bidrag til dette.

Begrepsforståelse er viktig ved samarbeid og informasjonsutveksling. Kjennskap til hvilken betydning samarbeidende aktører legger i uttrykkene er en avgjørende forutsetning for samhandlingen. En felles begrepsforståelse vil være en styrke og begrense misforståelser. Statoil har fått kritikk gjennom media for ikke å ha tatt sikkerheten alvorlig nok ved sine anlegg i inn- og utland (Steiro, 2013). Til tross for urolighetene i området og kunnskap om dette endret ikke Statoil på sikkerheten ved In Amenas-anlegget. Et tettere samarbeid og større informasjonsflyt mellom Statoil og norske myndigheter kunne muligens påvirket deres risikoforståelse og risikoerkjennelse på en slik måte at hendelsen fikk et annet utfall. Manglende risikoforståelse og -erkjennelse er tema også i 22. juli-rapporten (NOU 2012:14, 2012) og flere andre offentlige rapporter/vurderinger (Etterretningstjenesten et al., 2013; Nasjonal sikkerhetsmyndighet, 2014).

1.2 Avgrensing og definisjon av sikkerhetsrådgivning

Tema for oppgavens problemstillinger er sikkerhetsrådgivning og jeg fokuserer på hvordan myndighetenes rådgivning bedrives overfor bedriftene og på hvilke områder det gjøres. Jeg vil i stor grad benytte meg av definisjoner hentet fra terminologien i Norsk Standard 5830:2012 (2012). Norsk standard «…fastsetter terminologi til bruk innenfor fagområdet sikring (beskyttelse mot og håndtering av tilsiktede uønskede handlinger)» (Standard Norge, 2012, s. 2). Oppgavens tema er først og fremst rådgivning opp mot tilsiktede uønskede hendelser og standarden er derfor passende. Videre er en felles begrepsterminologi et godt (og kanskje nødvendig?) grunnlag for effektiv sikkerhetsrådgivning, noe jeg ønsker å bidra til med denne oppgaven.

1.2.1 Sikkerhetsrådgivning

Sikkerhetsrådgivning er som nevnt et begrep uten en klar definisjon og kan dermed tillegges ulik betydning. Begrepet er eksempelvis ikke definert i Norsk Standard (Standard Norge, 2012). Det er flere ting som kan komme inn under begrepet, noe intervjuene jeg har gjennomført viser. Det kan spenne fra informasjon og veiledninger tilgjengelig for alle på nettet, til direkte kontakt mellom ulike aktører. Det kan være kommunikasjon én til én, én til flere, eller én til alle. Det kan gjøres direkte og/eller via andre.

Sikkerhetsrådgivning er sammensatt av to ord: sikkerhet og rådgivning. Rådgivning slik jeg bruker det i definisjonen kan forklares med å gi innsikt og forståelse i eller informasjon om et aktuelt tema eller problemstilling. Det kan være informasjon som en kan bruke slik den foreligger eller som en del av sitt totale vurderingsgrunnlag, eventuelt mer spesifikke forslag til tiltak. Informasjon som gis for at bedriftene skal ha et best mulig utgangspunkt for sine vurderinger av risiko og trusler faller dermed inn under definisjonen jeg bruker av begrepet sikkerhetsrådgivning. Sikkerhet kan deles i to: safety og security (NOU 2006:6, 2006). Sikkerhetsrådgivning faller inn under security eller det som på norsk kan kalles *sikring*. Differensieringen mellom de to begrepene forklares nærmere i kapittel to. Ved å legge denne forståelsen til grunn ser jeg bort fra naturkatastrofer, og ulykker/uhell som eksempelvis kan skyldes at en ikke følger fastlagte prosedyrer (safety).

Rådgivning knyttet til definisjonens andre spor (spesifikke råd knyttet mot sak eller hendelser) gis gjerne i en pågående beredskaps- eller krisesammenheng. Dette er også en viktig side av rådgivningen, gjerne i kombinasjon med forebyggende råd i forkant av slike situasjoner (definisjonens første spor).

For å kunne gi virksomheter tilpassede råd er man avhengig av god innsikt i virksomhetens situasjon og utfordringer. Denne innsikten forutsetter at virksomheten først gjennomfører en analyse. En kvalitativ god og til en hver tid tidsoppdatert analyse gir et godt beslutningsgrunnlag for rådgivning og tiltak. Tilsvarende vil en overfladisk analyse, eksempelvis gjennomført bare fordi det er et pålegg i en virksomhetsplan, forringe muligheten for tilpassede tiltak og råd. Analysen kan gjennomføres av virksomheten selv eller gjennom samarbeid med andre. På PST sine nettsider kan vi lese at «for å gi gode råd

om tryggingsspørsmål krevst det ein analyseprosess føreåt» (Politiets sikkerhetstjeneste, u.å.)[8]. Samt at kvalifiserte råd utfra analysen krever gode opplysninger fra ulike kilder.

1.2.2 Risikoforståelse og risikoerkjennelse

Begrepene risikoforståelse og –erkjennelse har vært mye benyttet i forbindelse med og i etterkant av evalueringen av 22. juli. Da det kan være (stor?) forskjell på hva man hevder å synes er viktig og hva man faktisk vektlegger vil jeg forklare begrepene nærmere her. Dette kan være problematisk ved sikkerhetsrådgivning som ved andre sikkerhetsrelaterte områder. Både for myndigheter («sender») og bedriftene («mottaker») av slik rådgivning. Bevissthet rundt egen virksomhet og risiko er viktig for å være mottakelig for og for å etterspørre sikkerhetsrådgivning. Begrepene vil derfor bli gjennomgått. Hvordan skal vi forstå begrepene risikoforståelse og risikoerkjennelse? Er det to uavhengige begrep der en kan oppfylle kravene til det ene, men ikke det andre? Eller er begrepene gjensidig avhengig av hverandre?

Trussel er en «mulig uønsket handling eller forhold som kan føre til en uønsket handling» (Standard Norge, 2012, s. 4). Risiko er et «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (Standard Norge, 2012, s. 5). Sårbarhet er «manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for en uønsket påvirkning» (Standard Norge, 2012, s. 5). *Risikoforståelse* kan forklares som det å ha kunnskap om hvilken risiko og tilhørende sårbarhet som til enhver tid er og kan bli aktuell. *Risikoerkjennelse* kan forklares som det å ta kunnskapen om risiko og sårbarhet innover seg på en slik måte at en det medfører nødvendige tiltak både i forebyggende øyemed og ved konkrete hendelser. 22. juli-rapporten påpeker forskjellen mellom begrepene (NOU 2012:14, 2012). Vi hadde kunnskapen, eksempelvis gjennom erfaringer fra øvelser, men dette førte ikke til nødvendige og påpekte behov for endringer. «En forutsetning for god risikoerkjennelse er at det foreligger gode analyser av risiko og sårbarheter. Dette er imidlertid ikke tilstrekkelig. God risikoerkjennelse forutsetter at kunnskapen blir anvendt og at sårbarhetsreduserende

[8] Henvisninger til nettsider i oppgaven har ikke sidetall.

tiltak iverksettes om nødvendig» (Meld. St. 21 (2012-2013), 2013, s. 115). Slik jeg forstår begrepene kan en ha risikoforståelse uten å erkjenne (vedkjenne seg) risikoen. Risikoerkjennelse krever derimot risikoforståelse. En endring i synet på og økning i bruken av sikkerhetsrådgivning vil kunne være et eksempel på et ønske om større risikoforståelse. Utgangspunktet for risikoerkjennelse vil da bli bedret.

1.3 Beskrivelse av caset

Oppgaven er gjennomført som en casestudie. Jeg intervjuet informanter hos fem norske myndigheter og et rådgivende organ stiftet av næringslivet. Samt benyttet meg av åpne kilder for å belyse sikkerhetsrådgivningen som bedrives. Myndighetene som ble intervjuet er Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM), Forsvarets sikkerhetsavdeling (FSA), Utenriksdepartementet (UD), og Kripos sin næringslivskoordinator i Næringslivets sikkerhetsråd (NSR). NSR er det nevnte rådgivende organet stiftet av næringslivet. I UD ble flere informanter intervjuet. På bedriftssiden intervjuet jeg informanter hos to store norske bedrifter med lengre virksomhetserfaring i utlandet. Nærmere bestemt Statoil, Telenor Group og Telenor Norge AS.

Det blir benyttet fem referansehendelser i oppgaven: 1) anslaget mot den norske ambassaden i Damaskus i 2006[9], 2) anslag mot Telenors butikker i Pakistan i 2006, 3) piratkapringer i Adenbukta og omkringliggende områder (2006-), 4) terrorangrepet mot regjeringskvartalet og Utøya (2011), og 5) terrorangrepet mot In Amenas-anlegget i Algerie (2013).

Med utgangspunkt i en omfattende datainnsamling belyser jeg sikkerhetsrådgivningen som gis og sammenligner hvordan denne rådgivningen benyttes.

[9] I motsetning til 22. juli som er en klart avgrenset hendelse en bestemt dag, kan tiden referansehendelsene anslaget mot den norske ambassaden i Damaskus og anslag mot Telenors butikker Pakistan fant sted forstås som en lengre periode med uroligheter. Dette er som følge av Muhammed-karikaturer aktuelt enda, eksempelvis terrorangrepet mot Charlie Hebdo januar 2015.

1.4 Oppgavens videre oppbygging

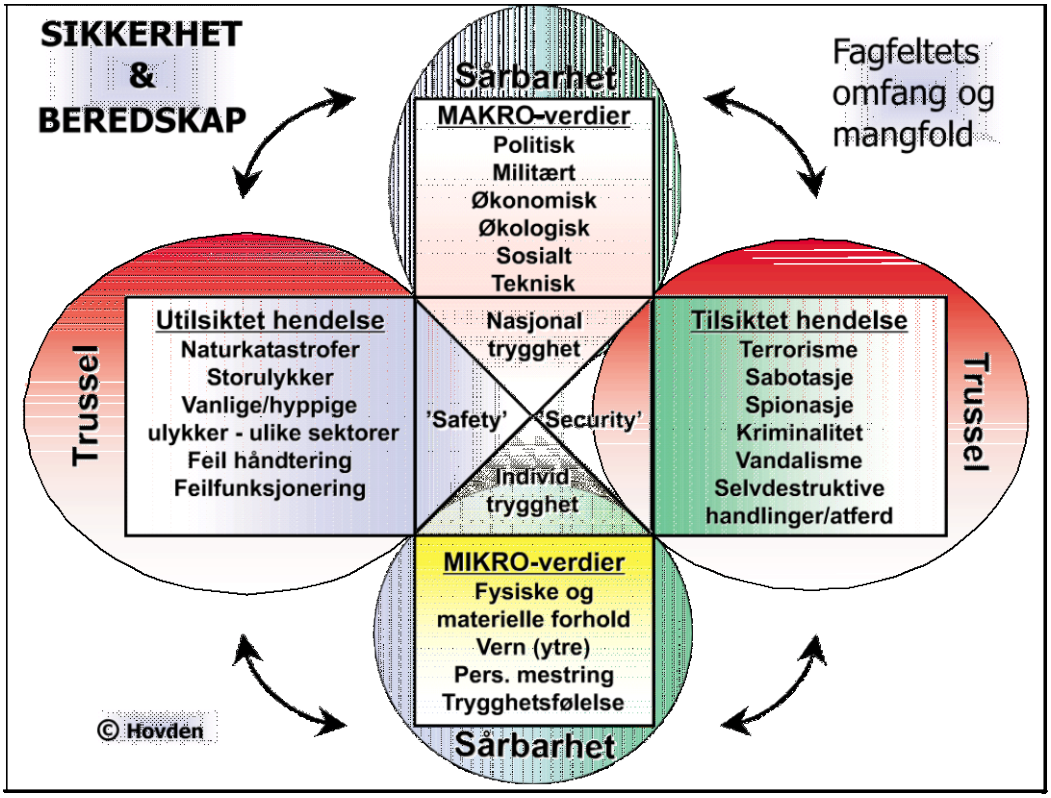
I oppgavens andre kapittel ser jeg nærmere på teori, forskning og utredninger som kan relateres til sikkerhetsrådgivning. Dette blir videre brukt i oppgavens analyse og funn-kapittel. Det tredje kapittelet er viet til å plassere oppgaven vitenskapsteoretisk og beskrive metode og forskningsdesign. Kapittel fire, som er det mest omfattende kapittelet i oppgaven, besvarer oppgavens fire problemstillinger. Analysens vurderinger og funn blir presentert med utgangspunkt i de fire problemstillingene. Det siste og femte kapittelet oppsummerer funnene i oppgaven, har forslag til videre forskning og hvilken betydning jeg mener funnene har.

2. Teori, forskning og utredninger på feltet

2.1 Innledning

I dette kapittelet vil jeg se nærmere på teori som kan knyttes til sikkerhetsrådgivning. Jeg bruker det jeg finner av litteratur og trekker veksler på litteratur fra andre tilstøtende felt som etterretning/analyse og kommunikasjon. Informasjonsutvekslingen som ligger implisitt i denne rådgivningen bygger på forståelse og tolkning av det vi kan kalle ulike varsler (signaler). Etterretning og analyse i forkant av sikkerhetsrådgivningen er en forutsetning for å kunne gi korrekte og situasjonstilpassede (bedriftstilpassede) råd. Signaler og tolkning av disse er derfor en del av oppgaven. Hva som formidles eller ikke formidles, hvorfor, hvordan og når dette gjøres er vesentlig når jeg ser nærmere på rådgivningen fra myndigheter til bedrifter. Teorien vil jeg benytte i funn- og analysekapittelet der jeg knytter teorien opp mot funn i datamaterialet. Da teori og forskning relatert til temaet sikkerhetsrådgivning i flere sammenhenger også kan knyttes til ulike utredninger (NOU, stortingsmeldinger, evalueringsrapporter m.m.) vil jeg benytte meg av slike. Noen av utredningene har mer eller mindre egne teoribolker. I *Når sikkerheten er viktigst* er det eksempelvis et eget avsnitt (3.10 Safety og Security - på norsk) der begrepene safety og security gjennomgås (NOU 2006:6, 2006). Dette avsnittet har igjen et utdypende vedlegg (begrepsutredning) som går over fem sider. Avsnittet *Sikkerhetsforskningens mangfold og omfang* i *Et sårbart Samfunn* er et annet eksempel (NOU 2000:24, 2000).

Samfunnssikkerhet og sikkerhetsforskning er et mangfoldig og tverrfaglig felt, noe som tydelig fremgår i figuren under:



Figur 1: Illustrasjon av sikkerhetsforskningens omfang og mangfold – et tankekors (Figur 25.1) (Hovden, 1998; NOU 2000:24, 2000, s. 287)[10].

Figuren har to akser hvor den ene spenner fra safety til security. To begreper som er inngående beskrevet senere i kapittelet. Den andre aksen spenner fra makronivå (nasjonalt og slik jeg forstår det også internasjonalt) til mikronivå (grupper og individ). Figuren viser hvor stort og bredt sikkerhetsforskningsfeltet er (NOU 2000:24, 2000). Foruten å vise bredden vil jeg bruke figuren til å plassere min oppgave innen sikkerhetsforskningen. Oppgaven ser nærmere på rådgivning innen tilsiktede handlinger, *security-siden* i modellen, og aktørene er myndigheter og bedrifter. Det er bedriftene som er mottaker av rådgivningen, selv om det kan gis hensiktsmessig informasjon begge veier. Det er

[10] Figuren er ikke identisk med figuren i utredningen *Sikkerhetsforskning* (Hovden, 1998, s. 13). Figuren benyttet i NOU 2000:24, samt brukt her i oppgaven, fremstår som en bearbeidet utgave av figuren fra forannevnte utredning.

vanskeligere å plassere oppgaven i forhold til mikro- og makronivå. Tilsiktede hendelser mot store norske bedrifter med virksomhet i utlandet kan eksempelvis få økonomiske og politiske konsekvenser (makro-verdier i modellen). Samtidig kan enkeltindivid bli skadelidende og rådgivningen kan være rettet mot fysiske og materielle forhold slik som grunnsikring[11] (mikro-verdier i modellen). Grunnsikring kan forklares som «…et etablert sikkerhetsregime for å ivareta sitt grunnleggende sikkerhetsbehov» (Nasjonal sikkerhetsmyndighet, Politidirektoratet, & Politiets sikkerhetstjeneste, 2010, s. 6). Sikkerhetsrådgivning dekker dermed et stort spekter (felt) og truslene en gir råd i forhold til kan om de inntreffer føre til (mer eller mindre alvorlige) konsekvenser, reaksjoner og handlinger på mikro- og makronivå[12]. Oppgaven plasseres derfor ikke på et bestemt sted av denne *mikro-makro-aksen*.

Sikkerhetsrådgivning kan som nevnt i oppgavens innledende kapittel deles i to spor: 1) forebyggende råd, og 2) spesifikke råd knyttet mot sak eller hendelser. Bedrifter kan motta rådgivning knyttet til begge disse sporene. Forebyggende rådgivning (spor nr. 1) som er mottatt og benyttet av bedriftene kan gi et godt grunnlag for ytterligere rådgivning knyttet til sak og hendelser (spor nr. 2). Spor nr. 2 kan i mange tilfeller være en del av en pågående operativ innsats. Informantene er ikke spurt hvordan de eventuelt er gitt råd under pågående saker slik som underveis i In Amenas-angrepet i 2013 eller under anslagene mot Telenors butikker i Pakistan i 2006.

2.2 Informasjonsdeling og forståelse av varsler

Implisitt i sikkerhetsrådgivning ligger formidling av informasjon. Det kan være generell eller spesifikk informasjon. Generell informasjon kan være landinformasjon, informasjon om generelle trusler etc. Spesifikk informasjon kan være knyttet til hendelser en må ta hensyn til der en har sin virksomhet, steds- og/eller bransjespesifikk informasjon etc. Informasjonen kan være toveis ved at myndigheter gir informasjon til bedrifter og mottar informasjon fra dem. Hva som formidles er avhengig av vurderingen som gjøres av opplysningene som

[11] Grunnsikring kan være et omfattende arbeid med mange involverte og innbefatte flere anlegg (i inn- og utland). Like fullt mener jeg det er riktig å kalle det en mikroverdi.
[12] Det kan også dreie seg om abstrakt risiko (NOU 2000:24, 2000, s. 287).

foreligger. Det har vært flere hendelser der en i ettertid ser at en i større grad kunne forutsett det som skjedde om en hadde tolket informasjonstilfanget korrekt. Angrepet på den amerikanske marinebasen Pearl Harbour (7. desember 1941) og Al-Qaidas terroranslag mot USA 11. september 2001 (9/11) er to kjente eksempler (Agrell, 2005). Terroranslagene i Frankrike januar 2015 gjør at det stilles spørsmål ved franske sikkerhetsmyndigheters og styresmakters håndtering av informasjonen de hadde om terroristene i forkant av hendelsene (Johnsen, 2014). Fremmedkrigere[13] har over lengre tid hatt stort søkelys og «allerede i 2003 var [Kouachi-brødrene] en del av en gruppe mennesker som jobbet for å sende franske jihadister til Irak» (Brenna et al., 2015). I VG kunne vi lese at gjerningspersonene fra Paris- og Københavnterroren har vært i politiets søkelys i forkant av hendelsene (Mjaaland & Wibe-lund, 2015). Det er flere utfordringer ved vurderingen som skal gjøres og forklaringer på hvorfor en kan tolke signalene feilaktig. I følge Agrell er det vanskeligere å avdekke terroraksjoner sammenlignet med militære aksjoner da de har ulikheter i beslutningstaking og forberedelser (Agrell, 2005, s. 31). Likefult var ingen av de to nevnte hendelsene (Pearl Harbour og 9/11) det vi kan kalle «lyn fra klar himmel» eller «blixt från en blygrå himmel» som Agrell skriver (2005, s. 31). Varsler og signal er særlig utfordrende ved tilsiktede handlinger utført av enkeltpersoner. «I slike situasjoner kan det ikke påregnes noen varslingstid, og tradisjonelle beredskapstiltak vil ha liten eller ingen effekt» (Politiets sikkerhetstjeneste, 2015, s. 3). I Programplanen for SAMRISK II vises det til vanskeligheter med «…å ta høyde for alle relevante signaler og forstadier til risiko» (2013, s. 17). Både falske negative indikasjoner og falske positive signaler er problematisk.

Utredningen etter 11. september skulle undersøke hva sikkerhetstjenestene visste eller burde visst, identifisere eventuelle systemfeil, og foreslå forbedringer (Agrell, 2005, s. 37-38). 11.september-kommisjonen fant at systemet ikke tilrettela for samarbeid, og at ansvar og oppfølging av varsler var diffus (Agrell, 2005). Wermdalen viser til at det er visse likheter mellom konklusjonene etter 11. september og 22. juli: manglende fantasi (forestillingsevne), manglende lovgivning, manglende evne til å håndtere trusselen, og manglende informasjonsdeling mellom myndighetene (2013, s. 523-525). Joint venture er «…et samarbeidsprosjekt der to eller flere foretak, gjerne fra forskjellige land, deler eierskap,

[13] Fremmedkrigere («foreign fighter») kan defineres som: «…someone who leaves or tries to leave the West to fight somewhere else (Hegghammer, 2013b, s. 1). En annen definisjon er «en person som kjemper en annens krig som tredjepart» (Politiets sikkerhetstjeneste, 2015, s. 9).

kontroll og risiko» (Vikøren, u.å.). Offentlig privat samarbeid kan være basert på en joint venture-avtale der risikoen er delt (Nærings- og Handelsdepartementet, 2003). På lik linje med uklare ansvarsforhold mellom samarbeidende tjenester og myndigheter, kan det være et tilsvarende problem ved joint venture-samarbeid. Gasslandanlegget In Amenas i Algerie, er og var et slikt samarbeidsprosjekt. Firmaene som samarbeidet da terroranslaget inntraff 16. januar 2013 var Sonatrech (et algerisk statseid olje- og gasselskap), BP (British Petroleum) og Statoil (Statoil ASA, 2013b). Ved joint venture-samarbeid og installasjoner for øvrig kan en benytte seg av private sikkerhetsselskap.

Det kan skilles mellom signaler og støy (brus). Støy er informasjon som fremstår som relevant, men i ettertid viser seg å ikke være relevant eller feilaktig (Agrell, 2005). Dette skillet er ofte tydelig først i etterkant. Signaler og støy tolkes innen en tolkningsramme og informasjon som faller utenfor rammen eller ikke passer inn med det en ser etter kan føre til feiltolkninger. Dette kan sammenlignes med Kuhns paradigmer. «Et […] paradigme bestemmer hva som skal gjelde som fakta, hvordan disse faktaene skal tolkes, hvilke konklusjoner man kan trekke av forskjellige fakta osv.» (Fjelland, 1999, s. 112). Rammeforutsetningene legger begrensninger på hvilke varsler som identifiseres, og vel så viktig hvordan det *tillates* å tolke varslene. Faren er tilstede for at en forbereder seg på det som har skjedd tidligere og ikke det fremtidige. Varslingssystemer bygger på mønstergjenkjenning og tolkningsrammer (Agrell, 2005), men en må også kunne identifisere og analysere det ukjente og uvanlige. Nye typer hendelser, kjente hendelser i uvante kombinasjoner eller med ukjente konsekvenser, og fremmede aktører som opptrer på en annen måte skaper vanskeligheter (Agrell, 2005, s. 89). Revisjonsterskler og paradigmer kan være et analyse- og varslingshinder (Agrell, 2005). Motstanden mot å endre mening, og det å se ting på nye måter legger da begrensninger på forståelsen av informasjon. Hvem som har definisjonsmakt, og gruppedynamikk er da vesentlige faktorer. Fokus og søken etter bestemte bekreftelser kan føre til selvoppfyllende resultat (confirmation bias). I National intelligence and science kan vi lese at amerikansk etterretning på 70- og 80-tallet hadde en tendens til å se etter informasjon som validerte deres antagelser og tidligere konklusjoner (Agrell & Treverton, 2015, s. 43-44). Agrell (2005) bruker uttrykkene revirforsvarer (revirförsvarere) og revirinntrenger (revirintränglingar): dersom det å bestemme over eget felt blir viktigere enn å imøtese konstruktive innspill og samarbeid er det svekkende for

produktet en skal levere. På en *reaksjonsskala* kan ytterkantene være over- og underreaksjon. En overreaksjon kan være det Romarheim, i forbindelse med reaksjoner på terror, kaller en kraftfull reaksjon (Romarheim, 2012). På den ene siden kan en la være å reagere på noe en skulle håndtert, mens en på den andre siden håndterer det på en unødvendig og omfattende måte. Agrell viser til fire ulike problemer knyttet til over- og underreaksjon (2005, s. 107-108). For det første risiko for kritikk for å komme med for mange varslinger («alarmism»). For det andre at det fører til en gradvis tilvenning og dermed lavere beredskap («ulv-ulv»). Kostnader er det tredje problemet og uforutsette skadevirkninger det siste. I etterkant av den forhøyede terrorberedskapen i Norge (sommeren 2014) har det eksempelvis vært stilt spørsmål med om tiltakene var for omfattende og om det var riktig å gå åpent ut og informere om terrortrusselen (Jakobsen, 2014). I forbindelse med det oppdaterte trusselbildet høsten 2014 har Martin Bernsen, informasjonssjef i PST, uttalt at åpenhet kan være problematisk og at advarsler kan svekke PSTs troverdighet (Klassekampen, 2014). Dette slik jeg forstår det fordi informasjonen kan oppfattes som det Agrell kaller «ulv ulv».

Agrell deler varsler i fire hovedtyper: treff, manglende varsel, falsk alarm, og korrekt avvist (Agrell, 2005, s. 110). Ved den første typen får en et varsel og hendelsen finner sted. Ved den andre typen får en ikke varsel til tross for at hendelsen skjer. Ved den tredje formen får en varsel selv om det ikke skjer noe. Til sist har vi intet varsel og ingen hendelse.

Utredninger kan deles inn i tre kategorier (Wermdalen & Nilsson, 2013, s. 575): *reaktiva och proaktiva utredningar*, *öppna och hemliga utredningar*, og *brottsutredningar och icke-brottsutredningar*. Evalueringen etter 11. september, In Amenas-rapporten, 22. juli-rapporten og UDs evalueringsrapport kan være eksempler på reaktive og åpne rapporter der en evaluerer hendelser i etterkant for å lære og finne forbedringspunkter (Agrell, 2005; NOU 2012:14, 2012; Statoil ASA, 2013b; Utenriksdepartementet, 2013). In Amenas-rapporten har to hovedspørsmål, derav ett av dem er «Hva kan Statoil lære for å forbedre selskapets arbeid med sikkerhet og beredskap i fremtiden?» (Statoil ASA, 2013a, s. 1). Forelå det opplysninger i forkant av hendelsen som kunne vært benyttet og derigjennom hindret eller endret terroranslaget og/eller følger av dette? Det har eksempelvis vært stilt spørsmål med hva PST hadde av opplysninger og hvordan en kunne benyttet dette i forhold til hendelsen 22. juli (Meld. St. 21 (2012-2013), 2013). I UDs evaluering har de blant annet vurdert «…hvilken

informasjon norske myndigheter var i besittelse av om sikkerhetssituasjonen i Algerie forut for terrorangrepet og hvordan denne ble delt» (Utenriksdepartementet, 2013, s. 5). Det er henvist til at daværende statsminister, Jens Stoltenberg, ville ha en vurdering av hvordan norske myndigheter kunne «…gi norske selskaper råd om hvordan de kan håndtere sine sikkerhetsutfordringer i utlandet» (Utenriksdepartementet, 2013, s. 5). Statsministeren tok dette opp i sin redegjørelse om terrorangrepet i Algerie[14]. Årsaker til at informasjon ikke videreformidles er et av flere spørsmål knyttet til slik rådgivning.

Boin et al. deler utfall av kriser inn i tre kategorier: finjustering, policyendring eller paradigmeskifte (Fimreite et al., 2014, s. 207). Endringene kan forandre seg gradvis etter som tiden går, fra først å være mindre endringer (finjusteringer) til senere å føre til større endringer (policyendringer eller paradigmeskifte). Hatlestad-raset i Bergen (en safety-hendelse) er brukt som eksempel der det først førte til mindre endringer for å håndtere slike hendelser bedre, for deretter å medvirke til kartlegging av rasfare og lovendringer (Fimreite et al., 2014, s. 207). Eventuelle endringer i fokus og benyttelse av sikkerhetsrådgivning kan skje som følge av kriser. Terrorangrep blir brukt som referansehendelser i denne oppgaven: det vi kan kalle menneskeskapte kriser (tabell 1).

2.3 Deling av informasjon: Joharis vindu

«Det finnes kjente kjensgjerninger, ting vi vet at vi vet. Det finnes kjente ukjente, ting vi vet at vi ikke vet. Men det finnes også ukjente ukjente, ting vi ikke vet at vi ikke vet» (Indregard, 2013, s. 22)[15]. USAs forsvarsminister Donald Rumsfeld uttalelse helt tilbake til 2002 er en hensiktsmessig start på dette avsnittet som tar for seg informasjonsdeling mellom myndigheter og bedrifter ved hjelp av Joharis vindu[16].

Joharis vindu kan brukes til å vurdere vår *selvrepresentasjon (Steensæth, Hellesøy, Skogstad, & Einarsen, 2000)*, og vurdere personers lederegenskaper (Wermdalen & Nilsson, 2013). Det kan også brukes til å vurdere i hvilken grad informasjon er kjent og delt mellom personer på

[14] Sak nr. 3, Redegjørelse av statsministeren om terrorangrepet i Algerie, Stortinget – Møte onsdag 23. januar kl 10.
[15] Sitatet er oversatt, uvisst av hvem.
[16] Modellen har fått sitt navn fra opphavsmennene Joseph Luft og Harry Ingham.

arbeidsplasser mm. I boken National intelligence and science brukes en modell som ligner på Joharis vindu for å vise interaksjon gjennom sosiale medier (Agrell & Treverton, 2015, s. 133). Joharis vindu har fire felt, der en skiller mellom hva en selv vet/ikke vet og hva andre vet/ikke vet. Dette fører til fire kombinasjoner eller felt. Området kjent for en selv og andre – arenaen (arena). Området kjent for meg, men ikke andre – fasaden (facade). Området jeg ikke kjenner til, men andre kjenner til – blindflekken (blind spot). Området verken en selv eller andre kjenner til – det ukjente (unknown). Dette har jeg under satt inn i konteksten med sikkerhetsrådgivning mellom myndigheter og bedrifter: hva skal en formidle (kommunisere), hvorfor, hvordan og når? Sikkerhetsrådgivning er en form for kommunikasjon og de fire feltene kan brukes til å vurdere denne informasjonsutvekslingen og hvorfor denne utvekslingen utføres slik den gjøres eller eventuelt er helt eller delvis mangelfull. De fire feltene utdypes nærmere under figuren.

	Kjent for myndighetene	Ukjent for myndighetene
Kjent for bedriftene	**Arenaen** Åpen og tilgjengelig informasjon (media, internett, informasjonsbrosjyrer etc.) Ugradert og/eller offentlig	**Fasaden** Skjult eller hemmeligholdt informasjon (bevisst/ubevisst) Skjult (tilbakeholdt) informasjon for myndighetene - kjent for bedriftene
Ukjent for bedriftene	**Blindflekken** Skjult (tilbakeholdt) informasjon for bedriftene (bevisst/ubevisst) - kjent for myndighetene Gradert og/eller taushetsbelagt, klausulert informasjon[17].	**Det ukjente** Begge parter kan ønske informasjon (Kan være kjent for *tredjeparter* at det foreligger informasjon om det aktuelle emne/tema.)

Figur 2: Joharis vindu - tilpasset sikkerhetsrådgivning mellom myndigheter og bedrifter

Det *åpne* feltet – arenaen - består av kjent og tilgjengelig informasjon. Informasjonen kan ligge åpent i form av nettsider, brosjyrer og veiledningsmateriell. Utfordringen her er å kjenne til kildene for informasjonen, vite hvem og hvor en skal henvende seg for å få ønsket (og nødvendig) informasjon. Tilgjengeligheten har to sider: for det første hvor dyktig en er til å søke kunnskapen på egenhånd, og for det andre hvor aktivt de som sitter på informasjonen er til å spre denne. Er tilgangen lik for interessentene, eller er det personavhengig? Med personavhengig tenker jeg på om en må kjenne noen (ha en relasjon) for å få tilgang til informasjonen. Eksempelvis at vedkommende tidligere ha arbeidet hos dem en henvender seg til, eller av andre årsaker har en relasjon. Omskriving fra gradert til ugradert er en

[17] Klausulert informasjon kan eksempelvis være informasjon norske etterretningstjenester mottar fra samarbeidende tjenester under forutsetningen om at det ikke formidles videre.

mulighet for å øke størrelsen på dette feltet. Kanskje kan en få frem det viktige selv om en utelater og *omskriver* informasjonen? En annen mulighet, muligens mer ressurskrevende, er å sikkerhetsklarere personer i bedrifter som har sikkerhetsfeltet som sitt arbeidsområde. Dersom det gis informasjon gjennom andre er det interessant å finne ut hvorfor en ikke gir informasjonen direkte.

Rådgivningsoppgaver kan være hjemlet i lovverket. Eksempelvis er PSTs organisering og oppgaver beskrevet i politilovens kapittel III a (§§ 17 bokstav a – f) (Politiloven, 1995). I PST-instruksens § 6, 1. ledd *Trusselvurdering og sikkerhetsrådgivning* (Instruks for Politiets sikkerhetstjeneste, 2005) kan vi lese at PST skal «…utarbeide trusselvurderinger og gi råd om tiltak av betydning for norske interesser, virksomheter og enkeltpersoners sikkerhet». Videre kan vi lese i 2. ledd at «tjenesten skal bistå ved gjennomføringen av sikkerhetstiltak i […] offentlig og privat næringsvirksomhet og annen virksomhet av betydning for viktige samfunnsinteresser». I instruks om Etterretningstjenesten (Instruks om Etterretningstjenesten, 2001) § 11 *Forebyggende varsling og rådgivning* står det at «etter Forsvarsdepartementets nærmere bestemmelser og innenfor rammen av sikkerhetsloven § 12 kan tjenesten i forebyggende øyemed varsle og rådgi norske og utenlandske juridiske og fysiske personer om forhold som faller innenfor tjenestens oppgaver». Det er også en instruks vedrørende samarbeidet mellom PST og E (Instruks om samarbeidet mellom E og PST, 2006).

Norske selskaper, uavhengig av om de driver virksomhet i Norge eller utenlands, må følge bestemmelsene i arbeidsmiljøloven og den tilhørende internkontrollforskriften. Arbeidsmiljøet skal være trygt og i internkontrollforskriften (Internkontrollforskriften, 1996) § 5, 1. ledd punkt. 6 står det at virksomheten skal «kartlegge farer og problemer og på denne bakgrunn vurdere risiko, samt utarbeide tilhørende planer og tiltak for å redusere risikoforholdene». Sikkerhetsrådgivning kan bidra til denne kartleggingen.

Blindflekken består av informasjon som av en eller annen grunn er skjult eller hemmeligholdt for bedriftene. Informasjonen kan være gradert og slik kreve sikkerhetsklarering for å få tilgang til dette. Sikkerhetsklareringer foretas av NSM og er en «avgjørelse, foretatt av klareringsmyndighet og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad» (Sikkerhetsloven, 1998, § 3 punkt 19). Dette er positivt

med tanke på at en av sikkerhetsmessige årsaker må behandle beskyttelsesverdig informasjon på en slik måte at den ikke kommer i hende på ondsinnede aktører. Den negative siden er at personer (herunder bedrifter) som ikke er klarert vil gå glipp av informasjonen. Omskriving fra gradert til ugradert er som tidligere nevnt en mulighet for å få ut og frem viktige opplysninger likevel. Lovverket kan sette begrensinger gjennom gradering og regulering av informasjonsutveksling.

Taushetsbelagt informasjon kan være gradert, men er i mange sammenhenger ikke det. Ved taushetsbelagt informasjon er det viktig at en undersøker/har god kunnskap om hva som kan deles slik at en ikke håndterer informasjon på måten vi kan kalle *bedre å si lite - enn å risikere å si for mye*. Informasjon fra samarbeidende (utenlandske eller norske) sikkerhetstjenester kan være klausulert og av den grunn ikke tillatt å dele (Sætre, 2015). I *Kampen mot organisert kriminalitet* kan vi lese at Næringslivet og NSR «…opplever at taushetspliktsbestemmelsene i lovverket utgjør et hinder for rette myndigheter til å gi informasjon» (Meld. St. 7 (2010-2011), 2010, s. 109). Det er i følge næringslivet variasjoner fra politidistrikt til politidistrikt, og konsekvensen er at de opplever at relevant informasjon ikke utveksles (Meld. St. 7 (2010-2011), 2010). Gundhus har blant annet sett nærmere på informasjonsdeling ved en spesialavdeling i Oslo politidistrikt som bekjemper organisert kriminalitet (H. I. Gundhus, 2009; H. O. Gundhus, 2005). NSM, PST og E må eksempelvis kunne regnes som store spesialiserte enheter (tjenester). Gundhus har sett på informasjonsdelingen internt i politiet, men kombinasjonen av spesialiserte arbeidsfelt og håndtering av beskyttelsesverdig informasjon gjør at jeg mener funnene hennes kan relateres til sikkerhetsrådgivningen jeg undersøker. Gundhus skiller mellom begrepene *nødvendig å vite* (need to know) og *kjekt å vite* (nice to know). «Effekter av «nødvendig å vite»-kulturen kommer til uttrykk på Spesialseksjonen ved at det oppleves som viktig å holde informasjon for seg selv av hensyn til lekkasjer, men også fordi kunnskap knyttes til anseelse og posisjon» (H. I. Gundhus, 2009, s. 88). I forhold til sikkerhetsrådgivningen vil dette også kunne være aktuelle årsaker til manglende informasjonsutveksling. Det å vite noe andre ikke vet kan gi posisjon, og frykten for lekkasje kan i det lyset brukes som en «unnskyldning» for å la være å dele det en vet med andre.

Informasjon kan holdes tilbake for bedriftene (og allmenheten for øvrig) med begrunnelse i at en ønsker å unngå å spre (det myndigheter anser som) unødig frykt. Ved en terrortrussel

er nettopp det å skape frykt og usikkerhet en viktig del av terroristenes målsetning. Myndighetene får da den vanskelige avveiningen: skal en informere og slik kunne forebygge også på denne måten, eller unngå å spre frykt med fare for å bli kritisert for tilbakeholdelse av informasjon med den følgen at en hendelse fant sted. Et annet dilemma er at informasjon (i likhet med manglende informasjon) kan gi medieoppslag som kan påvirke utfallet av en pågående hendelse eller (trussel)situasjon. Tilbakeholdelse kan da bero på en taktisk vurdering (hensyn) der det er flere positive sider ved dette enn deling av denne informasjonen. Bekymringen for at medieoppslag skal kunne påvirke er i UDs evalueringsrapport omtalt ved gisselsituasjonen i Algerie under punktet *Mediehåndtering* (Utenriksdepartementet, 2013, s. 32).

Informasjonen kan gå direkte mellom aktører eller gjennom (via) andre (kanaler). Foruten at dette kan gjøre informasjon ugradert (omskrive), kan informasjon bli borte på veien. I verste fall når ikke tiltenkt informasjon tiltenkt mottaker. I andre tilfeller kan informasjon få (ubevisst?) endret karakter og dermed ikke være like nyttig og verdifull.

Fasaden er det som er kjent for bedriftene og ukjent for myndighetene. Bedriftene kan holde informasjonen tilbake bevisst eller ubevisst. Ubevisst ved at en ikke forstår at det er vesentlig informasjon, bevisst ved at en lar være å informere om noe en vet er av betydning. Det er utfordrende å ha et konstruktivt samarbeid innen sikkerhetsfeltet (og andre områder) dersom bedriftene holder tilbake vesentlig informasjon om en eller flere problemstillinger. Redsel for å miste kontroll over forretningsmessige fordeler eller tap av omdømme ved å vise *svakheter* overfor myndigheter (og offentligheten som sådan) kan være to av flere årsaker til en slik holdning. En tredje årsak kan være at bedriften ikke har gjennomført nødvendige endringer som tidligere er påpekt internt eller fra eksterne aktører. I Sikkerhetstilstanden 2014 trekker NSM Telenor frem for sin åpenhet omkring dataangrep på deres systemer i 2013 (2014, s. 4). Tilfellet brukes som et eksempel på at åpenhet ikke nødvendigvis trenger å gi negative effekter. Et annet problem kan være at enkeltpersoner sitter på informasjon som ikke deles med andre. Det kan bero på en vurdering fra vedkommende som kunne vært annerledes om andre hadde tolket og analysert opplysningene.

Det *ukjente* er det verken bedriftene eller myndighetene kjenner til. Det kan være irrelevant informasjon eller vesentlig og viktig informasjon. Manglende varsel og hendelse (r) som inntreffer er et eksempel på slik informasjon (Agrell, 2005). Informasjon som andre aktører har, eksempelvis andre utenlandske selskaper eller utenlandske etterretningstjenester, som ikke deles kan være ukjent for norske bedrifter og norske myndigheter. Selv om det er kjent for noen, kan det være ukjent for aktørene jeg ser nærmere på. Informasjon kan som nevnt under blindflekken bli borte, eller endre karakter av ulike årsaker (tiltenkt eller ubevisst) og dermed ikke videreformidles i sin opprinnelige og tiltenkte form, eller rett og slett ikke nå frem til mottaker.

Denne modellen vil bli brukt i analysen fordi den er godt egnet til å få frem aspekter ved rådgivningen myndigheter bedriver overfor bedrifter. Den illustrerer flere problemstillinger knyttet til informasjonsutvekslingen (rådgivningen) myndigheter utfører. Denne modellen vil jeg se opp mot en annen modell, *Strategic knowledge framework for sector policing of organized crime* (Dean, Fahsing, & Gottschalk, 2010, s. 175), som ser på «kampen» mellom politi og kriminelle som en kunnskaps- og kompetansekonkurranse.

Å kunne utføre kriminalitet og unngå å bli tatt av myndigheter/politi kan ses på som en kunnskapskamp. Med det menes at den aktøren som sitter på den beste kunnskapen har muligheten til å utføre kriminalitet uten å bli tatt, eller motsatt gode forutsetninger for å avdekke og stanse kriminell aktivitet. Forholdet mellom politiets kunnskap (policing) og kriminelles kunnskap (organized crime) blir i boken *Organized Crime* satt inn i en figur bestående av fire kvadrat (Dean et al., 2010, s. 174-177). Figuren har slik jeg ser det likheter med Joharis vindu, selv om det her ikke er snakk om (frivillig) formidling av informasjon mellom partene. I begge modellene ønsker en kunnskap og informasjon. Mens det i denne modellen er det en «konkurranse» om å inneha den beste og mest oppdaterte kunnskapen som en ikke ønsker å dele med den andre parten, er det i Joharis vindu ved sikkerhetsrådgivning mellom myndigheter og bedrifter (oppgavens kontekst) andre årsaker til at en ikke utveksler informasjonen. På den ene aksen/siden er det kunnskap om policing (fra lav til høy), på den andre siden det vi kan kalle *kriminell kunnskap* (også fra lav til høy). I det første feltet, *random policing*, har begge parter liten kunnskap og det er mer eller mindre tilfeldig hvem som lykkes. I felt to har de kriminelle mer kunnskap enn politiet, *disadvantaged policing*, og er slik i forkant av politiet. I felt tre, *targeted policing*, har politiet

styringen og har mest kunnskap. I felt fire, *competetive policing*, har begge parter kunnskap. De er innovative og tilpasser seg til hverandre – de konkurrerer (competetive).

Overført til sikkerhetsrådgivning er det om å gjøre for myndigheter (og bedrifter) å inneha den beste kunnskapen, da sett i forhold til å være i forkant av ondsinnede aktører. Denne kunnskapen (informasjonen) må formidles videre fra myndigheter til bedriftene på en slik måte at det ikke kommer «i feile hender» og dermed faller i «verdi». Det kan være gode (taktiske) årsaker til at en ikke gir informasjon. For eksempel at en mister fordelen overfor den ondsinnede aktøren ved å spre informasjonen. Dette med den fare at informasjonen tilfaller denne aktøren. Ved å sette sikkerhetsrådgivningen inn i Joharis vindu kan en strukturere og finne forklaringer på hvorfor informasjon som ville fungert som sikkerhetsråd blir holdt tilbake eller formidlet i en annen form. Årsakene til manglende informasjonsutveksling kan være godt begrunnet, men det kan også ha mindre tilfredsstillende forklaringer.

2.4 Public Private Partnership (PPP)

PPP kan oversettes til *offentlig-privat samarbeid (OPS)*. Sikkerhetsrådgivning fra norske myndigheter kan være en større eller mindre del av et PPP. I *Kartlegging og utredninger av former for offentlig privat samarbeid (OPS)* defineres OPS på denne måten: «en offentlig tjeneste som utvikles og/eller drives av private (eller sammen med det offentlige) etter forespørsel fra det offentlige, og der risiko fordeles mellom privat og offentlig sektor» (Nærings- og Handelsdepartementet, 2003, s. 4). Samarbeidet mellom myndigheter og private har som målsetning å føre til et bedre resultat enn om en arbeidet hver for seg. Det er både et kvalitativt og et økonomisk insentiv (Nærings- og Handelsdepartementet, 2003). Sikring av kritisk infrastruktur og norske borgeres sikkerhet i utlandet kan være samarbeidsområder. Samordning og samvirke har vært savnet, og det er «…viktigt att näringslivet och brottsbekämpande myndigheter smarbetar och byter information åt båda håll» (Wermdalen & Nilsson, 2013, s. 523). Dette er også omtalt i Kampen mot organisert kriminalitet (Meld. St. 7 (2010-2011), 2010). Erfaringer (Boin & Smith, 2006; Meld. St. 7 (2010-2011), 2010; Taghavi, 2010) med PPP er relevant for oppgavens problemstilling. Det er

et forbedringspotensial i å undersøke hva som fungerer bra og hva som fungerer mindre bra. Nærmere bestemt hvordan sikkerhetsrådgivningen utføres. Bakgrunnen for et slikt samarbeid er gjerne at en ser at en er avhengig av et samarbeid mellom offentlige og private på grunn av overlappende ansvarsområder og en målsetning om et best mulig resultat innenfor sikre rammer (sikkerhet). Selv om hovedansvaret for å forebygge kriminalitet og terrorisme er et statlig anliggende, i det landet en har virksomhet, er en avhengig av et samarbeid med private virksomheter. FNs globale strategi for kontraterrorisme oppfordrer til PPP og G8-landene[18] har lansert et globalt forum for partnerskap mellom stater og virksomheter for å bekjempe terrorisme (Organization for Security and Co-operation in Europe, u.å.). Erfaringer med PPP som ledd i terrorbekjempelse er ulikt (Taghavi, 2010).

Scottish Business Crimes Centre (SBCC) og Overseas Security Advisory Council (OSAC) er to eksempler på PPP-modeller. SBCC er en modell som omtales i Kampen mot organisert kriminalitet (Meld. St. 7 (2010-2011), 2010). Det er et samarbeid mellom myndigheter og næringslivet for å redusere forretningskriminalitet. «Hovedbidraget fra SBCC for å redusere forretningskriminaliteten, er samarbeid og utveksling av informasjon mellom næringsliv, politi og offentlige myndigheter» (Meld. St. 7 (2010-2011), 2010, s. 112). En av de *avsluttende betraktninger og prioriteringer* i stortingsmeldingen har overskriften: «Nytt samarbeidsforum mellom, departement, politiet, påtalemyndigheten og næringslivet» (Meld. St. 7 (2010-2011), 2010, s. 117). Dette skal utredes videre med tanke på organisering og finansiering (Meld. St. 7 (2010-2011), 2010, s. 117).

OSACs målsettning (mission) er følgende: «The U.S. State Department's Overseas Security Advisory Council (Council) is established to promote security cooperation between American private sector interests worldwide (Private Sector) and the U.S. Department of State» (The U.S. State Department`s Overseas Security Advisory Council, u.å.). OSAC arbeider for å etablere samarbeid mellom State Department security functions og privat sektor, regulær og tidsriktig informasjonsutveksling, anbefale metodikk, og redusere risiko for amerikansk privat sektor med internasjonale interesser. Statoil er et norsk internasjonalt selskap også med virksomhet i USA. Selskapet deltar i møter som OSAC arrangerer internasjonalt.

[18] G8-landene: Canada, Frankrike, Italia, Japan, Storbritannia, Tyskland, USA og Russland.

Taghavi har undersøkt PPPs levedyktighet i kampen mot internasjonal terrorisme (2010). 250 store UK-firma svarte på spørreundersøkelsen, og 27 av firmaene som svarte ble fulgt opp med intervjuer. Ca 40 % av firmaene, noe som må kunne sies å være en stor andel, oppfattet at informasjonen om terrorangrep fra myndighetens side enten var misledende, unøyaktig eller overdrevet (s. 1)[19]. Joharis vindu kategoriserer informasjonen med hensyn til om den er kjent eller ukjent. Dersom informasjonen er eller oppleves som uriktig eller overdrevet vil det kunne svekke samarbeidet og utbytte av dette. Det vil kunne påvirke om bedriftene aktivt søker kunnskap hos myndighetene. Tilsvarende vil slike funn kunne påvirke hva myndigheter vil utveksle av informasjon. Undersøkelsen ser på store britiske bedrifter, men vil likevel kunne ha overføringsverdi til norske forhold og store norske bedrifter. Bedriftenes vurdering av informasjonen de får fra myndighetene er avgjørende også for norsk virksomhet.

Strategier for risikohåndtering kan deles i fire. Herunder unnvikelse, overføring, aksept (passiv eller aktiv) og fjerning eller reduksjon (Nasjonal sikkerhetsmyndighet et al., 2010, s. 18). Overføring av risikohåndtering kan eksempelvis innebære at virksomheten benytter seg av private sikkerhetsselskap, også kalt utkontraktering eller outsourcing av oppgaver. Veiledningen utgitt i fellesskap av NSM, POD og PST nevner lojalitet og manglende mulighet for kontroll ved ansettelser som to problematiske sider ved utkontraktering av eksempelvis sikkerhetsarbeidet ved bedrifter (2010, s. 18). Samtidig er det også fordeler med en slik overføring. Kompetanse er her et viktig stikkord. En kan kjøpe tjenester fra firma som har erfaring og kunnskap innen slike tjenester i stedet for å bygge opp egen kompetanse. Outsourcing kan dermed være både tids- og kostnadsbesparende. Samtidig som overføring av slike oppgaver kan påvirke virksomhetens risikoforståelse og risikoerkjennelse. Selv om en kjøper slike tjenester, er virksomheten hovedansvarlig. Nærhet til problemene, varslingsrutiner, avgjørelsesmyndighet og ansvarsforhold er særdeles viktige områder ved outsourcing og samarbeidsprosjekt. Bevissthet rundt valget om å kjøpe slike tjenester er et godt utgangspunkt for å kombinere ansvar (både risikoforståelse og risikoerkjennelse) og sikkerhet. Oppgaver kan delegeres og outsources, men ansvaret tilligger virksomheten like fullt.

[19] Artikkelen er unummerert. Jeg angir sidetall med første side som side nummer 1.

2.5 Private sikkerhetsselskap (PMSCs)

Bruk av private sikkerhetsselskaper kan si noe om virksomhetens vektlegging av sikkerhet. I samarbeidsprosjekt (eksempelvis joint venture) mellom flere bedrifter vil et PMSC kunne bli en av aktørene. Å benytte seg av slike tjenester kan på den ene siden kan det bety at en tar sikkerheten på alvor, mens det i den andre ytterkanten kan bety at en velger å outsource hele eller deler (overføring av risikohåndtering) til andre fordi en ikke ser viktigheten av dette. Her er det selvsagt mange ulike mellomliggende varianter. En profesjonell virksomhet er bevisst mulige problemstillinger knyttet til det å kjøpe sikkerhetstjenester og tyr ikke til dette som en *enkel* løsning på en viktig del av virksomhetens risikovurdering. Vurderingene som ligger til grunn her er vil gjenspeile virksomhetens risikoforståelse og risikoerkjennelse.

Kommersielle private sikkerhetsselskap og militære selskap kan leies inn for å ta seg av hele eller deler av en virksomhets sikkerhetsarbeid. Av tjenestene en kan kjøpe kan en nevne vakthold (væpnet og uvæpnet), beskyttelse av personer og verdier, rådgivning og bistand til å utføre risikoanalyser (helt eller delvis). Benyttelse av PMSC er ikke et nytt fenomen, men de er en stadig mer økende aktør i moderne konflikter (Jarvis & Holland, 2015, s. 134).

The Democratic Control of Armed Forces (DCAF) er en rådgivende stiftelse som blant flere oppgaver driver forskning for å fremme godt styresett og reformering av sikkerhetssektoren (The Geneva Centre for the Democratic Control of Armed Forces, u.å.). Østensen har skrevet en rapport om bruk av private sikkerhetsselskap utgitt av DCAF (Østensen, 2011b). Rapporten viser til flere merkelapper som er brukt for å beskrive private militære og sikkerhetsselskap, også av industrien selv. I rapporten beskrives selskapene som «private business entities that provide military and/or security services, irrespective of how they describe themselves» (Østensen, 2011b, s. 7). Den engelske betegnelsen på disse selskapene er Private Military and Security Companies (PMSCs).

PMSCs opererer innen et område som tidligere var et kjerneområde forbeholdt staten og endringen kan beskrives som et skifte fra *government* til *governance* (Østensen, 2011a, s. 369). Det vil si et skifte fra statsvirksomhet til et system der flere aktører får innflytelse og forpliktelser innen det samme området. Dette kan ses i sammenheng med privatiseringen på

80- og 90-tallet der private aktører har fått ansvar for viktig deler av infrastrukturen i samfunnet (Boin & Smith, 2006, s. 295).

I artikkelen *Sikkerhet som salsvare* har Stensvand intervjuet Østensen (2013). Stensvand skriver at den økte bruken av slike kommersielle selskap har gitt dem politisk innflytelse, direkte og indirekte (Stensvand, 2013, s. 40-41; Østensen, 2011a). Bruken har økt til tross for at deres virksomhet har vært omdiskutert og beskyldninger av alvorlig karakter mot sikkerhetsselskapene. FN benytter seg av slike tjenester i sine operasjoner og Norske UD bruker også private sikkerhetsselskap. Norske sikkerhetsselskap kan ikke bære våpen i inn- og utland, med unntak av norske skip i bestemte havområder. Det som kan kalles et *land/sjø-paradoks* (Stensvand, 2013). Dette er en følge av piratproblematikken i Adenbukta som ligger mellom Somalia og Jemen (Stensvand, 2013). Piratproblematikk er en av flere referansehendelser som blir brukt i oppgaven. In Amenas-anlegget benyttet seg av private sikkerhetsselskaper for å ta seg av sikkerheten inne på selve gassanlegget, mens den algeriske hæren skulle ta seg av den ytre sikkerheten. De algeriske myndighetene tillater bevæpnede sivile vakter, men de kan da ikke være utenlandske statsborgere (Statoil ASA, 2013b, s. 48). I Algerie var Statoil og BP enig i at væpnet vakthold skulle utføres av militæret om nødvendig (Statoil ASA, 2013b).

Det er to forhold som gjør at en benytter seg av private sikkerhetsselskap (Stensvand, 2013): 1) forestillingen om bedre kompetanse, og 2) ønske om lavere utgifter. Østensen kaller det et paradoks siden private selskap «stort sett hyrer folk med bakgrunn frå militæret eller politiet» (Stensvand, 2013, s. 40). I tillegg viser studier at det vanligvis ikke er billigere å benytte seg av private tjenester. Stensvand skriver at i følge Østensen er bruk av bevæpnede vakter fra private sikkerhetsselskaper er i Norge blitt aktualisert, men lite omdiskutert, i forbindelse med piratvirksomhet og press fra norske redere (2013, s. 40-41).[20] Private sikkerhetsselskaper har vært mistenkt for kritikkverdige forhold (Stensvand, 2013). I Aftenposten kunne vi lese at fire ansatte i Blackwater[21], tidligere amerikanske militære

[20] For ytterligere kjennskap til piratproblematikken kan en se på Tore Bjørgo og Ingvild M. Gjelsvik sitt forskningsprosjekt, *Strategies for preventing piracy in Somalia*, som er et eksempel på forebygging av piratproblematikken i Somalia.
Norges Rederiforbund (Norwegian Shipowners` Association) er en viktig støttespiller ved håndteringen av piratproblemet.

[21] Selskapet er solgt og har skiftet navn.

soldater, er dømt til lange fengselsstraffer[22] for å ha drept 14 og skadet 17 sivile i Bagdad (Irak) i 2007 (Ask, 2014).

2.6 Evaluering etter 22. juli og In Amenas

I etterkant av terrorangrepet mot regjeringskvartalet og Utøya 22. juli 2011 ble det nedsatt en gruppe for å gjennomgå hendelsene. Hendelsene er én av i alt fem referansehendelser jeg har brukt i intervjuguidene (appendiks nr. 1 og appendiks nr. 2). Etter terrorangrepet mot In Amenas, 16.-19. januar 2013, ble det nedsatt en gruppe for å granske angrepet. Hendelsen er i likhet med 22. juli benyttet som referansehendelse i intervjuguidene. UD var lederdepartement under krisehåndteringen ved In Amenas-krisen. Det er i den forbindelse foretatt en evaluering av norske myndigheters håndtering av krisen, fremlagt i den gjerne ikke fullt så kjente (?) rapporten *Terrorangepet på gassproduksjonsanlegget i In Amenas – Evaluering av norske myndigheters krisehåndtering* (Utenriksdepartementet, 2013). De tre nevnte evalueringene er skrevet i etterkant av hendelsene (NOU 2012:14, 2012; Statoil ASA, 2013b; Utenriksdepartementet, 2013). Rapportene etter 22. juli og In Amenas påpeker viktigheten av samarbeid med relevante samarbeidspartnere og informasjonsutveksling dem i mellom. UDs rapport har avslutningsvis fire områder som trenger avklaring. Punkt fire heter *Sikkerhetsinformasjon til norske virksomheter i utlandet*. Her fremgår det at det skal undersøkes «…hvorvidt norske myndigheter ytterligere kan bistå norske virksomheter i utlandet i spørsmål av sikkerhetsmessig karakter» (Utenriksdepartementet, 2013, s. 37). Sikkerhetsrådgivning er en slik form for støtte som kan gis til bedriftene.

Stortingsmeldingen *Terrorberedskap* (Meld. St. 21 (2012-2013), 2013) er en oppfølging av 22. juli-rapporten (NOU 2012:14, 2012). Her kan vi lese at flere land har felles analyseenheter der ulike tjenester samarbeider. Det ble besluttet at PST og E skulle utrede organiseringen av et slikt senter (Meld. St. 7 (2010-2011), 2010, s. 55), og Felles Kontraterror Senter (FKS) under ledelse av PST har vært i drift siden februar 2014.

[22] Saken ble anket.

FKS har tre oppgaver (Bjørnland, 2014):

- «ivareta rettidig og relevant informasjonsutveksling mellom tjenestene»
- «koordinere og tilrettelegge for et effektivt operativt samarbeid»
- «utarbeide analyser av terrortrusler rettet mot Norge og norske interesser»

PST har Norge som arbeidsfelt og E utlandet. Et tettere samarbeid dem i mellom vil kunne gi PST og E et bedre grunnlag for sikkerhetsrådgivning til norske bedrifter og norske bedrifter med virksomhet i utlandet. «PSTs sikkerhetsrådgiving retter seg i første rekke mot virksomheter i Norge, men sikkerhetsrådgivingen kan ha verdi ved etablering og drift i utlandet. PST kan bistå virksomheter i arbeidet med å utarbeide risikoanalyser med sikte på å etablere risikoreduserende tiltak» (Meld. St. 7 (2010-2011), 2010, s. 69).

Samarbeid med andre myndigheter vil kunne gi et bedre informasjons- og beslutningsgrunnlag. For eksempel E, NSM, UD, NSR for å nevne noen. NSM har i likhet med PST Norge som arbeidsfelt. E har området utenfor Norges grenser som sitt arbeidsområde. UD bistår nordmenn i utlandet, og er en naturlig samarbeidspartner ved norsk virksomhet i utlandet. Med ansvarsprinsippet menes at det departement som har et område som arbeidsfelt også er ansvarlig for eventuelle kriser som oppstår på dette feltet. Sagt på en annen måte: ansvar «…for samfunnssikkerhet innenfor sitt område» (Fimreite, Langlo, Lægreid, & Rykkja, 2011, s. 16). UD er som utgangspunktet lederdepartement ved hendelser i utlandet hvor norske borgere er involvert som en følge av dette prinsippet. NSR fokuserer på det som skjer på land og Rederiforbundet på det som skjer på sjø og hav.

2.7 Tilsiktede uønskede hendelser

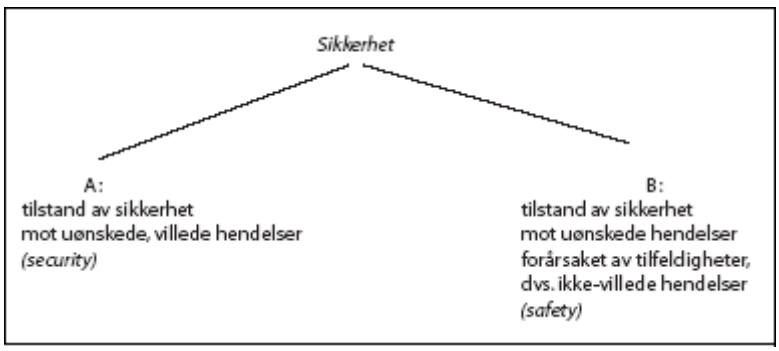
Terrorisme får mye sendetid i TV og medieoppmerksomhet ellers. Terrorister er nettopp avhengig av dette mediefokuset for at aksjonene skal få effekt (Rasch, 2005), noe som kan skille det fra andre typer kriminalitet som ønsker å foregå mer i det skjulte. Til tross for en slik *skjevhet* (?) i medieoppmerksomhet er det viktig å presisere at det er flere typer hendelser som faller inn under hendelsesgruppen tilsiktede uønskede hendelser. «Ulike former for kriminalitet, organisert og uorganisert, er en vel så viktig del å fokusere på i et

security-perspektiv. Bak de tilsiktede, ondsinnede handlingene står en trusselaktør. Trusselaktører kan være alt fra misfornøyde ansatte i en bedrift til pressgrupper, organiserte kriminelle, terroristorganisasjoner eller andre stater» (NOU 2006:6, 2006, s. 233). Håndtering av bedrifter og myndigheters beskyttelsesverdige informasjon og personellrekruttering (bakgrunnssjekk) er derfor også av stor betydning. Her kan sikkerhetsrådgivning fra respektive myndigheter være et av flere tiltak.

Aktørers hensikt eller motiv kan deles i to slik det gjøres i *Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger – Terminologi* (Standard Norge, 2012, s. 2): 1) ondsinnet eller 2) å fremme egne interesser. De to motivene kan slik jeg ser det kombineres.

2.8 Safety og security

Differensieringen mellom begrepene safety og security er nøye gjennomgått i *Når sikkerheten er viktigst* (NOU 2006:6, 2006). To begreper som på norsk kan fremstå som uklare. De kan være delvis overlappende, uten klare avgrensninger seg i mellom. Derav er begrepene utredet i Når sikkerhet er viktigst NOU 2006:6 (2006), herunder mer inngående i utredningens vedlegg 5. Bruken av ordene og deres betydning diskuteres og utvalget mener at sikkerhet er et overordnet begrep (hypernym) sett i forhold til safety og security. Videre skiller en mellom tilsiktede (villede) og ikke-villede hendelser. Dette er skjematisk fremstilt i figuren under.



Figur 3: Når sikkerhet er viktigst, figur 5.1 (NOU 2006:6, 2006, s. 229).

Finn-Erik Vinje, som har skrevet overnevnte vedlegg, foreslår at en kan bruke ordet *trygghet* under safety og *sikring* under security. Vinje understreker videre viktigheten av å forklare hvilken betydning man legger i ordene da betydningen ikke har en naturlig differensiering på norsk. Enkelte bedrifter bruker *sikkerhet* for å dekke begrepet safety og *sikring* for å dekke begrepet security (NOU 2006:6, 2006, s. 38).

I In Amenas-rapportens sammendrag nevnes det at sikkerhet på norsk dekker både safety- og security-begrepet (Statoil ASA, 2013a). Det fremgår også av sammendraget at security er beskyttelse mot «viljestyrte handlinger» og at granskningsgruppen ikke vurderte «…sikkerhet (safety) innenfor det tradisjonelle helse, miljø- og sikkerhetsområdet» (Statoil ASA, 2013a, s. 1). Slik jeg ser det er Statoils differensiering i samsvar med utvalgets differensiering over, og viser at en ser nødvendigheten av å avklare begrepene safety/security for å unngå misforståelser i begrepsbruken.

I Et sårbart samfunn (NOU 2000:24, 2000, s. 307) skiller en mellom begrepene ved at safety er «sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter», og security er «sikkerhet mot uønskede hendelser som er et resultat av overlegg og planlegging». I anglosaksiske land skilles det i følge Wermdalen og Nilsson mellom begrepene safety (skydd) og security (säkerhet) ut fra trusselen en ønsker å beskytte seg mot (2013, s. 49). Safety når en beskytter seg mot ulykker (f. eks. brann og arbeidsmiljø). Security når en beskytter seg mot kriminalitet (f. eks. tyveri og terrorisme). Tap og skade kan i de to tilfellene unngås gjennom sikkerhetstiltak av ulik karakter. I denne oppgaven skiller jeg mellom safety og security ved om hendelsene en vil beskytte seg mot er uønskede og tilfeldige eller uønskede og tilsiktede. Dette er i tråd med modellen skissert ovenfor. Samt utvalgets beskrivelse av safety som «sikkerhet mot uønskede utilsiktede hendelser», og security som «sikkerhet mot uønskede tilsiktede hendelser» (NOU 2006:6, , s. 39). Eksempler på uønskede og tilfeldige hendelser er ulykker og hendelser forårsaket av at en ikke følger vedtatte prosedyrer. Terping på rutiner og bevissthet rundt dette kan være eksempler på safety-tiltak. Uønskede og tilsiktede hendelser kan eksemplifiseres med terrorangrep og andre planlagte ondsinnede aksjoner. Fysiske barrierer, adgangskontroll og trusselvurderinger er eksempler på security-tiltak. Tilsiktede hendelser skiller seg ut ved at

det foreligger en viss form for planlegging. Det overlagte og ikke-tilfeldige ved handlingen er et vesentlig element ved terrorisme (Hoffman, 2006). Ved tilsiktede uønskede handlinger (security) har (trussel-) aktøren en hensikt. Denne hensikten (motivet) kan som nevnt være ondsinnet og/eller å fremme egne interesser (Standard Norge, 2012, s. 2).

Begrepsuklarheten mellom safety og security kan forståes slik at en ikke har skilt mellom sikkerhetsutfordringer knyttet til dem. Håndtering av risiko vil være ulik avhengig av om hendelsen er tilsiktet eller utilsiktet. Mulighetene for å forutsi og avverge vil også være ulik. En klar forståelse av begrepene og målrettede (og nødvendige) tiltak innen begge områdene er nødvendig for å forstå den totale risikoen og derigjennom begrense sårbarheten.

En vanlig forståelse av risiko er sannsynlighet ganget med konsekvens. I NS5830:2012 defineres risiko som et «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (Standard Norge, 2012, s. 4). Sannsynlighet er i følge Wermdalen og Nilsson mindre relevant innen sikkerhet dersom konsekvensene av et angrep er store (2013, s. 522). Risikotrekanten bestående av verdi, trussel og risiko brukes i større grad etter 22. juli, mens en tidligere brukte risikomatrisen for å prioritere risikoer (Wermdalen & Nilsson, 2013, s. 522).

Hendelser og trusler en gir sikkerhetsråd i forhold til kan være ulike former for kriser eller potensielle kriser. Krise kan forklares med «en situasjon med høy grad av usikkerhet og potensielt uakseptable konsekvenser for den entiteten som rammes» (Standard Norge, 2012, s. 2). En måte å kategorisere kriser på er med utgangspunkt i krisens årsak og krisens faser. Tabellen under er hentet fra *Organisering, Samfunnssikkerhet og krisehåndtering* (Fimreite et al., 2014, s. 13) og *tilført* to felt med begrepene safety og security. Nærmere bestemt har jeg lagt de to blå feltene til i den originale tabellen. Forebygging og håndtering har likheter med de to sporene i definisjonen jeg har laget av sikkerhetsrådgivning: 1) forebyggende råd (forebygging), og 2) spesifikke råd knyttet mot sak eller hendelser (håndtering).

		Krisens årsak	
		Naturskapt	Menneskeskapt
		Safety	Security
Krisens faser	Forebygging	Flyforbudet etter askeskyen	Kontraterrortiltak
	Håndtering	Rasulykker	Kugalskapssaken

Tabell 1: Bearbeidet tabell[23] Kriser – faser, årsaker og eksempler (tabell 1.1) (Fimreite et al., 2014, s. 13).

2.9 Terrorisme

Terrorisme[24] er en type tilsiktet uønsket og ondsinnet hendelse. Flere av referansehendelsene i oppgaven, eksempelvis In Amenas, er terrorangrep. Terrorisme er et «…omstridt og mangefasettert» (Rasch, 2005) begrep uten en klar og omforent definisjon. Begrepet er ikke naturgitt, men et sosialt konstruert fenomen (Spaaij, 2012). Forskere har eksempelvis funnet mer enn 200 definisjoner på terrorisme (Bjørgo, 2005, s. 1). Variasjonen i innholdet kan en få ytterligere belyst ved å studere Alex P. Schmids tabell med oversikt over elementer i 109 terrorismedefinisjoner (2011, s. 74). De ulike definisjonene vektlegger ulike elementer. Overnevnte oversikt viser foruten variasjonen, også prosentvis hvilke elementer som hyppigst brukes i de undersøkte definisjonene.

Elementene, og presiseringene, brukt i definisjonene kan si noe om aktørens fokus og ansvarsområde. Ulikt fokus kan skyldes flere faktorer. Ansvarsområde er allerede nevnt. Å definere eget ansvarsområde inn i definisjonen for å vise viktigheten av sitt arbeid og få tildelt ressurser en annen årsak. Å definere egen virksomhet ut av begrepet kan også være en forklaring til hvorfor en definerer på en bestemt måte.

[23] Feltene safety og security er lagt til i den originale tabellen. Dette er uthevet med blå farge for å tydeliggjøre endringen.
[24] Terrorisme reguleres i straffelovens 14de kapittel §§ 147 a – 147 d.

Foruten at det er mange definisjoner av terrorisme, vil det også kunne være usikkerhet om en hendelse er å anse som terrorisme. Angrepene på Telenors butikker fant sted i kjølevannet av de omstridte Muhammed-karikaturene. Disse hendelsene er i følge Tønnesen riktigere å benevne som demonstrasjoner og sabotasje, heller enn terrorisme (2008). Det er også blitt stilt spørsmål om myndighetene medvirket eller lot være å gripe inn for å stanse folkemengdenes angrep mot blant annet norske interesser. Senere har en kunne lese i media at en terrorcelle bestående av syv personer ble pågrepet med planer om å ramme flere mål, deriblant Telenors virksomhet i Pakistan (Ravndal, 2009). Selv om hendelsene ikke trenger å ha noen sammenheng, i alle fall ikke direkte, viser det at norske interesser i utlandet kan være potensielle mål i flere sammenhenger.

Oppmerksomhet utenfor selve *konfliktteateret* er en vanlig målsetning for terrorister. Terrorangrep mot utenlandsk virksomhet og eller interesser kan være en effektiv måte å skape oppmerksomhet rundt sin sak. Terrorangrepet mot Westside kjøpesenter i Nairobi i Kenya i 2013 (Hansen, 2013) er et eksempel på en hendelse som fikk stor medieoppmerksomhet, terrorangrepet mot gassanlegget In Amenas i Algerie et annet eksempel. Å slå til mot store anerkjente firma kan foruten omtalen gi inntrykk av handlekraft og styrke. Myndighetenes reaksjoner på hendelsen kan deles i *kraftfull* og *svak (Romarheim, 2012, s. 87)*. Der kraftfull viser til militære operasjoner, og svak (eller avstemt) viser til diplomatiske og/eller juridiske virkemidler. Sterke reaksjoner kan ha negativ virkning. Dette ved at omtalen kan bli mer omfattende, og at det viser at en må reagere mot denne farlig og potente fienden. Sterke reaksjoner blir derfor ofte korrigert ved neste korsvei (Romarheim, 2012, s. 85).

Jeg legger den vanligste definisjonen på terrorisme (Hegghammer, 2005) til grunn i oppgaven: «Premediated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents[25], usually intended to influence an audience» (United States, 2004, s. 12)[26]. Årsaken til at jeg bruker denne definisjonen er vektleggingen av at handlingen er overlagt (ikke tilfeldig) som poengtert av Hoffman (2006), politisk motivert og ønske om å påvirke andre enn de direkte ofrene. I følge Bjørgo forsøker

[25] Setningen før komma er hentet fra Title 22 of the United States Code, Section 2656f(d)
[26] Sidetall angitt med romertegn i originaldokumentet (xii).

terrorister å maksimere politiske og ideologiske verdier (Bjørgo, 2014, s. 3)[27]. Soloterrorisme eller lone wolf terrorism er en form for terrorisme som også er omdiskutert og som i likhet med terrorisme ikke har en omforent definisjon[28]. Handlinger utført av enkeltpersoner er som nevnt innledningsvis i kapittelet utfordrende med tanke på varsel og signal.

2.10 Spionasje og fremmed etterretning

Spionasje og fremmed etterretning er tilsiktede uønskede handlinger som kan være ondsinnede, samtidig som det gjennomføres for å fremme egne interesser. Etterretning er innhenting og sammenstilling av informasjon som grunnlag for beslutningstaking. Spionasje er en metode for slik innhenting og kan forklares med «innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt» (Sikkerhetsloven, 1998, § 3 punkt 3). Rekruttering av medarbeidere og sikkerhetsklarering av personer i gitte posisjoner er derfor viktig for å unngå personer med slike hensikter. I Fokus 2014 kan vi lese at «for fremmede etterretningstjenester, kriminelle og hackere er internett en arena for informasjonsinnhentning og spionasje» (Etterretningstjenesten, 2014a, s. 59). Mens vi i PSTs årlige trusselvurdering kan vi lese at Norge vil utsettes for etterretningsvirksomhet (Politiets sikkerhetstjeneste, 2014), og i Sikkerhetstilstanden 2014 forventes det et «økende antall spionasjeforsøk mot norske virksomheter» (Nasjonal sikkerhetsmyndighet, 2014). I PSTs åpne trusselvurdering for 2015 trekkes fremmed etterretnings skadepotensial frem, og det vises spesifikt til landene Russland og Kina (Politiets sikkerhetstjeneste, 2015, s. 5).[29] I rapporten Risiko 2015 kan vi lese «…at risikoen for spionasje mot norske interesser er høy» (Nasjonal sikkerhetsmyndighet, 2015, s. 3). Det fremgår i rapporten at olje- og energisektoren er utsatt for dataangrep, samt at «digital spionasje er en vedvarende og stor utfordring for Norge» (Nasjonal sikkerhetsmyndighet, 2015, s. 4). Statoil som er en av informantene i oppgaven er et olje- og energiselskap.

[27] Det upubliserte manuskriptet er benyttet i oppgaven etter avtale med Tore Bjørgo.
[28] Lone wolf terrorism kan defineres slik: «they (a) operate individually, (b) do not belong to an organized terrorist group or network, and (c) their modi operandi are conceived and directed by the individual without any direct outside command or hierarchy (Spaaij, 2012, s. 16).
[29] Trusselvurderingen er ikke nummerert. Første side angis som side 1.

2.11 Organisert kriminalitet, alvorlig kriminalitet, og volumkriminalitet

Sikkerhetsråd kan utøves på flere felt og er ikke bare rettet mot forhindring og håndtering av terrorisme. Kriminalitet er tilsiktede og uønskede handlinger overfor en fornærmet person, bedrift, myndighet eller lignende. Motivet er gjerne først og fremst å fremme egne interesser (vinnings hensikt), men hensikten kan også være ondsinnet. Kriminalitet kan deles i flere *grupper* og jeg vil kort forklare noen av dem. I likhet med terrorisme er ikke organisert kriminalitet[30] noe naturgitt fenomen, men et sosialt skapt fenomen, med en rekke ulike definisjoner (Larsson, 2008).

Organisert kriminalitet[31] kan defineres som «…lovbrudd som begås av flere personer i vinnings hensikt med en viss plan og organisering som strekker seg over tid» (Johansen, 1996, s. 12). Den organiserte kriminaliteten er profittmotivert (Larsson, 2008), eller sagt på en annen måte kjennetegnes den «… by mainly maximising economic profit» (Bjørgo, 2014, s. 2). Alvorlig kriminalitet kan være et av flere kjennetegn ved en definisjon av organisert kriminalitet. Da er spørsmålet hva som regnes som alvorlig. Skillet settes ofte ved handlinger med en strafferamme over tre år (Larsson, 2008). I straffelovens definisjon av en organisert kriminell gruppe er et av kriteriene en strafferamme på minst tre år[32]. Hverdagskriminalitet og volumkriminalitet er begrep som kan brukes om hverandre. En fordel med å bruke benevnelsen volumkriminalitet er at det viser at det er en form for kriminalitet som finner sted ofte, uten at følgene (fysisk og psykisk) bagatelliseres. Ordet hverdag kan gi et inntrykk av at det er noe bagatellmessig. For den fornærmede part oppleves det trolig ikke som en bagatell.

Avhengig av hvor bedriftene har virksomhet spiller de ulike tilsiktede (og ondsinnede?) truslene forskjellige roller. Sabotasje, korrupsjon, kidnapping, tyveri med mer kan være aktuelle trusler norske bedrifter må *leve med*. Både i enkeltland og områder rundt omkring i

[30] Straffelovens definisjon av organisert kriminalitet, nærmere bestemt organisert kriminell gruppe: «Med organisert kriminell gruppe menes et samarbeid mellom tre eller flere personer som har som et hovedformål å begå en handling som kan straffes med fengsel i minst 3 år, eller som går ut på at en ikke ubetydelig del av aktivitetene består i å begå slike handlinger» (Straffeloven, 1992, § 60 a, 2. ledd).
[31] Det er flere straffebud i straffeloven som er aktuelle ved organisert kriminalitet. Straffeloven § 60 a beskriver organisert kriminalitet nærmere.
[32] Se fotnote 30.

verden har slike trusler ulik betydning. Piratkapringer er et annet eksempel på kriminalitet norske bedrifter utsettes for.

Bedrifter, myndigheter og trusselaktører endrer seg ettersom motparten gjør endringer i sin virksomhet og sine handlingsmønstre. Endrings- og tilpasningsevne er nødvendig for enten å avverge, og motsatt kunne fortsette den ulovlige virksomheten uten å bli avslørt og tatt. Dersom trusselaktør er i forkant kan situasjonen plasseres inn i den nevnte kategorien disadvantaged policing (Dean et al., 2010). Er det derimot politiet som endrer seg og tilpasser seg utviklingen best kan det falle inn i kategorien targeted policing (Dean et al., 2010). Organiserte kriminelle og terrorister har endret organisering fra toppledede hierarkiske organisasjoner til nettverksorganisasjoner. Dette for å unngå at arrestasjon av en høytstående leder skulle få omfattende følger organisasjonens virksomhet. Leders kontroll er stor ved en hierarkisk organisasjon, medium ved nettverks- eller desentraliserte celler, og lav ved lederløs organisering (Dishman, 2005, s. 242). Denne nevnte endringen fører til mer selvstyrte avdelinger (celler) som kan ta avgjørelser på egenhånd uten å kontakte topplederne. Videre ser en at samarbeid mellom organiserte kriminelle og terrorister ikke er like tidsavgrenset som tidligere. De har færre reservasjoner mot å samarbeide, og strategisk langtidssamarbeid der en utnytter hverandres ekspertise. Dette vil i følge Dishman gjøre gruppene farligere og vanskeligere å få fatt på (Dishman, 2005, s. 249). Bjørgo påpeker også at tendensen til at terrorister og organiserte kriminelle blir hybrider av hverandre har betydning for hvordan truslene håndteres (2014, s. 13)[33]. Frykten for at IS-pirater[34] (Den Islamske staten) skal begynne med piratvirksomhet i Middelhavet kan være et eksempel på at terrorister utfører flere typer «aktiviteter» (Ege, 2015). Terrorister er avhengig av økonomiske ressurser for å kunne drive sine aktiviteter og organiserte kriminelle er profittmotiverte. Eksempelvis dersom motivet i stor grad er økonomisk profitt og det politiske motivet er heller svakt, så kan det si noe om trusselens handlingsmønster og hva trusselaktøren (e) er villig til å risikere. Dette i motsetning til et «rent» ideologisk eller økonomisk motiv. Mulige kombinasjoner (hybrider) må hensynstas når trusler analyseres og vurderes, for slik å få et mest mulig fullstendig beslutningsgrunnlag. Ved sikkerhetsrådgivning har dette på tilsvarende måte betydning for vurderingene og utøvelsen av slik rådgivning.

[33] Bjørgo nevner også voldelige subkulturer i denne sammenhengen.
[34] Terrorgruppen har tidligere hatt navnene al-Qaida i Irak og Den Islamske staten Irak og Levanten (ISIL).

Terrorisme, spionasje, fremmed etterretning, organisert kriminalitet, alvorlig kriminalitet, og volumkriminalitet er tilsiktede hendelser som kan plasseres under security-siden i figuren (figur 1) som ble presentert innledningsvis i oppgaven.

I neste kapittel beskrives metode og forskningsdesign. Deretter analyserer jeg innsamlet data og presenterer funn i datamaterialet mitt ved hjelp av teori og forskning gjennomgått i dette kapittelet.

3. Metode og forskningsdesign

3.1 Innledning

I dette kapittelet vil jeg gjøre rede for vurderingene som ligger til grunn for mitt valg av metode og forskningsdesign. Med forskningsdesign menes «…alt som knytter seg til en undersøkelse» (Johannessen, Tufte, & Christoffersen, 2010). Dette med de vurderingene en gjør forut for undersøkelsen og fremgangsmåten en velger å følge. Oppgavens vitenskapsteoretiske forankring blir vurdert innledningsvis. Valg av informanter, utarbeidelse og gjennomføring av intervju, og forskningsetikk blir videre gjennomgått i denne delen.

3.2.1 Vitenskapsteoretisk forankring og plassering av oppgaven

Samfunnsvitenskapelig metode er «…innrettet mot å etablere kunnskap og teorier om ulike aspekter ved menneskenes samfunnsmessige liv og virke» (Grønmo, 2004, s. 27). Grønmo viser i den forbindelse til tre viktige prinsipper for samfunnsvitenskapelig metode (2004): det ontologiske prinsipp, det epistemologiske prinsipp, og det metodologiske prinsipp. Det ontologiske prinsipp kan forklares ved at «…samfunnsvitenskapen bygger på sannheten som en overordnet verdi» (Grønmo, 2004, s. 17). Kunnskapen forskeren kommer med skal være sann, samtidig som en er ydmyk for at andre studier og andre tilnærminger kan endre denne «sannheten». Det epistemologiske prinsipp «…er at oppfatninger av sannhet i samfunnsvitenskapen er teoretisk, metodologisk og kontekstuelt forankret» (Grønmo, 2004, s. 17). Forskeren må være seg bevisst at arbeidet og kunnskapen han eller hun frembringer påvirkes av disse forholdene. Til sist har vi det metodologiske prinsipp «…at vurderinger av sannhet […] bygger på rasjonelle og logiske kriterier» (Grønmo, 2004, s. 18). Fremgangsmåtene forskeren benytter må være rimelige og kunne være gjenstand for vurdering og kontroll av andre. Positivismekritikkens kjerne er om naturvitenskapelige metoder også kan brukes innen samfunnsforskning. De som er uenig i den positivistiske tilnærmingen, mener at forskere påvirkes av å være er en del av samfunnet de undersøker

og derfor ikke kan være en nøytral observatør (Johannessen et al., 2010, s. 361-363). Med en positivistisk forståelse ville sikkerhetsrådgivning og flere andre områder vanskelig latt seg undersøke med tanke på den dypere forståelsen jeg var ute etter. Denne «samfunnspåvirkningen» er noe jeg er bevisst på som forsker.

«Vitenskapen om tolkninger kalles hermeneutikk» (Fjelland, 1999, s. 43). Hermeneutiske studier og analyser baserer seg på at kunnskapen er påvirket av vår forforståelse og er en del av en større helhet. En kan skille mellom naturforskeren og samfunnsforskeren ut fra deres rolle og deltagelse i feltet som undersøkes. Naturforskeren kan i motsetning til samfunnsforskeren stå på siden og registrere, mens samfunnsforskeren som er en del av samfunnet ikke kan trekke seg unna på tilsvarende måte og konsentrere seg bare om å observere (Johannessen et al., 2010, s. 31). Utgangspunktet for min oppgave var at norske myndigheter bedriver sikkerhetsrådgivning, en del av det jeg kan kalle min forforståelse av tematikken jeg ville undersøke nærmere. Selv om jeg ikke har erfaring med sikkerhetsrådgivning som felt, er jeg i kraft av min arbeidserfaring i politiet påvirket av min forståelse av hvordan informasjon utveksles eller ikke utveksles til og fra politiet (en myndighet). Min forståelse av hvorfor dette gjøres eller ikke gjøres, og hvordan signaler tolkes og håndteres påvirker min tilnærming. Videre påvirker og påvirkes forforståelsen etter hvert som arbeidsprosessen skrider fremover. Dette må en være seg bevisst som forsker. Oppgavens tilnærming kan dermed sies å være av hermeneutisk karakter.

Deduktiv kan forklares med å slutte fra det generelle til det spesielle. Induktiv er en tilnærming der man utleder fra det spesielle til det generelle. Johannessen skriver at deduktiv er å gå «…fra teori til empiri», mens induktiv er å gå «…fra empiri til teori» (Johannessen et al., 2010, s. 51). Empiri kan forklares som «erfaringsbasert informasjon om faktiske forhold i samfunnet» (Johannessen et al., 2010, s. 415). Denne oppgaven tar utgangspunkt i begrepet sikkerhetsrådgivning og jeg tester ikke ut eksisterende teorier om dette temaet. Gjennom intervjuene ønsker jeg å få frem informantenes erfaringer omkring sikkerhetsrådgivning. Dette vil jeg analysere for slik å si noe om hvordan sikkerhetsrådgivningen fungerer ved hjelp av fire problemstillinger. Formålet er å fremskaffe ny kunnskap om sikkerhetsrådgivning. Oppgaven ligger slik nærmest den induktive tilnærmingen. Som det beskrives nærmere senere i kapittelet er ikke målet med oppgaven å generalisere eventuelle funn, selv om jeg ønsker å presentere et bilde av hvordan

sikkerhetsrådgivningen er på «måletidspunktet» mitt. Abduktiv tilnærming er en mellomting mellom induktiv og deduktiv metode. «Abduksjon kan […] knyttes til at forskerens teoretiske bakgrunn gir perspektiver for fortolkningen av dataenes meningsinnhold» (Thagaard, 2009, s. 194). Min erfaring med informasjonsutveksling mellom myndigheter kan gi slike perspektiver.

Hvilket felt en arbeider innen er også en måte å plassere oppgaven i et større bilde. *Samfunnssikkerhetsfeltet* må kunne kalles et tverrfaglig og tverrmetodisk felt. Her finner vi eksempelvis ingeniører og samfunnsvitere, og det arbeides kvalitativt og kvantitativt. *Et sårbart samfunn* kaller sikkerhetsforskningen for et tverrvitenskapelig forskningsfelt pga. den varierte utdanningsbakgrunnen til de som jobber med feltet (NOU 2000:24, 2000, s. 286). I Program for samfunnssikkerhet (SAMRISK II) kan vi lese at «flerfaglige perspektiver og samarbeid mellom ulike forskningsmiljøer er sterkt ønskelig» (Programplanutvalget, 2013, s. 4). Slik jeg ser det eksemplifiserer dette samfunnssikkerhetsfeltets tverrfaglighet. Sikkerhet kan som beskrevet i oppgavens andre kapittel deles i to: safety og security. Denne oppgaven «sorterer» under security (tilsiktede uønskede handlinger) eller sikring for å bruke et norsk ord. Den andre delen av sikkerhet er safety (uønskede handlinger) og kan kalles trygghet på norsk.

3.3.1 Metodevalg

Det er to hovedtyper samfunnsvitenskapelig metode, kvalitativ og kvantitativ metode. Kvantitativ metode bruker gjerne spørreundersøkelser og «man er opptatt av å telle opp fenomener, det vil si kartlegge utbredelse» (Johannessen et al., 2010, s. 31). En ønsker å generalisere, det vil si at en ønsker å si noe om hele populasjonen ut fra det utvalget en har undersøkt. Populasjon kan enkelt forklares med alle enhetene problemstillingen omfatter (Johannessen et al., 2010). Størrelsen på denne gruppen varierer slik fra problemstilling til problemstilling. «Kvalitativ metode er særlig hensiktsmessig hvis vi skal undersøke fenomener som vi ikke kjenner særlig godt, og som det er forsket lite på, og når vi undersøker fenomener vi ønsker å forstå mer grundig» (Johannessen et al., 2010, s. 32). Sikkerhetsrådgivning fra myndigheter til bedrifter som jeg ser nærmere på i denne oppgaven

er et slikt tema. En slik tilnærming kan gi det vi kan kalle *dybdekunnskap*, men dette gir ikke mulighet til å generalisere slik som ved kvantitativ metode. Mitt valg av tilnærming støttes av Jarvis og Holland som skriver at mange viktige områder innen sikkerhetsstudier krever ikke-tellbare tilnærminger for å produsere kunnskap (2015, s. 233).

Det er fordeler med begge tilnærmingene og en må velge hva som gir best grunnlag for å besvare oppgavens problemstilling. Det er også en mulighet å kombinere de to tilnærmingene. Dette kalles *metodetriangulering* og kan eksempelvis være en kombinasjon av spørreundersøkelser og oppfølgende intervjuer av et visst antall informanter. Informanter er de personene som deltar i spørreundersøkelsen. Metodetriangulering gir en kombinasjon av ulike typer data. Data er «informasjon som er bearbeidet, systematisert og registrert i en bestemt form og med sikte på bestemte analyser» (Grønmo, 2004, s. 414). Kvantitative data uttrykkes som tall eller mengdetermer og kvalitative data uttrykkes ofte med tekst (Grønmo, 2004). En kan skille mellom *harde* og *myke* data. Harde data «…kan registreres ved hjelp av tall» og myke data «…i form av av tekst, eventuelt lyd eller bilde» (Johannessen et al., 2010, s. 37).

Metoden skal gi relevant (valid) og troverdig (reliabel) informasjon. Jeg valgte en kvalitativ tilnærming til oppgaven fordi jeg vurderte verdien av å intervjue sentrale personer med god kjennskap og relevant kunnskap om temaet som mer formålstjenlig enn bruk av spørreskjema. Det er usikkert hvor mange svar jeg ville fått og hvilke svar jeg ville fått ved å sende ut en type spørreundersøkelse pr e-post til personer jeg ikke kjenner, med en delvis sensitiv problemstilling. Med delvis sensitiv problemstilling mener jeg at jeg undersøker et tema som ligger nært opptil taushetsbelagt og skjermet informasjon. Jeg har vært tydelig på at oppgaven er ugradert, og at tilnærmingen er valgt for å unngå at ondsinnede personer eller grupper skal kunne misbruke informasjonen. Ved å kontakte informantene i forkant oppstår det en relasjon og en form for tillitsforhold. Dette gir trolig bedre kvalitet på svarene og gjør det trolig lettere å komme med oppfølgingsspørsmål i ettertid. Muligheten til oppfølgingsspørsmål har en både under intervjuet, og i etterkant dersom noe skulle være uklart eller det er behov for utfyllende og oppklarende opplysninger. En kan samtidig få tilgang til annen informasjon. Informanten fra en av de norske myndighetene rådet meg til å lese informasjon om deres virksomhet som ligger åpent på internett, samt aktuelle veiledere på nettet. Dette ga meg bedre mulighet til å forberede meg, noe jeg ikke ville fått ved en

spørreskjemaundersøkelse med ukjente respondenter (personer som svarer på spørreskjema). Informantene jeg har pratet med i forkant av intervjuene har foreslått andre jeg burde kontakte (*snøballmetoden*), noe som også er en fordel med denne tilnærmingen. Næringslivskoordinatoren i Kripos (plassert hos NSR) er et eksempel på en slik informant.

Metodens arbeidsomfang er en del av vurderingen for hvilken metode eller kombinasjon av metoder en skal benytte seg av. En kombinasjon av spørreskjema og intervju ville kunne gi et bredere vurderingsgrunnlag for min oppgave, enn å benytte seg av en metode. Samtidig ville det medføre mer arbeid under informasjonsinnsamlingen, bearbeidelsen av data og analysen. Dybdeforståelse er prioritert i denne oppgaven fremfor et økt antall informanter og muligheten til å generalisere ut fra kvantitative data. Å intervjue tilstrekkelig mange personer til å kunne generalisere funnene ville blitt et for omfattende arbeid på lik linje med en metodekombinasjon. Når det er sagt ville en kombinasjon kunne gitt enda bedre forståelse for oppgavens problemstilling.

Selv om generalisering ikke lar seg ikke gjøre ved en kvalitativ tilnærming, kan en likevel danne seg et slags *situasjonsbilde* ved å intervjue sentrale personer med mye kunnskap om temaet. Muligheten til å gå i dybden på områder eller tema som kunne dukke opp underveis i intervjuene er en annen fordel med intervjuet. Jeg benyttet meg av to intervjuguider (appendiks nr. 1 og appendiks nr. 2): en for myndighetene og en for bedriftene. Intervjuguidene ble brukt som utgangspunkt for en semistrukturert tilnærming. Semistrukturerte intervju kan forklares ved at det «…verken [er] en åpen samtale eller en lukket spørreskjemasamtale» (Kvale, Brinkmann, & Anderssen, 2009, s. 47). Intervjuguidene ble brukt som utgangspunkt for intervjuene, men de ble ikke fulgt slavisk. Informanter er ulike og noen prater mer uoppfordret enn andre. Det en må spørre en informant om kan en annen fortelle uten at det er behov for å stille de samme spørsmålene. En intervjuguide kan derfor vanskelig følges slavisk. Intervjuguiden er likevel en fordel og en god støtte for slik å unngå at intervjuet blir en åpen og ustrukturert samtale. Samtidig sikrer en seg at en ikke glemmer å spørre om viktige tema som ville svekke intervjuenes relevans og muligheten for sammenligning informantene i mellom. Uavhengig av hvilken tilnærming en velger for å besvare problemstillingen (e), er formålet og skaffe til veie data som er relevant og troverdig.

Formålet med oppgaven var å få svar på hvordan sikkerhetsrådgivning bedrives fra norske myndigheter overfor store norske private bedrifter med virksomhet i utlandet. Dette undersøkte jeg ved å intervjue noen utvalgte virksomheter, flere norske myndigheter, og et rådgivende organ stiftet av næringslivet. Jeg arbeidet med utgangspunkt i fire problemstillinger:

1. Hvordan bedriver norske myndigheter sikkerhetsrådgivning overfor store norske bedrifter med virksomhet i utlandet, og på hvilke områder gis det slik rådgivning?
2. I hvilken grad er det kontakt mellom aktørene og hvorfor samarbeider de, hvilken type kontakt har de, og hvor hyppig er denne kontakten?
3. Er det noen aktører som samarbeider mer enn andre, og hvorfor er det eventuelt slik?
4. Er det, på bakgrunn av de fem referansehendelsene, mulig å se endringer i sikkerhetsrådgivningen og dialogen mellom myndighetene og bedrifter?

Med utgangspunkt i de fire problemstillingene ønsker jeg å undersøke hvordan sikkerhetsrådgivning utøves fra myndighetshold, og belyse eventuelle endringer som identifiseres. Dette med et ønske om å bidra til at sikkerhetsrådgivningen skal fungere best mulig for de involverte partene. Aktørene kan ha ulik tilnærming som følge av deres arbeidsforhold og ansvarsområder. Dette kan være et godt utgangspunkt for erfaringsoverføring og derigjennom forbedringer av samarbeid dem i mellom, samt egne rutiner. Videre ville jeg undersøke om fem alvorlige hendelser med stor medieomtale har påvirket myndighetenes oppfatning og tilnærming til temaet, og i så fall på hvilken måte. Referansehendelsene jeg benyttet meg av er anslaget mot den norske ambassaden i Damaskus (2006), anslag mot Telenors butikker i Pakistan (2006), piratkapringer de siste årene (2006-), terrorangrepet 22. juli 2011 og terrorangrepet mot In Amenas 16. januar 2013.

For å kunne besvare problemstillingen må den operasjonaliseres. «Prosessen fra det generelle til det konkrete kan betegnes som operasjonalisering» (Johannessen et al., 2010, s. 63). Validitet (validity) uttrykker «hvor godt, eller relevant, data representerer det

fenomenet som skal undersøkes» (Johannessen et al., 2010, s. 208). Spørsmålene måtte derfor være så konkrete at jeg kunne besvare problemstillingene. Reliabilitet (reliability) uttrykker «hvor pålitelige data er» (Johannessen et al., 2010, s. 404). I følge Kvale «…behandles [reliabilitet] ofte i sammenheng med spørsmålet om hvorvidt et resultat kan reproduseres på andre tidspunkter av andre forskere» (Kvale et al., 2009, s. 250). Informantene svarer på hvordan de opplever ting på det tidspunktet de intervjues og svarene deres vil derfor kunne endre seg ettersom tiden går. Etter å ha gjennomført intervjuene med utgangspunkt i intervjuguidene (appendiks nr. 1 og appendiks nr. 2) ønsket jeg å besvare de overnevnte problemstillingene.

Flere av informantene jeg har intervjuet gir ut veiledningsmateriell alene og/eller sammen med andre. Noen av dokumentene blir brukt som en del av grunnlaget for funn og analysekapittelet. I dokumentene kan det fremkomme henvisninger mellom aktørene, og tegn på samarbeid dem i mellom. Eventuelle henvisninger til referansehendelsene jeg har brukt kan også være interessant.

3.3.2 Informanter

I denne delen begrunner jeg valg av og antall informanter, samt viser en oversikt over informantene (figur 4).

3.3.2.1 Valg av informanter og utvalgsstørrelse

Det er ulike måter å komme i kontakt med informanter på og jeg benyttet flere fremgangsmåter. Fremgangsmåtene har igjen sine ulike styrker og svakheter. Noen navn har jeg fått fra faglærer på Politihøgskolen og via min veileder. Det å innledningsvis kunne si at en har blitt anbefalt å ta kontakt av en person informanten gjerne kjenner er en fin tilnærming. Min erfaring er at personene er positive til å stille opp, og at det er litt enklere med denne tilnærmingen. Samtlige jeg har kontaktet har vært positive til å stille opp som informanter og ønsket mer kunnskap omkring temaet sikkerhetsrådgivning.

Informantene har ved noen anledninger uoppfordret foreslått andre personer (eller etater) jeg burde kontakte. I kontaktetableringen begynte jeg derfor å spørre personene direkte om de samarbeider med personer eller etater som de mener jeg burde kontakte. Dette er en fin måte å finne sentrale personer med inngående kunnskap om temaet. Det er dermed ikke sagt at en vil kontakte alle som foreslås, men en kan ta en vurdering på hvem en vil kontakte og begrunne valgene. Dette har vært en effektiv måte å finne relevante og aktuelle informanter. Jeg har ønsket å snakke med de som faktisk arbeider sammen for å se hvordan dette samarbeidet fungerer. Det er informantene som best vet hvem de samarbeider med. Samtidig har det vært interessant å undersøke om det er myndigheter bedriftene pr i dag ikke samarbeider med, men som de ønsker et samarbeid med. Eventuelt et ønske om tettere samarbeid.

Det er praktisk umulig å undersøke hele populasjonen, og en må derfor avgrense undersøkelsen til et utvalg fra populasjonen. Et utvalg er de man velger å undersøke fra populasjonen. Utvalget en foretar fra populasjonen er *representativt* dersom «…sammensetningen av ulike egenskaper i utvalget tilsvare[r] sammensetningen i populasjonen» (Johannessen et al., 2010, s. 241). I denne oppgaven var ikke målet å velge ut et representativt utvalg fra populasjonen.

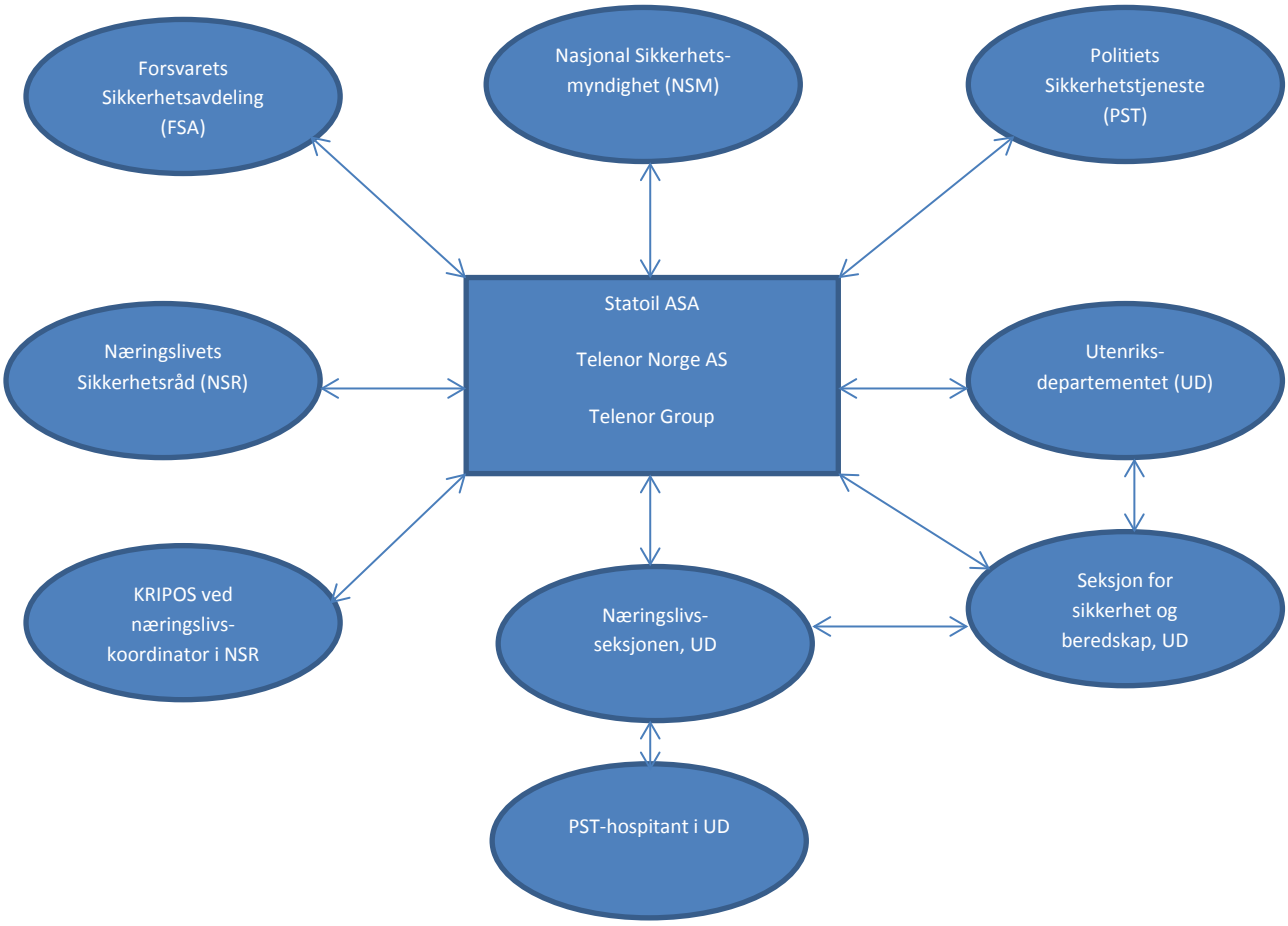
Det er en vurdering hvor mange informanter en skal intervjue og det er ingen klare regler for hvor mange intervjuer en skal gjennomføre. Jeg gjennomførte elleve intervju. Hensiktsmessigheten blir det avgjørende, «…det vil si hva som er mest formålstjenlig for å kunne besvare problemstillingen (e)» (Johannessen et al., 2010, s. 116). I tillegg må en vurdere tid og ressurser en har til rådighet. De to sistnevnte faktorene kan slik påvirke undersøkelsens kvalitet. Det å benytte seg av et begrenset antall informanter og prøve å få mest mulig informasjon fra dem er et kjennetegn ved kvalitativ metode (Johannessen et al., 2010). En må være bevisst på de valgene en tar, samt svakhetene og styrkene de medfører. I forkant av intervjuene vet en ikke om informantene har tilstrekkelig med informasjon og dette kan påvirke antallet intervjuer og antall informanter (Johannessen et al., 2010). Ved det første intervjuet jeg foretok viste det seg at informanten ikke kunne belyse spørsmålene på en tilstrekkelig måte i forhold til oppgavens tematikk. Jeg foretok derfor et nytt intervju med en annen person hos denne myndigheten med god kjennskap til tema. Informanten hadde fått spørsmålene tilsendt i forkant. Kanskje jeg kunne unngått å gjennomføre to

intervju med samme myndighet om jeg hadde pratet mer inngående med informanten i forkant for slik å forsikre meg om at informanten hadde den aktuelle typen kunnskap. Informanten kunne da henvist meg videre. Det kan som nevnt fremkomme aktuelle aktører under intervjuene som en ikke kjente til i forkant, noe som også kan påvirke mengden. Dersom en velger å ikke intervjue aktuelle aktører må dette begrunnes.

Etter at en informant henviste meg videre for å få besvart noen av spørsmålene han ble stilt, fikk jeg et skriftlig svar (e-post) på noen spørsmål. På det tidspunktet hadde jeg fått svar på spørsmålene fra en annen informant, og det ble derfor et supplement. E-posten ble besvart av Næringslivsseksjonen i UD og en hospitant i UD fra PST. Dette i en og samme e-post. I den skjematiske informantoversikten, under neste punkt, er det derfor piler mellom det vi kan kalle *UD-informanter*. UD hadde i april 2014 åtte avdelinger med flere underliggende seksjoner[35]. Seks intervjuer ble gjennomført ansikt-til-ansikt på informantenes arbeidssted. Fem av intervjuene ble foretatt pr telefon. Informanten fra FSA med kjennskap til E, har gitt informasjon også om Es virksomhet etter selv å ha pratet med E. Jeg har ikke lyktes å komme i kontakt med E, og henvendelsene mine dit har blitt kanalisert til FSA. Dette i tillegg til Informasjon fra nrk.no, artikler med mer har gitt et bilde av Es sikkerhetsrådgivning. Jeg intervjuet tre informanter i to ulike private norske selskaper med virksomhet i utlandet, syv informanter ved fem ulike offentlige instanser (myndigheter) og en informant ved et rådgivende organ stiftet av næringslivet (Næringslivets sikkerhetsråd). Den overnevnte e-posten har ytterligere to informanter. Jeg har prioritert informanters erfaring og kunnskap fremfor antallet informanter. Et økt antall med intervjuer vil ikke belyse oppgavens problemstilling ytterligere dersom informantene ikke har kjennskap og kunnskap om det aktuelle tema.

[35] UDs organisasjonskart oppdatert april 2014: Næringslivsseksjonen er plassert under Avdeling for kultur, norgesfremme og protokoll. Seksjon for sikkerhet og beredskap er plassert under Serviceavdelingen.

3.3.2.2 Oversikt og begrunnelse for valg av informanter



Figur 4: Oversikt over informantene

Utgangspunktet for mitt valg av informanter var myndigheter som jeg på forhånd antok at bedrev sikkerhetsrådgivning. På bakgrunn av oppgavens tema var det derfor naturlig å kontakte norske sikkerhetstjenester. PST, E og NSM ble valgt av denne årsaken. E lyktes jeg ikke å få som informant og i den forbindelse kom jeg i kontakt med FSA. UDs ansvarsområde er norske interesser utenfor Norges grenser og de var derfor en myndighet jeg ønsket å snakke nærmere med. NSR (rådgivende organ stiftet av næringslivet) er et kontaktpunkt mellom næringslivet og myndigheter, og gjennom kontakten med dem ble jeg tipset om næringslivskoordinatoren «deres» fra Kripos.

På bedriftssiden syns jeg Statoil var en interessant informant. For det første fordi de har hatt virksomhet i utlandet over lengre tid. For det andre, og ikke av mindre betydning, pga. In Amenas-hendelsen i 2013. Statoil selv (Statoil ASA, 2013b) og UD (Utenriksdepartementet, 2013) har evaluert hendelsen i åpne rapporter. Dette terrorangrepet har aktualisert sikkerhetsrådgivning fra myndigheter til næringslivet. Telenor ble valgt pga av deres erfaringer i Pakistan tilbake i 2006. Anslagene mot deres butikker på den tiden kunne ha betydning for sikkerhetsrådgivningen de mottar fra norske myndigheter.

Direktorat for samfunnssikkerhet og beredskap (DSB) og Politidirektoratet (POD) kunne vært aktuelle informanter. POD kunne kanskje gitt et overordnet bilde av politiets tilnærming, men jeg er ute etter hvordan sikkerhetsrådgivningen faktisk utøves og POD ble av den grunn ikke kontaktet. DSB har først og fremst Norge som arbeidsområde: herunder nasjonal, regional og kommunal beredskap. Videre regnes ikke DSB som en sikkerhetstjeneste slik som PST, E og NSM. Ut fra disse vurderingene og oppgavens omfang prioriterte jeg de informantene jeg anså som viktige og naturlige.

3.3.3 Ansikt-til-ansikt-intervju versus telefonintervju

Intervjuer kan bli foretatt direkte ansikt-til-ansikt, på telefon eller via internett. Jacobsen bruker uttrykkene *i fysisk nærhet av hverandre* og *fysisk atskilt* (2005, s. 143). Tilnærmingene har sine fordeler og ulemper. Telefonintervju er i likhet med internettintervju tids- og kostnadsbesparende, og de lave kostnadene er «…[dets] klart sterkeste side» ifølge Jacobsen (2005, s. 144). En fordel med telefonintervjuet er at en ikke begrenses av geografisk avstand (Gillham, 2005, s. 106). Ikke-verbale elementer er vanskeligere å fange opp ved telefonintervju, en svakhet som kan begrenses ved å benytte seg av lyd- og bildeoverføring ved bruk av eksempelvis Skype. Skype eller videointervju ble ikke brukt i oppgaven. For å skape en best mulig atmosfære var jeg bevisst på å bruke aktiv verbal lytting (virksomme småord) for å vise at jeg fulgte med og forstod det de fortalte (Mathisen & Høigaard, 2004). Det kan også være fordeler med at en ikke kan observere hverandres *opptreden* i intervjuet, da intervjuer og informant påvirker hverandre i intervjusituasjonen. Intervjueffekt kan forklares ved «…at intervjuers tilstedeværelse skaper spesielle resultater» (Jacobsen, 2005, s.

167) og/eller unormal opptreden hos respondenten. Dette kan begrenses ved telefonintervju, samtidig som det er vanskeligere å fange opp når en bør stoppe eller gi seg som intervjuer, eksempelvis ved *utspørring* (uttømming) av et tema eller avslutte et intervju. Tema som er sensitive kan være lettere å prate om ansikt-til-ansikt enn over telefon (Jacobsen, 2005). Ved å sende ut spørsmål i forkant har informantene kunne sette seg inn i tema og på den måten unngå at det kom uforutsette spørsmål som kunne oppleves som sensitive i telefonintervjuene. Her er det også mulighet til å få klarert uttalelser med overordnede om det skulle være behov for det.

En del intervju ble gjort over telefon for å begrense reisetid og utgifter. Telefonintervju ble etter en helhetsvurdering benyttet i 5 av de 11 intervjuene, hvorav en av informantene svarte for to aktører. Dette forenklet muligheten til å finne tidspunkt som passet for informanter, egen arbeidsgiver, og meg selv. Lengden på intervjuene begrenses ved telefonintervju (Gillham, 2005). Samtidig stiller det større krav til effektivitet og struktur i intervjuet, noe som også kan sies og være positivt.

De første intervjuene jeg gjennomførte var ansikt-til-ansikt. Jeg erfarte at det var en fornuftig tilnærming å starte med ansikt-til-ansikt-intervjuene. Det å kunne henvise til andre informanter (etter avtale med dem) og i noen tilfeller ha intervjuet personer i samme virksomhet tidligere var positivt for gjennomføringen av telefonintervju. Dette opplevde jeg at reduserte ulempene ved å bruke telefonintervju. Kombinert med utsendelse av spørsmål i forkant var det et godt utgangspunkt for intervjuene. En av informantene jeg intervjuet på telefon flyttet avtalen to ganger, dette hadde trolig ikke skjedd om jeg hadde møtt på informantens arbeidsplass. Dette kan tyde på at det er lettere å flytte på avtaler som skal gjennomføres på telefon, men det var ikke noe «problem» ved gjennomføringen av telefonintervjuene ellers i denne oppgaven. Ved telefonintervju kan en ikke se hvor informanten befinner seg, men jeg forstod det slik at de befant seg på sitt arbeidssted. Jeg opplevde informantene som konsentrert og *tilstede* på lik linje med intervjuene gjennomført ansikt-til-ansikt. Ved at de første intervjuene ble gjennomført ansikt-til-ansikt kunne jeg sammenligne gjennomføringen av telefonintervju med de intervjuene. Kvaliteten på telefonintervjuene skilte seg ikke slik jeg opplevde det ut på noen negativ måte.

Kunne eller burde jeg valgt andre informanter som er tilgjengelig i mitt «nærområde»? Utvalget i undersøkelsen er valgt på grunn av deres inngående kjennskap til temaet, og det var ikke aktuelle informanter i mitt nærområde. Svakheter ved å foreta telefonintervju tilstrebet jeg å redusere samtidig som jeg vurderte det som mindre viktig enn informantenes inngående kunnskap. Jacobsen oppsummerer at ansikt-til-ansikt-intervju har «…mindre alvorlige trusler både mot gyldighet og pålitelighet» sammenlignet med fysisk atskilte intervju, men det er ikke en «…absolutt sannhet» (2005, s. 144). Jeg hadde en bevisst tilnærming til svakhetene ved telefonintervju, gjorde flere tiltak for å begrense disse svakhetene og nyttiggjorde meg fordelene ved denne intervjuformen.

Innhenting av data ble gjort gjennom intervjuer med relevante og sentrale personer innen problemstillingens tema. For å svare på problemstillingen gjennomførte jeg en casestudie. Casestudie kan defineres som en «detaljert og intensiv studie av en enkelt analyseenhet eller av noen få analyseenheter som sammenliknes» (Grønmo, 2004, s. 414). Dette gjorde jeg ved å intervjue personer fra to store private selskap med virksomhet i utlandet og deres samarbeidspartnere (myndigheter). For deretter å sammenligne informasjonen som fremkom fra bedriftene og fra myndighetene. Ved å intervjue to virksomheter ønsket jeg få muligheten til å belyse eventuelle ulikheter dem i mellom, samt i hvilken grad de fem overnevnte hendelsene har påvirket sikkerhetsrådgivningen de mottar fra myndighetene. Dette med tanke på hvordan kontakten og samarbeidet er mellom myndighetene, og mellom myndigheter og bedrifter. Videre ønsket jeg at en av virksomhetene skulle ha erfaring med angrep mot virksomheten forut for de to siste referansehendelsene. Dette for å se om det kunne hadde påvirket deres virksomhet på en slik måte at hendelsene hadde en annen betydning/påvirkning.

Jeg har sett nærmere på 22. juli-rapporten (NOU 2012:14, 2012), Statoils In Amenas-rapport (Statoil ASA, 2013b) og UDs rapport etter In-Amenas-hendelsen (Utenriksdepartementet, 2013). De er skrevet i etterkant (reaktive og åpne rapporter) av alvorlige terrorhendelser og gir mye informasjon om hvordan ting fungerte og forslag til endringer. Rapportene brukes i ulik grad i oppgavens funn og analyse-kapittel (kapittel 4).

3.3.4 Valget av referansehendelser

Det har vært flere terrorhendelser i nyere tid. Jeg har valgt å relatere spørsmålene i intervjuguidene (appendiks nr. 1 og appendiks nr. 2) til fem hendelser som jeg kan kalle *norske*. Dette er hendelser jeg antok at informantene hadde kjennskap til, dog i større og mindre grad. Anslaget mot den norske ambassaden i Damaskus i 2006 rammet norske interesser, nærmere bestemt norske myndigheter. Anslag mot Telenors butikker i 2006 rammet en norsk bedrift med virksomhet i utlandet direkte. Piratkapringer i Adenbukta og omkringliggende områder har rammet både norsk og utenlandsk rederivirksomhet. Terrorangrepet mot regjeringskvartalet og Utøya fant sted i Norge (2011), og terrorangrepet mot In Amenas-anlegget i Algerie (2013) har norske Statoil som en av partene i et joint-venture samarbeid. I etterkant av hendelsene er det nedsatt granskningsgrupper og skrevet omfattende rapporter (NOU 2012:14, 2012; Statoil ASA, 2013b; Utenriksdepartementet, 2013). Rapportene er viktige ikke bare for de som er direkte involvert i granskningen, men også aktører som har samfunnssikkerhet som arbeidsfelt. De belyser samarbeid mellom norske myndigheter og privat virksomhet. Videre gir rapportene anbefalinger og forslag til forbedringer.

Nærheten til hendelser medvirker trolig til hvordan vi påvirkes av hendelsene, både bevisst og ubevisst. Terrorangrepet mot USA den 11. september 2001, Madrid 11. mars 2004 og London 7. juli 2005 kunne eksempelvis vært brukt som referansehendelser. Jeg valgte fem *norske* hendelser av to årsaker. For det første fordi jeg ønsket at informantene skulle ha kjennskap til hendelsene. Noe som er en forutsetning for å kunne svare på om hendelsene har påvirket myndigheters sikkerhetsrådgivning overfor bedrifter. For det andre fordi dette er hendelser som (i ulik grad) har påvirket Norges befolknings forhold til terror og andre tilsiktede og ondsinnede handlinger i en eller annen grad. Hendelsene kan karakteriseres som *nære* i form av den omfattende medieomtalen, gjerne særlig 22. juli og In Amenas. 22. juli gikk 77 menneskeliv tapt, og i In Amenas gikk fem norske menneskeliv tapt.

I etterkant av intervjuene ønsket jeg å undersøke om det over tid var mulig å se en endring i myndighetenes sikkerhetsrådgivning til bedriftene. Ved gjennomføringen av intervjuene avtalte jeg med informantene at det kunne komme oppfølgingsspørsmål når jeg senere

skulle arbeide med analysen. Dette var informantene positiv til og jeg kontaktet dem i etterkant med spørsmål knyttet til ytterligere tre referansehendelser. Dette for å se om det var eventuelle (merkbare?) endringer i sikkerhetsrådgivningen (en tidslinje). Tilleggsspørsmålene (fremgår i appendiks nr. 1 og appendiks nr. 2) angikk hendelsene mot ambassaden i Damaskus, Telenor i Pakistan og piratkapringer. I intervjuet med informanten fra Telenor Group hadde anslagene mot deres butikker i Pakistan vært tema. De tre tilleggsspørsmålene og andre oppklarende spørsmål i etterkant av intervjuene viser viktigheten av å avtale muligheten for å ta kontakt i ettertid.

3.3.5 Intervjuguiden – spørsmål og anonymitet

Kunne endringer i intervjuguiden og dens spørsmål gitt mer relevant og troverdig informasjon (data)? Oppgaven er ugradert og jeg har valgt bort spørsmål som kunne berøre skjermingsverdig og taushetsbelagt informasjon. Det er med ett unntak åpenhet om arbeidssted og navn på informantene i oppgaven. Informanten ved FSA ønsket å være anonym. Det er ikke laget noe vedlegg i oppgaven med oversikt over informantenes navn og arbeidssted. Dette kan derimot legges frem for oppgavens sensorer om ønskelig.

Utgangspunktet for forskning er offentlig tilgjengeliggjøring av informasjonen som fremkommer og åpenhet om hvem som er informanter. Dette bør tilstrebes da dette forenkler etterprøvbarheten og kontroll av informasjonen. Til tross for dette vil det ved noen arbeidssteder være ønskelig med anonymitet på grunn av deres arbeidsoppgaver og arbeidsfelt. Anonymitet kan da forsvares for ikke å hemme deres videre arbeid, og kan også være en nødvendig forutsetning for at de vil uttale seg. Dette gjelder informanten ved FSA.

Spørsmål som gjelder opplevelsen av samarbeidet med andre aktører tenkte jeg i forkant av intervjuene at kunne være utfordrende å svare på, men det var tilsynelatende uproblematisk. Målet med oppgaven er å belyse og gjerne gi et bidrag til å videreutvikle dagens sikkerhetsrådgivning. Da kan kritikk dem i mellom være negativt for et videre samarbeid, noe som igjen kan ha betydning for hvilken vekt en kan tillegge svarene.

3.3.6 Utsending av spørsmål i forkant

Tema kan som nevnt oppleves å være delvis sensitivt, og det å uttale seg om samarbeid med andre kan være utfordrende. Utsending av intervjuspørsmål til informantene i forkant kan derfor være positivt. De kan da vurdere om de må avklare hva de kan si noe om og dette kan slik ha *en beroligende effekt*. Det kan samtidig virke positivt på hukommelsen. Med det mener jeg at de kan komme på ting de ellers ikke ville husket på om det skulle besvare spørsmålene direkte uten å ha fått tilsendt spørsmålene i forkant. Da jeg benyttet meg av et semistrukturert intervju kunne jeg foreta endringer fra de utsendte spørsmålene uten at det vil ødelegge den positive effekten av utsendelsen. Jeg sendte flesteparten av spørsmålene i forkant. På denne måten kunne informantene forberede seg (og ved behov klarere med ledere etc.). Samtidig ble de ikke overveldet ved at jeg sendte alle spørsmålene. Når dataene skal tolkes i ettertid må en ta til etterretning at informantene har hatt mulighet til å forberede seg og dataene kan ha blitt ulike sammenlignet med om en var uforberedt. Jeg sendte spørsmålene kort tid forut for intervjuene for å beholde litt av spontaniteten, noe Gillham har anbefalt (2005, s. 104). Da jeg ønsket mest mulig informasjon mener jeg dette var en fornuftig fremgangsmåte. Slik jeg vurderer det reduserte dette også sannsynligheten for at informantene skulle revurdere sin deltagelse. Informantene har sagt at de satte pris på å få tilsendt spørsmål i forkant. Muligheten til å få mest mulig informasjon (dybdeinformasjon) er i denne oppgaven prioritert fremfor det spontane en kan gå glipp av ved ikke å sende ut spørsmålene i forkant.

3.3.7 Gjennomføring av intervju

Intervjuene er tatt opp på lyd (mp3-spiller) etter samtykke fra informantene. De er deretter nedskrevet som resymé. Dette gjorde at jeg kunne fokusere på selve intervjuet og ikke nedtegning av svar underveis. Jeg noterte likevel stikkord underveis for å strukturere intervjuet og kunne ta tak i tema og nye spørsmål som dukket opp underveis. Informantene har fått tilsendt resymeene og kunne kommet med innspill dersom de ønsket det. Dette kan på lik linje med utsendelse av spørsmålene i forkant av intervjuet, være med på å skape en

avslappet atmosfære under intervjuet. Informantene er kjent med at lydopptak og resymeer destrueres etter at oppgaven er ferdig sensurert.

3.4 Forskningsetikk

«Begrepet «forskningsetikk» viser til et mangfoldig sett av verdier, normer og institusjonelle ordninger som bidrar til å konstituere og regulere vitenskapelig virksomhet» (Den Nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora, 2006, s. 5). Knut W. Ruyter bruker uttrykket forsvarslinjer for å vise behovet for forskningsetiske kontroll og beskyttelse, en betegnelse han opplyser at han har hentet ideen om fra Henriette Sinding Aasen (Ruyter, 2003). Jeg bruker benevnelsen retningslinjer i oppgaven. Jeg vil nå ta for meg etiske problemstillinger som har vært aktuelle for min oppgave.

3.4.1 Fritt informert samtykke

En retningslinje for forskning er at deltagelse i undersøkelser er frivillig. For å kunne anse deltagelsen som frivillig må vedkommende være informert om hva som skal undersøkes og hva undersøkelsen skal benyttes til. Det kan være vanskeligere å avvise forespørsler når forskeren henviser til personer informantene kjenner fra tidligere. Dersom en har fått kontaktinformasjon fra en overordnet er det viktig å opplyse at den overordnede samtykker til deltagelsen, men at informanten selv står fritt til å velge å delta eller ikke. Informanter skal også informeres om at et samtykke kan trekkes tilbake når som helst uten at dette skal få noen form for negative konsekvenser for informanten. Det kan by på utfordringer dersom en har begynt å benytte seg av data fra informanten, da et tilbakekall av samtykke medfører at en ikke kan bruke dataene. Informanten skal vite hva han eller hun har samtykket til å delta i og god informasjon i forkant vil i stor grad kunne redusere sannsynligheten for at informanter trekker seg underveis i forskningsprosessen. Utsendelsen av spørsmål i forkant av intervjuene ga informantene mulighet til å avklare hva de kunne uttale seg om dersom det var behov for det. Samtidig reduserte dette sannsynligheten for at informantene uttalte

seg om noe de ikke skulle og er slik en måte å ivareta informanter som intervjues om en tematikk som kan oppleves som sensitiv. Dette er i så måte et godt eksempel på at god forskningsetikk har positiv innvirkning også på den praktiske gjennomføringen.

Jeg har vært tydelig på at jeg studerer ved Politihøgskolen og er ansatt i politiet. Det er grunn til å tro at informanter og myndighetene/bedriftene de er ansatt hos ønsker å ha et godt forhold til politiet. Informantene kan derfor være mer positiv til deltagelse enn ellers. Dette må en være seg bevisst som student og polititjenestemann. Det er likevel ikke noe som tilsier at det er noen betenkeligheter knyttet til dette ved gjennomføringen av mine undersøkelser.

3.4.2 Konsesjon, meldeplikt og forholdet til anonymitet

Det er også en retningslinje at «alle forsknings- og studentprosjekt som innebærer behandling av personopplysninger skal meldes» (Den Nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora, 2006, s. 14). I innhentingen og senere bruk av data blir det i denne oppgaven ikke lagret eller behandlet personopplysninger og oppgaven er derfor ikke *meldepliktig*. Deltagelse i et forskningsprosjekt kan være anonym. Dette er et viktig tema ved deltagelsen og hvordan en forholder seg til dette kan være avgjørende for hvilke informanter som er villig til å stille opp. Grønmo viser til utviklingen av syv forskningsetiske normer hvorav offentlighet er den første normen: «vitenskapelig virksomhet skal foregå i full åpenhet, og rapporter om utgangspunkt, fremgangsmåter og resultater skal publiseres eller offentliggjøres i sin helhet» (Grønmo, 2004, s. 19). Det vil si at resultatene gjøres tilgjengelig for alle som ønsker det. Forskning på områder som berører taushetsplikt, og/eller kan gi personer med ondsinnede hensikter kunnskap de kan misbruke problematiserer og utfordrer dette offentlighetsprinsippet. Oppgaver med sensitivt innhold kan da skjermes. I denne oppgaven har jeg undersøkt hvordan sikkerhetsrådgivningen fungerer uten å gå nærmere inn på metoder. Dette nettopp for å unngå befatning med sensitiv informasjon og muligheten for at uvedkomne kunne misbruke informasjonen som fremkommer i oppgaven.

Dersom det er *åpenbart* hvem som blir brukt som informanter, eller det er få å velge mellom, er det vanskelig å kunne garantere anonymitet. Her er det svært viktig å være tydelig overfor informantene slik at en ikke har ulik forståelse. Forskeren har mest informasjon og har ansvaret for å holde informanten (e) informert. Dette kan i tillegg medføre unødvendig ekstraarbeid om misforståelser skulle komme frem underveis i arbeidet. Det å intervjue relevante og sentrale informanter uten at det er mulig å tenke seg til deres arbeidssted kan være utfordrende. I denne oppgaven er det bare benyttet anonymitet i forhold til navnet på informanten ved FSA.

Tema for oppgaven er valgt ut fra at oppgaven skal være åpen og ugradert. Den kan som nevnt sies å tendere mot sensitive områder og informantene må derfor være klar over at det som sies ikke kan være av gradert karakter selv om jeg er ansatt i politiet i tillegg til å være student. Denne «dobbeltrollen» kan også påvirke personers vilje til å fortelle om sensitive opplysninger. Skille mellom forskerrollen og politirollen må derfor tydeliggjøres overfor informanter og seg selv som forsker. Dette er derfor presisert i min kontakt med informantene.

4. Analyse og funn

4.1 Innledning

I denne delen analyserer jeg dataene jeg har samlet inn. Dette bruker jeg til å besvare oppgavens fire problemstillinger. Teori og forskning gjennomgått i oppgavens andre kapittel benyttes i analysen. Kapittelet starter med en presentasjon av de nevnte problemstillinger. Etter en kort presentasjon av informantene (myndigheter og bedrifter) brukes resten av kapittelet til å besvare de fire problemstillingene hver for seg.

Sikkerhetsrådgivning fra myndigheter til bedrifter er et felt i utvikling. Det er eksempelvis stilt spørsmål ved om E skal begynne å gi råd direkte til norsk næringsliv (Veum & Olsson, 2013). Daværende statsminister Jens Stoltenbergs holdt 23. januar 2013 en redegjørelse i Stortinget om terrorangrepet i Algerie (sak nr. 3). Helga Pedersen (Arbeiderpartiet) sa i sitt innlegg i redegjørelsen at «Norske næringslivsbedrifter må ha gode sikkerhetsforanstaltninger når de er i risikoutsatte land og norske myndigheter må bidra med best mulige råd». Daværende næringsminister Trond Giske (Arbeiderpartiet) uttalte omtrent på samme tidspunkt at «Vi må alltid være forberedt på at farlige situasjoner kan oppstå. Det vi må legge til rette for er at bedriftene kan bruke den informasjonen som finnes til å gjøre risikoen for arbeidstakerne så liten som mulig…» (Graf, 2013)[36]. En eller flere nye tilsiktede hendelser (terroraksjoner mm.), «vellykket» eller ikke, vil kunne føre til endringer i utøvelsen av og etterspørselen av sikkerhetsrådgivning fra norske myndigheter. Tidligere endringer i sikkerhetsrådgivningen (problemstilling nr. 4) er noe av det jeg undersøker i denne oppgaven.

Drøftingen i oppgavens innledningskapittel viser at begrepet sikkerhetsrådgivning ikke har en omforent definisjon, og at det kan variere hva en «legger i» begrepet. Dette vil komme frem i gjennomgangen under.

Der jeg benytter meg av direkte sitat fra informanter i oppgaven, er informantenes uttalelser skrevet i anførselstegn.

[36] Artikkelen er elektronisk og unummerert.

4.2 Oppgavens problemstilling (forskningsspørsmål)

Oppgaven har fire problemstillinger:

1. Hvordan bedriver norske myndigheter sikkerhetsrådgivning overfor store norske bedrifter med virksomhet i utlandet, og på hvilke områder gis det slik rådgivning?
2. I hvilken grad er det kontakt mellom aktørene og hvorfor samarbeider de, hvilken type kontakt har de, og hvor hyppig er denne kontakten?
3. Er det noen aktører som samarbeider mer enn andre, og hvorfor er det eventuelt slik?
4. Er det, på bakgrunn av de fem referansehendelsene, mulig å se endringer i sikkerhetsrådgivningen og dialogen mellom myndighetene og bedrifter?

4.3 Presentasjon av oppgavens informanter: myndigheter og bedrifter

Her er en kort presentasjon av myndighetene og bedriftene jeg har innhentet informasjon om og benytter i oppgaven. De fire myndighetene som blir presentert først (PST, E, FSA og NSM) er EOS-tjenester. På EOS-utvalgets nettsider nevnes FSA som en av EOS-tjenestene, men FSA er som beskrevet under (punkt 4.3.3) en avdeling underlagt både Forsvarssjefen og NSM. Offentlige myndigheter som bedriver etterretnings-, overvåknings- og sikkerhetstjeneste kontrolleres av EOS-utvalget[37] for å sikre at tjenestene ikke handler utenfor sitt mandat (EOS-utvalget, u.å.-a).

[37] Stortingets kontrollutvalg for etterretnings-, overvåknings og sikkerhetstjeneste

4.3.1 PST (Politiets sikkerhetstjeneste)

PST består i dag av 27 avdelinger[38], med den sentrale enhet for PST (DSE) som har totalansvaret plassert i Oslo. «PST er en del av politiet, men er direkte underlagt Justis og beredskapsdepartementet» (Etterretningstjenesten et al., 2013, s. 2). Det «…er Norges sivile innenlands etterretnings- og sikkerhetstjeneste» (Etterretningstjenesten et al., 2013, s. 2) og tjenestens oppgaver fremgår av politiloven (1995) § 17 b (kapittel III a) og instruks for Politiets sikkerhetstjeneste (2005). I *Politiets Sikkerhetstjeneste oppgaver og virksomhet* (Politiets sikkerhetstjeneste, 2007, s. 11-12)[39] er PSTs sentrale ansvarsområder listet opp: kontraterror, kontraetterretning, ikke-spredning av masseødeleggelsesvåpen (MØV), kontraekstremisme, trusselvurderinger, myndighetspersoner og livvakttjeneste, sikkerhetsrådgivning.

4.3.2 E-tjenesten (Etterretningstjenesten)

E som er underlagt Forsvarssjefen har i motsetning til PST ansvar for området utenfor Norges grenser. Det er Norges utenlandsetterretningstjeneste og E «…er ikke avgrenset til å arbeide med militære problemstillinger» (Etterretningstjenesten et al., 2013, s. 2). Es arbeidsområde fremgår av etterretningstjenesteloven § 3 (1998): internasjonal terrorisme, spredning av MØV er to av flere opplistede oppgaver. I likhet med PST samler tjenesten informasjon (tilveiebringelse av informasjon) som bearbeides og analyseres for slik å identifisere trusler rettet mot Norge og norsk virksomhet. E er som tidligere nevnt ikke informant i oppgaven, men presenteres her fordi tjenesten omtales inngående i oppgaven.

[38] Det kan være mer presist å si at det er 26 avdelinger og et hovedkontor (DSE) som har totalansvaret i tillegg til ansvaret for Oslo politidistrikt (27 til sammen).
[39] Informasjonsfolderen om PST, som er fra 2007, fikk jeg et eksemplar av i forbindelse med intervjuet av informanten i PST gjennomført i 2014.

4.3.3 FSA (Forsvarets sikkerhetsavdeling)

FSA er en avdeling i Forsvaret og er i likhet med E underlagt Forsvarssjefen. Da forebyggende sikkerhetstjeneste og operativ sikkerhet tilligger FSA er de «…underlagt Nasjonal sikkerhetsmyndighet når det gjelder utøvelse av forebyggende sikkerhetstjeneste i Forsvaret etter sikkerhetsloven, herunder personellsikkerhet» (EOS-utvalget, u.å.-b). Avdelingen utfører store mengder klareringssaker[40] og deres oppgaver fremgår av instruks for sikkerhetstjeneste i Forsvaret § 4 (EOS-utvalget, u.å.-b).

4.3.4 NSM (Nasjonal sikkerhetsmyndighet)

NSM «…er Norges ekspertorgan for informasjons- og objektsikkerhet, og er det nasjonale fagmiljøet for IKT-sikkerhet. Direktoratet er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser» (Nasjonal sikkerhetsmyndighet, u.å.-b). NSM som er et sivilt direktorat har en todelt oppgave: de gir råd og veiledning i tillegg til å drive tilsyn (Nasjonal sikkerhetsmyndighet, u.å.-a). De rapporterer til Forsvarsdepartementet og Justis og Beredskapsdepartementet (JBD). Sikkerhetsloven og underliggende forskrifter som objektssikkerhetsforskriften med flere er sentrale.

4.3.5 UD (Utenriksdepartementet)

UD, med dens mange underliggende avdelinger, har som oppgave å fremme norske interesser utenfor landets grenser. Dette fremgår av utenrikstjenesteloven § 1 (2002). Det kan dreie seg om enkeltindividers eller bedrifters interesser i forbindelse med virksomhet utenlands. De mer enn hundre utenriksstasjonene kan gi næringslivet støtte i form av nettverksbygging og lokalkunnskap.

[40] Nærmere 20 000 klareringssaker i året (EOS-utvalget, u.å.-b).

4.3.6 NSR (Næringslivets sikkerhetsråd)

NSR «…er opprettet av næringslivets sentrale organisasjoner[41] med formål å bekjempe kriminalitet i og mot næringslivet» (Næringslivets sikkerhetsråd, u.å.-b). I oppgaven har jeg derfor beskrevet NSR som et rådgivende organ stiftet av næringslivet. NSR jobber aktivt for å bedre bedriftenes sikkerhet blant annet gjennom det konsultative rådet og flere ulike utvalg.

4.3.7 Næringslivskoordinator Kripos ved NSR

Næringslivskoordinator Kripos ved NSR ble opprettet som en prosjektstilling, men er nå gjort om til fast stilling ved Kripos. Stillingen ble opprettet for å søke å få et bedre samarbeid mellom politi og næringslivet. Koordinatoren har ukentlig kontorplass i NSRs lokaler. For å kunne henvise på en oversiktlig måte kalles denne informanten for informant fra Kripos i oppgaven.

4.3.8 Telenor Group og Telenor Norge AS

Telenor Group er et samlenavn på alle selskapene i Telenorgruppen. Telenor Norge AS (heretter kalt Telenor Norge) er et av selskapene og har virksomhet i Norge. Telenor Group styrer de andre selskapene som igjen har egne styrer og administrasjon. På Telenor Groups nettsider kan vi lese at «Telenor-konsernet er en av verdens ledende mobiloperatører med 186 millioner mobilabonnementer. Vi har mobilvirksomheter i 13 land i tillegg til en eierandel i VimpelCom Ltd. som har mobilvirksomheter i 14 land» (Telenor Group, u.å.).

[41] Bedriftsforbundet, Næringslivets hovedorganisasjon, Finans Norge, Virke, Arbeidsgiverforeningen Spekter, Norges Rederiforbund/Den Norske Krigsforsikring for Skip.

4.3.9 Statoil ASA

Statoil ASA (heretter benevnt Statoil) et internasjonalt norsk olje- og gasselskap med produksjon i mer enn 30 land. Energiselskapet er i dag en av verdens største leverandører av olje og gass (Statoil ASA, u.å.).

4.4 Oppgavens problemstillinger

I det følgende vil jeg nå gå gjennom de fire problemstillingene hver for seg.

4.4.1 Hvordan bedriver norske myndigheter sikkerhetsrådgivning overfor store norske bedrifter med virksomhet i utlandet, og på hvilke områder gis det slik rådgivning?

Min datainnsamling og analyse viser at norske myndigheter bedriver sikkerhetsrådgivning til store norske bedrifter med virksomhet i utlandet. Det må samtidig presiseres at denne sikkerhetsrådgivningen gis på ulike områder. Videre må den sies å være både av forebyggende karakter og knyttet til spesifikke saker. Sikkerhetsrådgivningen tar ulik form og er ikke av regelmessig og jevnlig karakter. Veiledningsmateriell er et eksempel på rådgivende informasjon.

Bedriftene benytter seg av åpent tilgjengelig veiledningsmateriale fra myndighetene. Informantene i Telenor Norge, Telenor Group og Statoil viser til at de benytter seg av rådgivende materiell. De tre informantene nevner alle rådgivende materiell fra PST tilgjengelig på nettet. Telenor Norge og Statoil viser spesifikt til PSTs årlige åpne trusselvurdering. I PSTs åpne trusselvurdering kan vi lese at «vurderingen er også ment for virksomheter som har behov for en oppdatert trusselvurdering som en del av sin langsiktige risikohåndtering» (Politiets sikkerhetstjeneste, 2015, s. 4). *En veiledning - Sikkerhets- og*

beredskapstiltak mot terrorhandlinger (Nasjonal sikkerhetsmyndighet et al., 2010) blir brukt av Statoil i en bearbeidet form. Telenor Norge nevner også åpne vurderinger fra E og NSM.

PST-informanten forteller at PST gir sikkerhetsråd for å forebygge terror/voldelig ekstremisme, etterretning og spredning av masseødeleggelsesvåpen eller kompetanse om dette. Kriminalitetsområder som faller i kategorien tilsiktede og ondsinnede hendelser (security). Dette gjøres med bakgrunn i politilovens § 17 og Instruks for Politiets sikkerhetstjeneste §§ 4, 5 og 6. Informanten i PST vektlegger betydningen av det å arbeide på lang sikt, herunder sikkerhetsrådgivning, for å ikke mislykkes i sitt forebyggende arbeid. Hvem PST gir råd til endres hele tiden ut fra trussel, prioriteringer, hendelser og andre faktorer som for eksempel medieoppmerksomhet. Slik jeg ser det kan dette forstås slik at sikkerhetsrådgivningen fra PST til bedriftene ikke er regulær. Samtidig kan det tyde på at en er tilpasningsdyktig i forhold til situasjonen og prioriterer ut fra de overnevnte punktene, noe som er positivt. En form for mellomting (hybrid) mellom de to formene jeg deler sikkerhetsrådgivning inn i: spor 1) som er forebyggende råd, og spor 2) som er spesifikke råd knyttet mot sak eller hendelser. Informanten fra PST forteller at St.meld. 21 - Terrorberedskap - behandler sikkerhetsrådgivning, og at man ønsker at PST skal gi sikkerhetsrådgivning til norske bedrifter i utlandet. Samtidig står det ikke hvem, det står ikke hvordan, det er ikke midler og PST må gjøre det innen budsjettet. Informanten fra PST forteller at de stort sett blir målt på det som skjer i Norge og at det blir en salderingspost.

Bedriftenes uttalelser i intervjuene støtter opp under at PST gir sikkerhetsråd til store norske bedrifter med virksomhet i utlandet. Telenor Group og Statoil viser til et samarbeid der det utveksles råd. Informanten fra Statoil uttaler at de mottar og har mottatt sikkerhetsrådgivning fra PST, samt at de har jevnlige møter. Informanten fra Telenor Group opplyser at de jobber direkte med PST, men av mer uformell karakter. Informanten fra PST sier at de har økt fokus på Telenor etter Muhammed-karikaturene, men kontakten er likefullt saksknyttet og ikke-regulær i følge uttalelsene fra informanten i Telenor Group. Han sier at det er ikke generelt en åpen dialog, men ved spesielle hendelser en direkte dialog. Ut fra dette fremstår derfor Statoils samarbeid med PST som mer formalisert og regelmessig sammenlignet med Telenor Groups samarbeid. Deres beskrivelser faller inn i det jeg har kalt sikkerhetsrådgivningens to spor: Statoil i forebyggende råd (1), og Telenor Group i spesifikke

råd knyttet til sak eller hendelser (2). Statoil får også informasjon knyttet til sak eller hendelser.

Informanten hos Telenor Norge opplyser å ikke få sikkerhetsrådgivning fra PST eller andre norske myndigheter. I følge han benytter de seg av informasjon fra utenriksstasjonene i utlandet, men det er informasjon de bearbeider til eget behov. Videre forteller han at de kan spørre norske myndigheter, for eksempel PST om bransjespesifikke trusselvurderinger forutsatt at PST har kapasitet. I tillegg benytter Telenor Norge seg av åpne vurderinger fra eksempelvis PST, E, NSM og Forsvarets forskningsinstitutt (FFI). Samlet sett mener jeg at dette faller inn under oppgavens definisjon av sikkerhetsrådgivning, og flere av vurderingene utgis jevnlig. Telenor Norge driver sin virksomhet i Norge, og visste seg å være utenfor målgruppen for denne oppgavens tema. Til tross for det kan uttalelsen tyde på at sikkerhetsrådgivning ikke bedrives i stor skala, utover det som ligger ute som åpen informasjon tilgjengelig for de som måtte ønske det. Den ulike oppfatningen hos de to informantene i Telenor, henholdsvis Telenor Norge og Telenor Group, kan tolkes på minst to måter. For det første at sikkerhetsrådgivningen er ulik for virksomhet i Norge og virksomhet i utlandet. Samtidig viser ulikheten i svarene at det i et og samme selskap kan råde ulike oppfatninger om sikkerhetsrådgivning, hva en legger i begrepet og benyttelsen av slik rådgivning. En omforent definisjon av sikkerhetsrådgivning ville derfor vært avklarende.

Som beskrevet i metodekapittelet har jeg ikke lykkes i å komme i kontakt med E, og henvendelsene mine dit er som nevnt blitt videresendt til FSA. Til tross for dette ønsker jeg å si noe om forholdet mellom E og bedrifter i lys av Helga Pedersens, tidligere statsråd og medlem i utenriks- og forsvarskomiteen, uttalelse om å få et godt utgangspunkt for bedrifters utenlandsvirksomhet. Gjennom åpne kilder har jeg funnet informasjon slik at jeg kan forsøke å si noe om denne relasjonen. Kjell Grandhagen, sjef for E-tjenesten, har uttalt følgende: «Vi gir våre vurderinger til norske myndigheter. Aldri råd om hva som skal gjøres, men faktainformasjon. Så er det opp til andre å benytte den informasjonen. Det har ikke vært vanlig til nå med kontakter mellom etterretningstjenesten og norsk næringsliv» (Veum & Olsson, 2013, s. 2)[42]. Slik kontakt er det opp til myndighetene om det skal bli, sier Grandhagen (Veum & Olsson, 2013). Her kan en stoppe opp ved bruken av ordet *vanlig*: Det

[42] Artikkelen er nummerert når den skrives ut, jeg angir sidetall med første side som nummer 1 (totalt fire sider).

at det ikke er vanlig med slik kontakt, kan tolkes dit hen at det kan og har vært slik kontakt, men at det ikke skjer ofte. Videre sier Grandhagen også at han ser at denne typen kontakt er et tema, og at E følger beslutningene som blir tatt (Veum & Olsson, 2013). Forsvarsminister Ine Eriksen Søreide (Høyre) har uttalt at «det er åpenbart at Etterretningstjenesten ikke kan gi ut all informasjon, fordi den er gradert. […] Dersom Etterretningstjenesten sitter på informasjon om at det er overhengende fare for liv eller helse mot norske interesser i utlandet, så har de en plikt til å varsle for eksempel en norsk bedrift umiddelbart og direkte og det gjøres også» (NRK, 2014). Dette var en uttalelse fra forsvarsministeren for å avkrefte en misforståelse fra departementsråden i forbindelse med informasjonsutveksling og fare for liv/helse. Det var uttalt at en kunne holde tilbake informasjon til tross for at det kunne medføre fare for tap av norske menneskeliv. Informasjon i denne «kategorien» vil etter stor sannsynlighet være security-relatert (tilsiktede handlinger). Dersom en setter terskelen for å varsle (eller å gi sikkerhetsråd) på et slikt nivå vil feiltolkninger av signal kunne få fatale konsekvenser. Varsel og signal kan i følge Agrell deles i flere kategorier hvor manglende varsel er en av dem (Agrell, 2005). Hendelsen finner da sted uten at det er fanget opp et varsel i forkant. Dette kan slik jeg forstår det bero både på at det ikke eksisterer noe varsel å fange opp, eller at en ikke forstår at det foreligger et varsel. Isolert sett fører de to forståelsene jeg legger til grunn til at det ikke blir videreformidlet informasjon eller gitt rådgivning. Overført til oppgaven blir det ikke gitt informasjon til bedriftene. Nyttig informasjon som myndigheter holder tilbake for bedriftene pga. sensitivitet (taushetsplikt/gradering/klausulert informasjon etc.) eller en ikke forstår at er av interesse for dem kommer inn i feltet *blindflekken* i Joharis vindu. I etterkant av hendelser vil det etter all sannsynlighet bli stilt spørsmål ved en slik tilbakeholdelse. Da under forutsetning at det fremkommer informasjon om at myndigheter hadde slik kunnskap i forkant av hendelsen. I etterkant av In Amenas undersøkte UD blant annet hvilke informasjon norske myndigheter (E, PST, UD og Ambassaden i Alger) hadde i forkant av hendelsen (Utenriksdepartementet, 2013, s. 34-35).

E var en av tjenestene det ble sett nærmere på i forbindelse med UDs evaluering av In Amenas:

> «E-tjenesten har analysert denne trusselen nærmere og formidlet sine vurderinger til blant annet Forsvarsdepartementet og Utenriksdepartementet, men da som gradert informasjon. Heller ikke i de graderte dokumentene fremkommer det imidlertid spesifikke trusler mot gassproduksjonsanlegget i In Amenas eller mot nordmenn eller norske interesser i Algerie forut for angrepet» (Utenriksdepartementet, 2013, s. 34).

Dette kan forståes slik at systemet med formidling av informasjon gjennom andre departement fungerer på en tilfredsstillende måte. Videre kan en spørre om dette egentlig er et problem dersom informasjonen når frem via andre? Flere kontaktflater betyr ikke nødvendigvis bedre informasjon. Via andre kan informasjon samordnes og en klarer kanskje i større grad å se det store (og riktige?) bildet. Med utgangspunkt i at andre vurderer hva som er viktig, er man naturligvis prisgitt deres vurderinger. Samtidig er rommet for oppfølgingsspørsmål til fagmiljøet, i dette eksempelet E, begrenset ved at informasjon eventuelt blir videreformidlet av og via andre. E vil kunne ha informasjon som de ikke vet/forstod er aktuell for bedrifter (kan plasseres i feltet det ukjente), samtidig som bedriftene ikke kjenner til at E har denne informasjonen tilgjengelig. Bedrifter kan igjen sitte på kunnskap som de ikke deler (fasaden) eksempelvis fordi de ikke ønsker å vise svakheter, pga. manglende kontaktpunkt, eller at bedriftene ikke er klar over at det er interessant (også) for andre. Kontakt kan påvirke forståelsen for om ulik type informasjon en innehar er vesentlig og nyttig, dette gjelder også informasjon som er åpent tilgjengelig (arenaen). Dette kan igjen relateres til risikoforståelse og risikoerkjennelse. Feltene i Joharis vindu er ikke mindre aktuell for de andre myndighetenes rådgivning overfor bedriftene. Grunnen til å skrive om dette tilknyttet til E er at jeg har lite informasjon om deres kontakt opp mot bedrifter og vinduets fire felter er derfor egnet til å problematisere relasjonen. De fire feltenes kjennetegn vil være gjeldende i større eller mindre grad, også der det er tettere og mer jevnlig kontakt og samarbeid. Det fremkom heller ikke opplysninger i UDs evaluering om at PST eller UD holdt tilbake informasjon som burde vært videreformidlet (Utenriksdepartementet, 2013).

Det fremgår av instruks om Etterretningstjenesten (2001) § 11 *Forebyggende varsling og rådgivning* at «Etter Forsvarsdepartementets nærmere bestemmelser og innenfor rammen av sikkerhetsloven § 12 kan tjenesten i forebyggende øyemed varsle og rådgi norske og utenlandske juridiske og fysiske personer om forhold som faller innenfor tjenestens oppgaver». Sammenfattet kan en forstå kildene slik at E kan gi sikkerhetsråd til store norske bedrifter med virksomhet i utlandet. Samtidig oppfatter jeg det slik at denne sikkerhetsrådgivningen ikke er kontinuerlig, men hendelsesstyrt og knyttet til eventuelle pågående trusler eller saker. Kapittelets innledningsvise uttalelser fra Helga Pedersen og Trond Giske tyder på at styresmaktene i etterkant av In Amenas er (eller i alle fall var) positiv til rådgivning og deling av informasjon knyttet til norske bedrifters virksomhet utenlands. Dersom myndighetene skal bidra med best mulige råd er det naturlig at myndighetene som har relevant informasjon deler dette (i en eller annen form). Kunnskap om internasjonal terrorisme, som er et av Es arbeidsområder, vil kunne være nyttig informasjon for bedrifter med virksomhet i utlandet.

Informanten hos Statoil etterspør informasjon fra E: «Vi ønsker jo en tettere dialog med forsvaret, og spesielt E-tjenesten, i forhold til at vi har mye internasjonal virksomhet og kunne tenke oss mer regulære møter og informasjon derfra.» Han forteller videre at de ikke har etablert noen god struktur eller deling av informasjon der. «Der er det jo egentlig lovverket som stopper oss, eller stopper de fra å levere oss den informasjonen som vi ønsker oss.» Det står i følge han litt på vent foreløpig. Statoil er i stor grad eid av den norske stat og er å regne som norske interesser, om det er i Norge eller internasjonalt. Statoil syns derfor at det er litt rart at de ikke i større grad kan få tilgang til informasjon som kan ha betydning for sikkerheten på deres installasjoner, anlegg og kontorsteder rundt om i verden. Statoil ønsker seg bedre informasjon for at de skal kunne ivareta sikkerheten på best mulig måte. Norske myndigheter, spesielt forsvaret og E-tjenesten, sitter i følge informanten i Statoil på masse informasjon som de ikke får tilgang til. Han tror at Statoil kunne vært i bedre stand til å beskytte sine interesser og norske interesser dersom de fikk mer informasjon, og det er slik et stort rom for forbedring etter deres syn. Informanten er tydelig på Statoils ønske om et tett og regelmessig samarbeid, med god informasjonsflyt.

Informanten hos Telenor Group etterspør mer informasjon direkte fra fagmiljøene, og slik jeg forstår det er PST og E to av de aktuelle fagmiljøene. Informanten ønsker informasjon

som er konkret og operativ, ikke det han kaller vasket gjennom byråkratiet. Uttalelsene fra de to informantene, Statoil og Telenor Group, og informasjonene for øvrig tyder som nevnt på at sikkerhetsrådgivning fra E i alle fall ikke bedrives i noen stor skala. Det kan derfor antas at sikkerhetsrådgivning fra E til bedrifter er av uregelmessig karakter og hovedsakelig knyttet til spesifikke pågående saker, det jeg kaller spor to i definisjonen.

FSA bedriver ikke sikkerhetsrådgivning direkte til norsk næringsliv med virksomhet i utlandet. Informanten fra FSA er klar på at det er UD som gir sikkerhetsråd til norsk næringsliv i utlandet. Det er ikke noe i mitt datamateriale som tilsier at FSA gir sikkerhetsråd. Mine data viser derimot at sikkerhetsrådgivningen utøves av flere myndigheter. UD er en tung aktør, men de er ikke alene om å bedrive slik sikkerhetsrådgivning.

NSM gir sikkerhetsråd til bedrifter med virksomhet i utlandet og det er i følge informanten i NSM en økende aktivitet. Han uttaler at «Hovedgrunnen til at man driver rådgivning er kort og godt at det er et særdeles viktig tiltak for å forbedre sikkerhetstilstanden i samfunnet». NSM er pålagt dette gjennom lovverket, sikkerhetsloven med påfølgende forskrifter. NSM snakker sjelden om trusler, dette fordi de ikke er trusselaktørfokusert. Det er i følge informanten i NSM PST sin oppgave. NSM snakker om sårbarheter og risiko. Det er et viktig skille for oss. Det betyr ikke at NSM ikke kommer inn på trusselaktører og den type ting, da de må danne et bakgrunnsteppe for hvorfor en må gjøre enkelte ting. NSMs hovedfokus er i følge informanten sårbarhetene som eksisterer og tiltak for å redusere risiko knyttet til sårbarhetene. De fins i den fysiske verden og i den digitale verden. Ved å redusere sårbarheten gjør bedriftene seg bedre i stand til å håndtere en potensiell trussel.

I følge informanten i UD tar bedrifter hjemme også kontakt med ambassader for å få råd om etablering i andre land og informasjon om sikkerhetssituasjonen der. I utgangspunktet er det bedriftene som tar kontakt med UD for å få informasjon, ved mer spesielle hendelser kan det være motsatt. Ambassadene er knutepunkt og de har regulær kontakt med bedriftene som er tilstede i området. En del av kontakten, særlig i utsatte land, er rådgivning på sikkerhetsspørsmål og slik en helt naturlig og integrert del av kontakten. Dette sammenfaller med denne setningen hentet fra UDs evalueringsrapport: «Utenriksdepartementet og utenriksstasjonene arbeider løpende for å få et best mulig bilde av sikkerhetsutfordringene der norske interesser er representert» (Utenriksdepartementet, 2013). I forbindelse med

Sikkerhetsforum for norske internasjonale virksomheter (frokostmøte), arrangert av NSR 10. mars 2015, kunne vi lese at «Petter Ølberg, ekspedisjonssjef i Utenriksdepartementet så også behovet for et nettverk for informasjonsflyt og samarbeid mellom norske virksomheter og ambassadene lokalt» (Simonsen, 2015b). Dette bygger også oppunder at ambassadene har en viktig posisjon i kontakten mellom UD og bedriftene som har virksomhet i utlandet.

Det fokuseres på alle typer trusler avhengig av landet en er i, kriminalitet, terror, væpnede konflikter m.m. og sikkerhetsvurderingene som gjøres rapporteres i følge informanten hjem til UD. Dette er områder som faller i kategorien security og stemmer dermed overens med oppgavens definisjon. UD gir, i følge informanten fra Seksjon for sikkerhet og beredskap i UD, to typer sikkerhetsråd. Det ene er det UD gjør i en konsulær setting, som går ut på å løpende gi reiseråd til nordmenn (særlig turister) i utlandet. Det er faste prosedyrer for disse rådene – som mye er basert på den informasjonen UD får fra utenriksstasjonene. Dette går på alt fra å vise forsiktighet - til å fraråde å reise dit. Den andre typen «rådgivning» er informasjon som på anmodning gis til norske bedrifter i utlandet. I UD er de i følge informanten veldig forsiktig med å gi konkrete råd til hva bedriftene bør/skal gjøre. De enkelte tiltakene som innføres, og risikovurderingen basert på egen virksomhet og forutsetninger må bedriftene gjøre selv. Det UD kan bidra med det er å gi faktaopplysninger om den delen av verden hvor de har utvidet kunnskap. Han presiserer med å si at «vi verken kan juridisk sett eller vil være en rådgiver når det gjelder hvilke konkrete tiltak den enkelte bedrift skal/bør iverksette». Informanten presiserer at UD prinsipielt ikke utfører sikkerhetsrådgivning for privat næringsliv. Det nærmeste man kommer til rådgivning i denne sammenheng er utarbeidelse av offisielle reiseråd (landsider.no).

Uttalelsene om utøvelse av sikkerhetsrådgivning fra informanten i UD og informanten i Seksjon for sikkerhet og beredskap kan forståes å ikke være helt samsvarende. Den ulike oppfatningen er et funn som jeg tidligere i oppgaven har beskrevet hos Telenor, og kan også tas til inntekt for at sikkerhetsrådgivning er et uklart begrep. Det gis informasjon som bedriftene kan benytte i sine vurderinger, men slik jeg forstår det gis det ikke konkrete råd om hva man eksakt skal gjøre. Videre sier informanten i Seksjon for sikkerhet og beredskap at den enkelte bedrift er lovpålagt å utføre intern kartlegging av egne sikkerhetsutfordringer - enten ved bruk av egne ressurser eller ved hjelp av kommersielt tilgjengelige aktører/ressurser – slik at de er i stand til å vurdere/akseptere aktuell risiko ut fra egne

premisser. Avslutningsvis i sin redegjørelse om terrorangrepet i Algerie sa statsminister Stoltenberg 23. januar 2013 (sak nr. 3) at «Det er norske bedrifter som til syvende og sist må ta ansvaret for de prosjekter, investeringer og beslutninger de gjør ute, men de skal få den veiledning og bistand fra norske myndigheter som vi er i stand til å gi dem». Dette er sammenfallende med informantens poengtering av ansvaret som tilligger bedriftene. I følge informanten kan UD i denne forbindelse bidra med å gi et best mulig faktagrunnlag for situasjonen i de enkelte embetsdistrikt. Man kan også til en viss grad informere om hvilke vurderinger som er gjort og hvilke tiltak som er iverksatt for egne ansatte i henhold til kravene i arbeidsmiljøloven og internkontrollforskriften. Det han kaller to «spor»: ett for egen virksomhet, og ett for andre bedrifter. Dette må ikke forveksles med oppgavens definisjon av sikkerhetsrådgivning og dens to spor. Informasjon og fakta om ulike områder som kan brukes til risikovurderinger mener jeg det er riktig å karakterisere som sikkerhetsrådgivning og faller innfor definisjonen av sikkerhetsrådgivning som benyttes i oppgaven. Det gis for at bedriftene skal ha bedre områdekunnskap og beslutningsgrunnlag for sine egne vurderinger. Informantene i Statoil og Telenor Group forteller at de har kontakt med UD.

«NSR gir råd om sikkerhetstiltak mot industrispionasje, sabotasje, narkotika, ran, terrorisme, organisert kriminalitet, bedragerier, utpressing, korrupsjon, datakriminalitet ol. NSRs konsultative råd bistår i trusselvurderinger og utarbeidelse av tiltak mot kriminelle handlinger rettet mot næringslivet» (Næringslivets sikkerhetsråd, u.å.-b). Informanten i NSR fortalte at deres oppgave er å forebygge kriminalitet i og mot næringslivet. I tillegg til å være et toveis kontaktpunkt mellom myndighetene og næringslivet. I følge informanten er det viktig å ikke glemme den generelle kriminaliteten, korrupsjon osv. som er et problem i enkelte land, ikke bare terrorisme. Det er som han sier flere typer tilsiktede ondsinnede hendelser. NSR formidler trender, advarsler, og regulatoriske endringer innenfor det mandatet NSR har - fra myndighetene til næringslivet. Samt kommuniserer de utfordringene næringslivet har til myndighetene. NSR forsøker å finne løsninger sammen med myndighetene for å kunne forebygge. NSR har et bredt sammensatt konsultativt råd bestående av faste og konsultative medlemmer. Det konsultative rådet bedriver sikkerhetsrådgivning, og dette beskrives mer inngående under neste punkt i oppgaven.

Informanten forteller at NSR skal være et *single point of contact* hvis ønskelig: «det vi som er ansatte her ikke kan svare på selv, skal vi på en måte forsøke å vite hvem som kan svare på til enhver tid. Altså peke dem i riktig retning.» Ved noen tilfeller stiller NSR spørsmål til myndighetene på vegne av virksomheter. NSRs gir sikkerhetsråd til medlemsbedriftene. Denne rådgivningen må kunne kategoriseres som å være av regelmessig karakter gjennom dets utvalg, det konsultative rådet, utsendelse av nyhetsbrev og oppdatert informasjon på deres nettsider. Bedrifter kan også selv ta kontakt dersom det er behov for det. Begge de to sporene i definisjonen kan dermed sies å være dekket. Petter Haas Brubakk (NHOs[43] direktør for næringspolitikk) sa i forbindelse med sikkerhetsforumet, arrangert av NSR 10. mars 2015, at de setter pris på NSRs fokus på sikkerhet og samarbeid med tanke på den økende norske internasjonale virksomheten (Simonsen, 2015b). Dette tyder slik jeg ser det på at NSR har en viktig rolle ovenfor norsk næringsliv med internasjonal aktivitet.

Informanten i Kripos (næringslivskoordinator ved NSR) mener at PST og NSM driver systematisk med sikkerhetsrådgivning. De er regulert i lov. Det mener informanten også at politiet er gjennom politiloven, §§ 1 og 2 i forhold til ansvar og mål. Ikke minst under oppgaver (§ 2): beskytte og verne om/forebygge. «Samtidig så er vi ikke flinke nok på det, vi har ikke et system på det. Inn i Kripos så har man en strategi i forhold til forebygging og partnerskap og samarbeid. Men det er ikke formalisert og det er ikke strukturert. Sånn at den rådgivningen vi gir til bedrifter, og det kan være både innenlands og utenlands, er jo at vi ofte på konsernnivå eller sikkerhetsaspektet går inn og tegner et bilde av eller forteller om trusselen, altså hva er det vi ser. Hva er det store bilde, for det er jo det Kripos gjør.» En gang i året gir Kripos ut en rapport i forhold til organisert og annen alvorlig kriminalitet på områder Kripos monitorerer. Dette er slik jeg oppfatter det informasjon bedriftene kan bruke som grunnlag og/eller deler av grunnlaget for sine egne vurderinger og det faller inn under oppgavens definisjon av sikkerhetsrådgivning.

Informanten i Statoil fortalte at de i tillegg til sikkerhetsrådgivningen fra myndighetene har avtaler med eksterne kommersielle selskaper. Derfra kjøper de informasjon knyttet til trusselvurderinger, landinformasjon, informasjon om hva som skjer. I Bergens tidende kan vi lese at Statoil i etterkant av 22. juli benyttet Forsvarsbygg for å undersøke sikkerheten ved Statoils anlegg i Norge (Strand, 2013, s. 4). Dette er også omtalt i In Amenas-rapporten

[43] Næringslivets Hovedorganisasjon

(Statoil ASA, 2013b, s. 53). Forsvarsbygg ble også benyttet av Statoil i forbindelse med In Amenas, noe som fremgår av Forsvarsbygg årsrapport 2013 (Forsvarsbygg, 2014). «Forsvarsbygg er et forvaltningsorgan underlagt Forsvarsdepartementet, har Forsvaret som største og viktigste kunde, men har også kunder i andre offentlige markeder» (Forsvarsbygg, u.å.-b). Nasjonalt kompetansesenter for sikring av bygg som er en del av Forsvarsbygg tilbyr tjenester til statlig og privat virksomhet. Sikring av bygg og rådgivning knyttet til dette er et eksempel på en tjeneste de tilbyr (Forsvarsbygg, 2014). Forsvarsbygg er slik et eksempel på en både statlig og delvis kommersiell aktør innen sikkerhetsrådgivning.

Informanten fra Telenor Group opplyser at de nok er en stor kjøper av rådgivertjenester om trusselbildet og tiltak fra eksterne selskap, de store klassiske firmaene det være seg norske og utenlandske. Telenor Group får rådgivning i forhold til generelle terrortrusler og trusler mot nordmenn fra myndighetene. Når det gjelder andre typer trusler som kriminalitet, organisert kriminalitet, gatekriminalitet, og andre «sånne» ting får de i følge informanten mye gjennom de eksterne byråene. De eksterne byråene har mer fokus også på dette: hva byen er utsatt for, hvilke deler av landet er utsatt for hva? Fra norske myndigheter er det mer det store terrorbildet det det «går i». Når Telenor Group gjør vurderinger utenlands bruker de i følge han tre pilarer: egeninformasjon samlet inn lokalt, det de får fra norske myndigheter, og de sivile sikkerhetsselskapene ute. Informanten i UD nevnte også at selskaper kjøper inn sikkerhetsinformasjon fra private sikkerhetsselskaper.

Det overnevnte viser at bedriftene søker informasjon/rådgivning fra flere steder. Dette kan bety at norske myndigheter ikke har og/eller formidler tilstrekkelig informasjon. Det kan bety at regelverk (gradert og taushetsbelagt informasjon) vanskeliggjør utveksling av informasjon. En mer «positiv» forståelse er at store norske internasjonale selskaper søker best mulig kunnskap om områdene de opererer i og at kommersielle selskaper er en av flere bidragsytere innen sikkerhetsrådgivning. Det informanten i Telenor Group kaller en av flere informasjonspilarer. En oppfatning av at kommersielle private firma har større kompetanse enn det offentlige (Stensvand, 2013) kan også være en av flere forklaringer på kjøp av slike tjenester. Et privat firma kan kanskje i større grad enn norske myndigheter innhente spesifikk og tilpasset informasjon da de utfører tjenester de får betalt for, og ikke skal hjelpe «alle» slik utgangspunktet er for norske myndigheter. I et slikt lys vil denne typen tjenester etterspørres nær sagt uansett hvor mye informasjon norske myndigheter formidler til

bedriftene. Innhenting av informasjon kan ses på som *en kunnskapskamp* (Dean et al., 2010) mot aktuelle trusler, der bedriftene ønsker et best mulig utgangspunkt for sine vurderinger for å forebygge og beskytte seg best mulig mot ondsinnede aktører. Myndighetenes informasjonsutveksling og sikkerhetsrådgivning bidrar til dette, i tillegg til bedriftenes egenkunnskap og kommersielt kjøpte tjenester. Den nevnte kunnskapskampen er i utgangspunktet knyttet til politiets kriminalitetsbekjempelse. Overført til bedriftene er *targeted policing* målet: bedriftene innehar da den beste kunnskapen og er i forkant av potensielle trusler. Det fremstår som at informantene bruker flere kanaler for å kunne forstå og innrette seg best mulig i forhold til det til enhver tid eksisterende trusselbilde. Dette er sammenfallende med følgende uttalelse fra konserndirektør Jannicke Hilland i Statoil: «vi har styrket organisasjonen vår med en egen sikringsavdeling, som har som oppgave å samle informasjon fra ulike kilder…» (Aadland, 2014, s. 2)[44].

Rådgivende materiell benyttes av bedriftene som del av grunnlaget for deres egne vurderinger og faller inn i det forebyggende sporet i definisjonen (spor 1). Denne typen veiledningsmateriale er i en del tilfeller av (mer eller mindre) årlig karakter og dermed regelmessig, eksempelvis Es Fokus-rapporter og PSTs årlige åpne trusselvurderinger.

Informasjon som bedriftene selv kan bearbeide og knytte til sine bedriftsspesifikke risikovurderinger faller inn under begrepet sikkerhetsrådgivning. Dette er som det fremgår ovenfor en type sikkerhetsrådgivning som norske bedrifter med virksomhet i utlandet bedriftene nyttiggjør seg av.

4.4.1.1 Vertslandets ansvar

I denne oppgaven er det norske myndigheters sikkerhetsrådgivning overfor store norske bedrifter med virksomhet i utlandet som undersøkes. Det er likevel nødvendig å si noe om vertslandets rolle. Dette fordi sikkerheten til bedriftene og deres ansatte ivaretas fra flere hold.

[44] Elektronisk og unummerert artikkel. Jeg angir sidetall med første side som side nummer 1.

Det er myndighetene i landet hvor krisen oppstår som har ansvaret for å håndtere denne (Meld. St. 12 (2010-2011), 2011, s. 36). På lik linje er det vertslandet som er ansvarlig for sikkerheten for de som befinner seg på landets territorium (Utenriksdepartementet, 2013, s. 6). «Det er følgelig vertslandet som er ansvarlig for å treffe tiltak for å forebygge terrorisme og for å redusere skadevirkningene dersom terrorhandlinger finner sted» (Utenriksdepartementet, 2013, s. 6). I In Amenas var sikkerheten basert på prinsippet om lagdelt beskyttelse (Statoil ASA, 2013b, s. 44)[45]. Den ytre sikkerheten forstått som beskyttelsen utenfor In Amenas-anlegget skulle ivaretas av algeriske styresmakter, den indre sikkerheten på selve anlegget av private sikkerhetsselskaper. In Amenas-rapporten viser til at joint venture-samarbeidet hadde stor tiltro til algeriske myndigheters håndteringsevne. Denne tiltroen svekket egen forestillingsevne og scenarioplanlegging for situasjoner der den ytre beskyttelsen ikke ville virke hensiktsmessig (Statoil ASA, 2013b, s. 70).

Sikkerheten til store norske bedrifter med virksomhet i utlandet kan sies å ivaretas av flere aktører. For det første ansvaret som tilligger vertslandets myndigheter. Videre har norske bedrifter ansvar for sine ansattes sikkerhet som beskrevet i arbeidsmiljøloven og internkontrollforskriften. For det tredje kan bedriftene få sikkerhetsråd fra norske myndigheter. Eksempelvis fra norske sikkerhetstjenester, og UD som blant annet har som oppgave å fremme norske interesser utenlands. Informasjon fra fagmiljøene (PST og E) er etterspurt av bedriftene jeg har intervjuet og viser at bedriftene anser informasjon fra dem som betydningsfull. Til sist kan bedriftene kjøpe flere former for kommersielle tjenester fra ulike sikkerhetsselskaper. Dette er tjenester som informantene opplyser at de benytter seg av. Informantene er ikke spurt om deres kontakt opp mot vertslandets myndigheter da dette ligger utenfor oppgavens fokus.

Bedriftenes hensikt er å tjene penger til sine aksjonærer og en kan spørre om det er riktig ressursbruk om staten (den norske) skal påta seg mer ansvar overfor dem. Det er i oppgaven henvist til at norske myndigheter i etterkant av In Amenas ønsker å undersøke hvordan de ytterligere kan bistå bedriftene som opererer utenlands. Dette kan forståes slik at norske myndigheter ønsker å bidra til bedriftenes sikkerhetsarbeid og at det av myndighetene oppfattes som en del av deres oppgaver og ansvar. En avklaring av til hvem og hvordan

[45] Ytre beskyttelse (outer security): 1) grensebeskyttelse, 2) en militær sone, og 3) områdebeskyttelse. Indre beskyttelse (inner security): 4) perimetersikring og vakter.

sikkerhetsrådgivning skal bedrives av norske myndigheter er både i myndigheters og bedrifters interesse, også innenfor eksisterende rammer. Samtidig må det presiseres at det er bedriftenes ansvar å ivareta sine ansattes sikkerhet sammen med vertslandet. Forhenværende statsminister Stoltenberg har som nevnt uttalt at «… [bedriftene] skal få den veiledning og bistand fra norske myndigheter som vi er i stand til å gi dem» (redegjørelse i stortinget 23. januar 2013, sak nr. 3). Dette er sammenfallende med at norske myndigheter har et ansvar. Under anbefalingene i In Amenas-rapporten kan vi lese (punkt 12): bygge effektive relasjoner med vertslandene for å støtte felles forståelse, felles planlegging og trening. Samt at Statoil må avklare forventninger med regjeringer, vedrørende beskyttelse og støtte av kritisk nasjonal infrastruktur, og deres holdning og ressurser i en beredskapssituasjon (Statoil ASA, 2013b, s. 78). Det var bare en begrenset informasjonsutveksling mellom joint venture-samarbeidet og den algeriske hæren (Statoil ASA, 2013b, s. 70). Videre mener rapportens granskningsteam at en privat bedrift ikke kan forvente å få kjennskap til hemmelig (gradert) informasjon vedrørende militær kapasitet eller nasjonal sikkerhet (Statoil ASA, 2013b, s. 70). Det at slik informasjon ikke videreformidles kommer inn under feltet blindflekken i Joharis vindu (figur 2 – kapittel 2). Sammenfattet med anbefalingen nevnt over (punkt 12) kan dette tyde på at informasjonsflyt og dialog mellom Statoil og algeriske myndigheter kunne vært bedre.

4.4.2 I hvilken grad er det kontakt mellom aktørene og hvorfor samarbeider de, hvilken type kontakt har de, og hvor hyppig er denne kontakten?

Min studie og analyse viser at det er kontakt mellom myndigheter og bedrifter, men kontakten er av varierende type og karakter, kan muligens være personavhengig og er ikke nødvendigvis knyttet til funksjon. Bedriftene jeg har snakket med ønsker mest mulig informasjon slik at grunnlaget for å gjøre egne vurderinger er best mulig, mens myndighetene utfører (lov-)pålagte oppgaver og oppgaver som faller inn under deres arbeidsfelt (beskrevet under punktet over). Her har jeg under forrige punkt skrevet om ønsket om mer informasjon fra E og direkte kontakt med fagmiljøene. Kontakten mellom aktørene varierer fra å være direkte (eksempelvis én til én) til ulike typer åpen og

upersonlige informasjon, samt fora med flere til stede (eksempelvis NSRs konsultative råd). Kontakten virker å være uregelmessig, uten å kunne fastslå hyppigheten i kontakten nærmere. Når det er sagt kan «engangs» forebyggende råd være svært verdifullt.

Gradering og taushetsbelagt informasjon er trukket frem av myndighetsinformantene som en utfordring ved informasjonsdeling dem i mellom og ut til bedriftene. Wermdalen og Nilsson (2013) er av den oppfatning at det var manglende informasjonsutveksling mellom myndighetene knyttet til 22. juli i likhet med 11. september i New York. I NSRs konsultative råd er dette *løst* ved at medlemmene er sikkerhetsklarert. Løst betyr da at gradering ikke er et problem så fremt informasjonen ikke krever strengere klarering enn det medlemmene innehar (hemmelig). Det at bedrifter ikke er underlagt sikkerhetsloven kan gi tilsvarende forbud mot å dele informasjon. Dette betyr at myndighetene har informasjon de ikke kan dele selv om de skulle se behovet for det og ønsker å dele dette (blindflekken).

Sikkerhetsrådgivning kan utveksles på flere ulike måter, personlig og mer upersonlig. Norske myndigheters sikkerhetsrådgivning til store norske bedrifter med virksomhet i utlandet gjøres på flere ulike måter. Det kan være direkte fra myndighet til bedrift (én til én), fra myndighet til flere bedrifter samtidig (én til flere), eller én til alle (uttalelser i medier, åpent tilgjengelig informasjonsmateriale eksempelvis i form av nyhetsbrev og nettsider). Det gjøres også ved å formidle informasjon gjennom andre myndigheter. De ulike måtene å gi sikkerhetsråd på krever derfor større eller mindre grad av ressurser fra den rådgivende myndigheten.

PST gir i følge informanten i PST sikkerhetsråd på flere ulike måter: Én til én direkte til bedrifter, én til flere gjennom ulike utvalg og én til alle gjennom veiledere og aktuell informasjon på PSTs hjemmesider. PST gir ut årlige åpne trusselvurderinger (2012, 2013, 2014, 2015) med informasjon om aktuelt trusselbilde og utvikling og «politiets sikkerhetstjeneste utarbeider egne trusselvurderinger på grunnlag av innspill både fra E-tjenesten og andre kilder» (Utenriksdepartementet, 2013, s. 34). Da UDs evaluering heller ikke avdekket at PST hadde informasjon Statoil og/eller UD burde fått tilgang til, kan det tolkes dit hen at de i likhet med E har vurdert og håndtert informasjonen på en tilfredsstillende måte. PST har også gitt ut *En veiledning – Sikkerhets- og beredskapstiltak mot terrorhandlinger* (2010) i samarbeid med Nasjonal sikkerhetsmyndighet (NSM) og

Politidirektoratet (POD). Avslutningsvis har veilederen anbefalinger om relevant tilleggslitteratur. Slike samarbeidsprodukt kan øke forståelsen for hverandres arbeid og bedre kontakten dem i mellom, samt være mer helhetlige enn om bare en myndighet hadde forfattet den. Veilederen er ugradert og kan hjelpe virksomheter til å bli i stand til å håndtere ekstraordinære situasjoner. Det vil si forhold som ikke blir ordnet gjennom grunnsikringen. Denne veilederen er tilgjengelig og kan lastes ned av alle som har internettilgang. Veilederen er i følge informanten fra PST i forhold til terror og den gir en god metodikk for bekjempelse av kriminalitet. Informanten i Statoil fortalte at de bruker en bearbeidet utgave av denne veilederen. PST har i følge informanten i PST ikke mulighet til å gi pålegg, men de kan gi råd. Han syns dette er litt dårlig, samtidig som det også har en positiv side. PST er ikke en tilsynsmyndighet og har ikke noe ris bak speilet. De blir slik litt ufarliggjort og det kan gjøre det lettere å høre på de som rådgivere. Dette er sammenfallende med at NSM skilte rådgivnings- og tilsynsfunksjonen i deres organisasjon. Dette ble gjort nettopp for å ufarliggjøre det å ta kontakt med dem for å få rådgivning. PST skriver også artikler og produserer blogginnlegg på pst.no.

I PST er det i følge informanten i PST mange som gir sikkerhetsråd. Det fremgår i følge han av navnet sikkerhetstjeneste, og det er naturlig at de snakker om sikkerhet når de prater med folk i ulike sammenhenger. Dette gjøres på veldig mange måter innenfor forskjellige fagfelt: én til én, én til flere og én til alle. Sikkerhetsråd gis til de PST mener faller innfor sitt mandat. Én til flere er f.eks. til NSR. Fora som Kontaktgruppe for forebygging av terrorhandlinger et annet eksempel. Denne gruppen ble opprettet av Justisdepartementet i 2005 og ledes av PST. Det er mange offentlige og noen private aktører i gruppen, blant annet er NSR medlem. E-tjenesten er der, DSB, Statnett, Luftfartstilsynet og flere andre. Én til én er en svært ressurskrevende arbeidsmetode. Da får man personlig kontakt og det er en av måtene informanten i PST opplyser at de arbeider på. I de sammenhengende PST er i kontakt med andre, kommer de med råd. Alle har ikke like mye kompetanse på det og bakgrunn for å gi råd, men sier det ut fra sin oppgave og sitt ståsted. PST har enkelte som er spesialister og har tittelen sikkerhetsrådgivere. Når de som f.eks. har kontraetterretning som sitt ansvar, har møter med departement eller andre tar de i følge informantene med seg en sikkerhetsrådgiver i møtet. Dette for å få med denne dimensjonen. PST har fora, faste møter, og mer løselige møter, eller det dukker opp noe. In Amenas-hendelsen aktualiserte

eksempelvis sikkerhetsrådgivning. PST jobber både hendelsesstyrt og har kontinuerlig arbeid opp mot risikoområder. I det konsultative rådet i NSR er det PSTs oppgave er å informere om trusselbildet, og PST ønsker å selge inn Norsk Standard. I følge informanten en veldig fin arena hvor PST også får mye informasjon. PST har en representant i NSRs konsultative råd.

Es kontakt med bedrifter er det vanskelig å si noe detaljert om. Informasjon kan slik jeg forstår de åpne kildene gis, og da antar jeg at det utføres én til én mellom E og bedrift. Samtidig kan E gi gradert informasjon til Forsvarsdepartementet og UD, og PST kan få «…innspill fra både E og andre kilder» i forhold til sine trusselvurderinger (Utenriksdepartementet, 2013, s. 34). Terrorisme og fremmed etterretning (tilsiktede handlinger) er to av Es og PSTs prioriterte områder opplistet i deres samarbeidsinstruks (Instruks om samarbeidet mellom E og PST, 2006, § 3)[46]. Informasjon kan gis til andre norske myndigheter som kan videreformidle informasjon i en annen og gjerne ugradert («avgradert») versjon.

Informantene i PST og informanten i UD har uttalt at de samarbeider med E. Informanten fra FSA forteller at personellet ved norske ambassader er autorisert og sikkerhetsklarert. Samarbeid mellom militær og sivil side er i følge han selvfølgelig, og informasjon deles mellom militær og sivil side dersom det dreier seg om en trussel rettet mot ambassaden. Når norske myndighetspersoner reiser eller besøker konfliktområder i utlandet har PST og UD ansvar overfor sivilt personell, FSA ansvaret for militært personell. E og FSA er ikke representert i NSRs konsultative råd. Dersom det blir endringer i kontakten mellom E og næringslivet, som omtalt tidligere i kapittelet, kan kanskje NSR og dets konsultative råd bli en aktuell arena også for E? Det er all grunn til å tro at næringslivet ville satt pris på en slik deltagelse.

I følge informanten i NSM har de tradisjonelt vært en organisasjon som ene og alene har forholdt seg til virksomhetene som har vært underlagt sikkerhetsloven. Dette er det endret på. NSM henvender seg i større og større grad generelt, primært på virksomhetsnivå, men også helt ned til mannen i gaten. NSM gjorde et større tiltak for to år siden. Dette ved å skille ut tilsynsvirksomheten deres i en egen enhet, og etablere flere mindre enheter innenfor fagmiljøene som driver ene og alene med råd og veiledning. Det skal som informanten i NSM

[46] Samt spredning av MØV og viktige norske interesser.

sier være mulig å ta kontakt med NSM og stille spørsmål som gjennom spørsmålstillingen tilsier at sikkerhetstilstanden ikke er like god, men det skal ikke direkte medføre et tilsyn fra NSM. På teknisk side har NSM en egen seksjon som heter Råd og veiledning, de skal utarbeide veiledningene og gi aktiv rådgivning innenfor teknologiske spørsmål. På operativ avdeling, som også er en høyteknologisk avdeling i NSM, har de også en avdeling som heter Informasjonsdeling. Selv om den kalles noe annet ligger det i følge informanten betydelig sikkerhetsrådgivning og veiledning i forhold til en rekke ting der. I Rapport om sikkerhetstilstanden, en årlig rapport utgitt av NSM, gjør NSM opp status i deres syn på sikkerhetstilstanden i samfunnet og kommer med en rekke forslag til tiltak. Det siste informanten nevnte er en rekke arrangementer der NSM kommer i kontakt med dem de ønsker å nå. Ulike arrangementer, regionale seminarer i de største norske byene. For både å etablere en dialog, gi råd, og ikke minst gjøre det mulig for de som møter å stille spørsmål og møte fagfolk. NSM holder foredrag, og arrangerte i 2014 for første gang topplederseminaret. NSM kan ikke, nettopp pga. loven, dele sikkerhetsgradert informasjon med myndigheter eller personer som ikke er autorisert for denne typen informasjon. Før var omtrent alt NSM gjorde og sa gradert, men de er i følge informanten over tid blitt flinkere til å skille disse tingene. NSMs Rapport om sikkerhetstilstanden var tidligere gradert. Nå eksisterer den i to versjoner, en gradert til de som er autorisert og en ugradert versjon som kan gis til alle. NSM har gitt ut flere veiledninger som er tilgjengelig på deres nettsider knyttet til deres arbeidsfelt, deriblant Veiledning i verdivurdering (Nasjonal sikkerhetsmyndighet, 2009) og Veiledning i sikkerhetsadministrasjon (Nasjonal sikkerhetsmyndighet, 2010). Hensikten med de ulike veilederne er å få bedriftene til å identifisere skjermingsverdige verdier og objekter i henhold til sikkerhetsloven og sikre disse best mulig. Veilederne som ligger åpent tilgjengelig på nettet kan brukes av bedrifter som ikke er underlagt sikkerhetsloven.

Den konkrete sikkerhetsrådgivningen til næringslivet er det i følge informanten i UD Seksjon for sikkerhet og beredskap som står for. Næringslivsseksjonen har ansvaret for UDs arbeid med næringslivet. Det er mange seksjoner som er involvert i arbeidet og i tillegg hele uteapparatet, i overkant av hundre ambassader. De står for mye av kontakten med lokalt norsk næringsliv ute i de ulike embetsdistriktene. Videre forteller han at UD har ansvar for norske borgere og norsk virksomhet i utlandet. Både sikre norske borgere og fremme norsk næringsliv. Dette går hånd i hånd, ved at en både skal hjelpe næringslivet med å etablere seg

ute og da er sikkerhetsdelen en del av det bildet de må forholde seg til. UD har i følge utenriksloven og politiske prioriteringer plikt og fokus på å hjelpe næringslivet. Dette sammenfaller med at informanten fra Næringslivsseksjonen i UD opplyste at Næringslivsseksjonen er kontaktpunkt i UD for næringsliv som driver internasjonalt[47]. I følge han er de en «postboks» som næringslivet kan ringe til, samt at de kan formidle kontakter til fagseksjoner på huset. Sammen med fagseksjonene har Næringslivsseksjonen møter med de større selskapene, eksempelvis Statoil, Telenor, DNVGL[48] og Yara. Næringslivsseksjonen har møter med NSR. Det viktigste er hva utenriksstasjonene gjør på det enkelte sted. Det er forventet at det er en god dialog mellom norske selskaper og stasjonene. Informantene i Statoil og Telenor Group viser begge til UD og viktigheten av denne kontakten, både nasjonalt og på utenriksstasjonene rundt om i verden.

Informanten ved NSR og informanten i Kripos påpeker begge viktigheten av at kontakten bedrift-myndighet må være funksjons- og ikke personavhengig. En spesielt interessant kommentar fra informanten fra Kripos er: *«…det er sinnssykt viktig å få på plass, fordi at forsvinner personen så forsvinner også ofte kunnskapen og det samarbeidet.»* Informanten fra NSR sier at vi må få funksjoner, uavhengig av om en kjenner noen. Det er argumentet vårt når vi har «sloss» for den stillingen som næringslivskoordinator[49]. Viktigheten av samarbeid og informasjonsdeling mellom myndigheter og næringsliv er omtalt i Säkerhetsboken (Wermdalen & Nilsson, 2013) og i Kampen mot organisert kriminalitet (Meld. St. 7 (2010-2011), 2010). Ulikheten i Statoils og Telenor Groups kontakt med PST kan være et eksempel på at kontakt er personavhengig slik de to informantene her «advarer» mot. De to bedriftene er store norske internasjonale selskaper og skulle derfor begge ha et godt utgangspunkt for myndighetskontakt. Det er ikke noen grunn til å tro at forholdene skal ligge bedre til rette for andre selskaper, eller selskaper av mindre størrelse.

NSRs konsultative råd er et bredt sammensatt råd bestående av faste og konsultative medlemmer. Rådet kalles det konsultative rådet og ledes av Runar Karlsen fra NHO Service. Rådet er sammensatt av representanter fra tilsluttede organisasjoner, medlemsbedrifter, stifteorganisasjonene, regionale representanter og myndigheter.

[47] E-post 29.07.2014 fra Tor Arnt Dahlstrøm Næringslivsseksjonen (UD)
[48] Det norske veritas (DNV) og Germanischer Lloyd (GL)
[49] Stillingen ble først kalt næringslivsrådgiver for deretter å bli kalt næringslivskoordinator slik den benevnes i dag.

Myndighetsrepresentantene[50] er alle blant de konsultative medlemmene. Medlemmene i det konsultative rådet, både de faste og de konsultative, er sikkerhetsklarert til hemmelig.[51] Dette rådet møtes 3-5 ganger i året. Undergrupper (ulike utvalg) møtes tilsvarende ofte. Personene i utvalgene er personer med kompetanse og interesse for de aktuelle feltene. I dette rådet videreformidles det informasjon og råd for å gjøre bedriftene bedre i stand til å møte sikkerhetsutfordringer, eksempelvis sikkerhetsutfordringer knyttet til bedrifters virksomhet i utlandet. Det videreformidles også informasjon mellom medlemmene og gjennom NSRs egne utvalg, samt informasjon åpent for alle på NSRs nettsider. Grenseløse utfordringer er NSRs utvalg for internasjonale og globale sikkerhetsutfordringer. Informanten i NSR kunne fortelle at i det konsultative rådet løfter man opp de store temaene. Gjennom diskusjon kan det ende opp i veiledere, utvalg og lignende. NSR ønsker flere næringslivskontakter og de «…synes det er svært positivt at regjeringen ønsker å etablere næringslivskontakter i de «nye» politidistriktene etter mønster fra Kripos» (Simonsen, 2015a). Dette styrker inntrykket om at NSR er en viktig bidragsyter og pådriver innen sikkerhetsrådgivning til bedriftene.

Informantene er ikke spurt hvordan de er gitt råd under pågående saker, eksempelvis Statoil under tilfellet In Amenas-angrepet eller Telenor under anslagene mot deres butikker i Pakistan. Informanten i Statoil opplyste at de kan motta råd før en hendelse, og etter en hendelse. Det førstnevnte kaller han security, det andre kaller han beredskap. Informanten regner begge deler som rådgivning.

På NSR sine nettsider er det under fanen *Globalt* samlet informasjon og lenker til informasjon for bedrifter som har virksomhet i utlandet. Det er henvisninger til organisasjoner, myndigheter og veiledere. Informanten ved NSR viste til utvalget Grenseløse utfordringer[52], et forum for norske internasjonale virksomheter. Det er det internasjonale som er fellesnevneren, og de deler erfaringer ut fra ulike steder i verden, som krever litt andre tiltak på håndteringer. I følge informanten i Telenor Group samarbeider de norske, og de har selv et godt samarbeid med Statoil. I landene Telenor jobber er de så mye «hands on»

[50] PST, NSM, POD, Kripos, Økokrim, Direktorat for samfunnssikkerhet og beredskap (DSB), og Toll- og avgiftsdirektoratet.
[51] Telefonsamtale med Runar Karlsen NHO Service, leder i det konsultative rådet, 23.01.2015.
[52] Utvalget har 8 medlemmer med representanter fra olje- og gassektoren, telekom, maritim industri, finans og rådgivning (Næringslivets sikkerhetsråd, u.å.-a).

at de i følge han har mer informasjon enn norske myndigheter. Han håper myndighetene får større forståelse for det selskapene ute kjenner til og har av informasjon. Overført til Joharis vindu faller dette inn under *fasaden*. Dette kunne blitt delt på faste kontaktpunkt mellom myndighetene og bedriftene. Behovet for slike kontaktpunkt, og faktisk informasjonsutveksling kan eksempelvis formidles i NSRs konsultative råd. Grenseløse utfordringers arbeidsområde er internasjonale sikkerhetsutfordringer med følgende målsetning: «…å bidra til at NSRs medlemmer spesielt, og næringslivet generelt, står bedre rustet til å møte sikkerhetstrusler i utlandet» (Næringslivets sikkerhetsråd, u.å.-a). NSR har flere utvalg[53], deriblant det nevnte Grenseløse utfordringer. De arrangerer frokostmøter, har nyhetsbrev en kan melde seg på og samler nyttig informasjon og kontaktopplysninger på sine nettsider. Veilederen for vurdering av sikkerhetsrisiko ved etablering i utlandet er et eksempel på skriftlig rådgivning fra NSR til bedrifter. Kort fortalt viser veilederen blant annet til betydningen av at forhold i Norge og utlandet kan være ulike og at en bør vurdere sikkerhetsrisikoen forut for etableringen i det aktuelle landet (Næringslivets sikkerhetsråd, 2011c). Et annet eksempel er *En orientering om tiger kidnapping – Er du eller din virksomhet et attraktivt mål?* (Næringslivets sikkerhetsråd, 2011b). Denne er bare tilgjengelig for NSRs medlemmer. Tiger kidnapping[54] er et problem som foreløpig har vært forholdsvis ukjent i Norge, men som er aktuelt ved virksomhet i utlandet. B*akgrunnssjekk – en brukerveiledning* (Næringslivets sikkerhetsråd, 2011a) er også et eksempel på slikt veiledende materiale utarbeidet av NSR.

10. mars 2015 arrangerte NSR et sikkerhetsforum (Simonsen, 2015b) med deltakere fra flere av myndighetene jeg har intervjuet informanter hos. I lys av hendelser den siste tiden ble det blant annet satt fokus på samarbeid mellom næringsliv og myndigheter. E, UD, Statoil og NSR deltok i den forbindelse i en paneldebatt. Granhagen, sjef for E, uttalte der at «Etterretningstjenesten ønsker å være så åpen vi kan…» (Simonsen, 2015b). Han brukte Fokus-rapportene som eksempel på denne åpenheten. Dette ønske om åpenhet kan slik jeg ser det være positiv med tanke på fremtidig kontakt med bedrifter med utenlandsvirksomhet og derigjennom sikkerhetsrådgivning. Jan Helge Skogen i Statoil

[53] Kriminalitetsutvalget for varehandel, logistikk, transport og reiseliv, Narkotika, Informasjonssikkerhetsutvalget, Grenseløse utfordringer, og Ran (Næringslivets sikkerhetsråd, u.å.-c).
[54] «Tiger kidnapping skiller seg fra andre former for kidnapping ved at dette er en handling som er kortvarig, og kun har som formål å være i vinnings hensikt» (Næringslivets sikkerhetsråd, 2011b, s. 3). Tiger kidnapping er økonomisk motivert og utføres ikke pga. hat mot offeret.

fortalte hva de anså som viktig ved virksomhet i utlandet. Han trakk blant annet frem grundig risiko- og trusselforståelse, samt aktiv bruk av spisskompetanse og nettverk inklusive ambassaden. Sikkerhetsrådgivning fra myndigheter til bedrifter mener jeg at kan være viktige bidrag til punktene Skogen nevner. Kontakt mellom myndigheter og bedrifter, her eksemplifisert med NSRs sikkerhetsforum, vil kunne være positivt for deres samarbeid og forståelse for hverandres utfordringer og behov.

4.4.3 Er det noen aktører som samarbeider mer enn andre, og hvorfor er det eventuelt slik?

Det fremstår som at PST, E, UD og NSM har et velfungerende samarbeid, og bruk av liaisoner i UD fremstår som å være positivt for samarbeidet.

Dette mener jeg er et argument for å ha representanter hos hverandre, eksempelvis næringslivskoordinatoren i NSR og opplysningene fra NSM-informanten om at NSM skal opprette en key-account manager som skal ha kontakt med deres samarbeidspartnere. Det foreslåtte tiltaket om næringslivskontakter i politidistriktene (Simonsen, 2015a) vil kunne være et godt utgangspunkt for kontakt og informasjonsutveksling, og derigjennom sikkerhetsrådgivning.

Informanten i Seksjon for sikkerhet og beredskap i UD forteller at UD har et nært samarbeid med PST og E. Videre forteller han at de to sikkerhetstjenestene har faste liaisoner i UD – noe som sikrer at fagmiljøene raskt kan bidra med å håndtere spesielle saker/hendelser. Informanten i PST forteller at ordningen med liaison er bra for samarbeidet med UD. Hva E mener om dette samarbeidet er uvisst. Når det er sagt har ingen av de andre informantene sagt noe negativt om samarbeidet. PST[55] og E hadde liaison i UDs krisestab som ble satt under krisehåndteringen av In Amenas (Utenriksdepartementet, 2013), et annet eksempel på samarbeid mellom de tre myndighetene. Det er naturlig at ordningen med liaisoner vil være positivt for samarbeidet og at denne jevnlige kontakten vil gjøre samspillet bedre over tid. I tillegg vil det å ha en liaison hos en samarbeidende aktør (her: myndighetene) vise at

[55] PSTs faste liaison i UD.

partene ønsker samarbeid og at de ser nytten av dette samarbeidet. Betydningen av personlige relasjoner når en jobber sammen over tid skal heller ikke undervurderes. Informanten fra PST forteller at dersom det kommer en bedrift til PST som ønsker å opprette virksomhet i utlandet, så sier de kontakt UD. UD har en viktig rolle. PST har primært ansvar for hva som skjer innenfor Norge.

Det fremgår av PST-instruksen § 10 at PST skal samarbeide med E og NSM, samt offentlige myndigheter og organisasjoner (Instruks for Politiets sikkerhetstjeneste, 2005)[56]. Informanten i PST syns de samarbeider bra med de fleste, men de får påpakning om at de må samarbeide bedre og PST ønsker å samarbeide mer. Han forteller videre at det er mye å hente på samarbeidet mellom NSM, E og PST. Særlig i forhold til næringslivet i utlandet. Det har i følge han kanskje med hvordan Norge er organisert med sektorer, og det kan være vanskelig å «hoppe» fra sektor til sektor. Hovedregelen er UD, men PST blir også spurt. Informasjonen PST får kan være både fra samarbeidende tjenester i Europa og E. Utfordringen er hva de kan si videre og hva de kan gi av informasjon. Da må PST se på hva som er skjermingsverdig. Hvilke regler som gjelder for å gi informasjon videre. Det står blant annet i Gjørv-rapporten at en ønsker at samarbeidet mellom E og PST skal bli bedre. Det er I 2013 utgitt et fellesprodukt om sårbarhet og risiko av E, NSM og PST. Den eneste som er utgitt foreløpig i følge informanten. Den handler i følge informanten egentlig om risiko, og en ser på hele bildet, med utgangspunkt i Norsk Standard[57]. Det var en bestilling fra departementene. Selv om samarbeidsproduktet foreløpig (på intervjutidspunktet) ikke er fulgt opp av flere stemmer dette overens med inntrykket om at E, NSM og PST har et godt samarbeid.

I *Politiets sikkerhetstjeneste Oppgaver og sikkerhet* er E, NSM og UD nevnt blant PSTs mest sentrale norske kontakter (Politiets sikkerhetstjeneste, 2007)[58]. Vi kan også lese at «trusselvurderinger som gjelder norske myndighetspersoner og interesser i utlandet, utarbeides i nært fellesskap med Etterretningstjenesten, som er vår sivile og militære utenlandstjeneste» (Politiets sikkerhetstjeneste, 2007, s. 12). I den åpne trusselvurderingen for 2015 trekkes E og NSM frem som de viktigste myndighetene de har samarbeidet med i forhold til denne trusselvurderingen (Politiets sikkerhetstjeneste, 2015, s. 4). Dette

[56] POD er på lik linje nevnt.
[57] Norsk standard er det som tidligere i oppgaven er omtalt som NS 5830:2012 (Standard Norge, 2012).
[58] POD, DSB, TAD og UDI (Utlendingsdirektoratet) er også nevnt.

underbygger inntrykket om at disse myndighetene har et viktig samarbeid. Informanten fra PST uttaler eksempelvis at samarbeidet kan bli bedre spesielt i forhold til næringsliv i utlandet, noe som viser at samarbeidet også har et forbedringspotensial. På Es nettsider kan vi lese at de «…samarbeider med PST, blant annet om trusselvurderinger i forbindelse med internasjonal terrorisme» (Etterretningstjenesten, u.å.). Opprettelsen av FKS, samt en egen samarbeidsinstruks mellom PST og E (Instruks om samarbeidet mellom E og PST, 2006) tilkjennegir at det er et samarbeid og slik jeg ser det et ønske om å bedre dette ytterligere. Følgende uttalelse er samsvarende med denne forståelsen: «De to tjenestene jobber ut fra ulike juridiske grunnlag. Utfordringen har vært og er fremdeles hvordan og hvilken informasjon som skal deles mellom tjenestene. Det jobbes med å få klarhet i dette, og i mellomtiden jobber tjenestene innenfor eksisterende juridiske rammer, sier Grandhagen» (Etterretningstjenesten, 2014b). Bedre informasjonsflyt mellom E og PST, og fremmedkrigere i Syria er to områder FKS har jobbet med i 2014 (Etterretningstjenesten, 2014b). I Forsvarets årsrapport for 2014 kan vi lese at E samarbeider med NSM og PST innen ulike trusselområder[59] (Forsvaret, 2015, s. 86). «I arbeidet med terrorisme står samarbeidet med Politiets sikkerhetstjeneste sentralt» (Forsvaret, 2015, s. 86), samt at E og PST har videreutviklet deres samarbeid gjennom FKS. I Joharis vindu (figur 2) kunne man satt inn én myndighet på hver side, i denne sammenhengen E og PST, og dermed *fjernet* bedriften fra figuren. Utfordringen knyttet til hva man kan dele av informasjon ligger da i fasaden og blindflekken alt ettersom hvem av myndighetene man tar utgangspunkt i. Endringer tilknyttet det to nevnte feltene vil kunne ha en tenkt positiv effekt på de to siste feltene (arenaen og det ukjente). Da med tanke på forståelsen av åpen tilgjengelig informasjon. Samt redusere størrelsen på det ukjente feltet – eller det Donald Rumsfeld kaller det *ukjente ukjente* (oppgavens punkt. 2.3). Bedre informasjonsflyt kan føre til et bedre, mer korrekt og tidsriktig informasjonsgrunnlag som igjen kan være utgangspunkt også for (en kvalitativt bedre) sikkerhetsrådgivning fra myndigheter til bedrifter.

I Sikkerhetstilstanden 2012 kan vi lese at NSM bruker blant annet PSTs og E-tjenestens trusselvurderinger som grunnlag for rapporten som er koordinert med de to tjenestene

[59] «…grenseoverskridende trusler, inkludert terrorisme, spredning av masseødeleggelsesvåpen og trusler i det digitale rom» (Forsvaret, 2015, s. 86).

(Nasjonal sikkerhetsmyndighet, 2012). I sikkerhetstilstanden 2014[60] (Nasjonal sikkerhetsmyndighet, 2014) vises det til Es rapport Fokus 2014. Selv om dette ikke er et samarbeidsprodukt er det et eksempel på at myndighetene bruker hverandres produkter i sine egne vurderinger. Dette er i likhet med samarbeidsproduktet nevnt over et godt utgangspunkt for samarbeid og vitner om forståelse for hverandres kunnskap og kompetanse.

I følge informanten fra NSM er PST en av deres hovedsamarbeidspartnere. NSR trekkes også frem som en viktig aktør for NSM som har en plass i NSRs konsultative råd. Informanten opplyste også at NSM er i ferd med å etablere en key-account manager som skal ha direkte kontakt mot en rekke samarbeidspartnere, deriblant NSR.

Informanten i Statoil ønsker tettere kontakt med E for å få et større og bedre beslutningsgrunnlag i deres risiko- og trusselvurderinger. Informanten i Telenor Group ønsker mer direkte kontakt med fagmiljøene og ikke informasjon videreformidlet gjennom UD. Selv om E og PST ikke nevnes eksplisitt forstår jeg det slik at E og PST er blant fagmiljøene han ønsker mer og direkte kontakt med. Informasjon som videreformidles via andre kan endres og i verste fall ikke komme frem til mottakerne i sin tiltenkte form, omtalt under blindflekken i Joharis vindu. Det kan være gode intensjoner bak det å gi informasjon via andre aktører. De kan ha en allerede velfungerende relasjon, et godt utgangspunkt for kontakt vedrørende «sensitive» tema. Bevissthet omkring potensielle utfordringer ved videreformidling gjennom andre er derfor helt nødvendig. Informasjonen fra informanten i Statoil og informanten i Telenor Group tyder på at bedrifter har ulik kontakt med PST, noe som kan være tilfelle også i kontakten med andre myndigheter.

Felles kontraterrorsenter for E og PST skal i følge informanten fra PST ha fokus på terror og å lage fellesprodukter: mer fellesprodukter og mer samarbeid, og slik svare opp 22. juli-rapporten. Trusselvurderingene blir trolig gradert og unntatt offentligheten i følge han. Denne opprettelsen vil trolig være positivt for samarbeidet mellom de to sikkerhetstjenestene. Et tettere samarbeid vil også kunne være med på å forhindre at informasjon en ikke trenger holde skjult pga. lov- eller regelverk blir gjort tilgjengelig. I statsministerens redegjørelse i Stortinget om terrorangrepet i Algerie (sak nr. 3), 23. januar

[60] Ingen utgivelse i 2013.

2013, uttalte han at «Regjeringen arbeider med tiltak for å forsterke samarbeidet mellom Politiets sikkerhetstjeneste og Etterretningstjenesten. Målet er en ytterligere styrkning av evnen til å forebygge, avdekke og bekjempe terrortrusler mot Norge og norske borgere og interesser i utlandet».

Informanten i Statoil nevnte deres tilknytning til organisasjonen OSAC. Informanten i Kripos nevnte Scottish Business Crime Resilient Center, som også er omtalt i stortingsmeldingen Kampen mot organisert kriminalitet (Meld. St. 7 (2010-2011), 2010). Dette er eksempler på public private partnership, to fora der det utveksles informasjon mellom det offentlige og det private. I følge informanten i Statoil er OSAC i USA en organisasjon der myndighetene er veldig flink, og har etablerte fora for å dele informasjon. Der har de en etablert praksis som fungerer veldig godt og myndighetene er veldig proaktive når det gjelder informasjon. OSAC har forum i ulike land, og Statoil er tilstede på møtene. Statoil har landkontor i USA og får informasjon fra OSAC. Dette er noe Statoil i følge informanten har kommunisert til norske myndigheter: at dette forumet finnes og fungerer veldig bra. OSAC arbeider for å gi regulær og tidsriktig informasjon, og faller slik inn under oppgavens definisjon av sikkerhetsrådgivning.

Det kan tenkes at informanter er forsiktig eller unnlater å trekke frem aktører de samarbeider med. Dette for å unngå publisitet eller gi sensitiv informasjon. På samme måte kan det være at en ikke ønsker å fortelle om dårlige sider ved samarbeidet for å unngå å gjøre samspillet mer utfordrende eller forringe muligheten for tettere kontakt. Direkte kontakt med dem det gjelder er av flere grunner den mest konstruktive måten å forsøke å bedre samarbeid som fungerer mindre bra, og i mindre grad gjennom intervjuer utført av en utenforstående forsker.

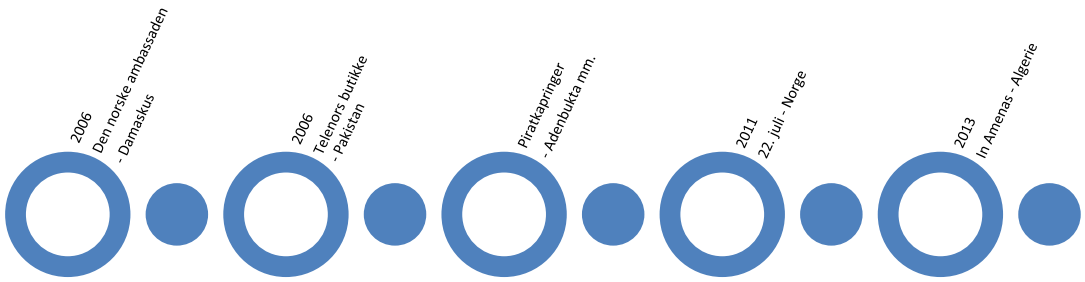
4.4.4 Er det, ved hjelp av de fem referansehendelsene, mulig å se endringer i sikkerhetsrådgivningen og dialogen mellom myndighetene og bedrifter?

Det viser seg å være delvis korrekt at store og alvorlige hendelser nasjonalt og internasjonalt har ført til endringer innen sikkerhetsrådgivningen som bedrives fra norske myndigheter. Samtidig lar det seg vanskelig gjøre å peke på bestemte hendelser som merkbart har endret norske myndigheters sikkerhetsrådgivning overfor store norske bedrifter med virksomhet i utlandet. To av oppgavens referansehendelser ble av informantene ansett som betydningsfulle. Referansehendelsen 22. juli ble trukket frem av flere, og In Amenas hadde i følge et flertall av informantene påvirket sikkerhetsrådgivningen i en eller annen form.

I etterkant av 22. juli og In Amenas er det blitt mer fokus på virksomhet i risikoutsatte områder, sikkerhetsrådgivning er blitt mer etterspurt, samt at tema er blitt aktualisert blant annet i media. Det kan derfor se ut som at det er en årsaksforklaring (causal explanation)[61] mellom de to sistnevnte hendelsene og fokus på og bruk av sikkerhetsrådgivning. Det er likevel slik at fokuset/bruken kan skyldes summen av mange hendelser og/eller andre faktorer samlet sett. Endringer som følge av alvorlige hendelser (kriser) kan som beskrevet tidligere i oppgaven være finjusteringer, policyendringer eller paradigmeskifte (Fimreite et al., 2014). Økt fokus kan gjerne sies å være finjusteringer, mens kombinasjonen av økt fokus og bruk av sikkerhetsrådgivning er nærmere en policyendring enn en finjustering. Økt fokus og bruk av sikkerhetsrådgivning kan være et tegn på at risikoforståelse prioriteres høyere, og at bedriftene dermed kan få en bedre (risiko-) erkjennelse av potensielle trusler.

Jeg har benyttet fem referansehendelser i oppgaven for å identifisere eventuelle endringer i sikkerhetsrådgivningen som utøves fra myndighet til bedrift: anslaget mot den norske ambassaden i Damaskus i 2006, anslag mot Telenors butikker i Pakistan i 2006, piratkapringer (2006-)[62], terrorangrepet 22. juli 2011, og terrorangrepet i In Amenas 2013. Se tidslinjen under.

[61] Årsaksforklaring kan forklares ved at det «angir at et fenomen eller en hendelse er frembrakt eller produsert av en eller flere forutgående fenomener/hendelser» (Johannessen et al., 2010, s. 409).
[62] Lar seg vanskeligere tidfeste, men fra og med 2006 har piratvirksomhet påvirket «…økonomien i fattige land i regionen» (Norges Rederiforbund, u.å.). «Norske rederier brukte over en milliard kroner på sikringstiltak mot piratangrep i 2013» (Norges Rederiforbund, u.å.) noe som viser at det fortsatt er et aktuelt problem.



Figur 5: Referansehendelsene

En av årsakene til at jeg sendte ut spørsmålene i forkant av intervjuene var for å «hjelpe» hukommelsen til informantene. Når jeg spurte om hendelser der den eldste er om lag ti år tilbake i tid er det sannsynlig at informantene har glemt omstendigheter omkring hendelsene. Det er heller ikke sikkert at informanten arbeidet med *sikkerhetsfeltet* på det aktuelle tidspunktet. Nye «ferske» hendelser som fortsatt omtales med jevne mellomrom vil kunne få uforholdsmessig stor betydning og tillegges innflytelse som mer riktig burde vært plassert andre steder. Å fortelle at hendelser har ført til (store?) endringer kan informanter oppleve at er det samme som å vise svakhet og manglende (eller feil?) fokus. Det å fremstille situasjonen som bedre enn det den er/var kan da være en strategi for å fremstå som profesjonell og kompetent.

Det er flere mulige forklaringer på hvorfor det ikke fremkommer (store) endringer. En forklaring kan være at en ikke vil erkjenne svakheter. En annen forklaring at hvis det fungerer bra i dag kan tidligere utfordringer nå være «glemt». En tredje forklaring kan være at en kanskje ikke jobbet innen sikkerhetsfeltet på den tiden, samt at det kan være vanskelig å huske tilbake.

In Amenas var i følge flere av informantene en viktig hendelse som påvirket synet på sikkerhet og sikkerhetsrådgivning. Der In Amenas bekreftet behovet for samarbeid og informasjonsutveksling. Hendelsen i Algerie fikk partene til å innse samarbeidsbehovet og gå fra å snakke om det til å gjøre noe med det. Det er stilt spørsmål med Es kontakt opp mot næringslivet, og hvordan norske myndigheter som helhet kan bidra til at norske bedrifter kan drive virksomhet i utlandet på en sikrest mulig måte.

Svarene på hvilke referansehendelser som myndighetene og bedriftene mener er viktig, er fremstilt i en enkel tabell under dette avsnittet. Tabellen er laget med utgangspunkt i innsamlet data vedrørende referansehendelsene. Informantene har ikke selv krysset av i en tabell. Avkrysning i tabellen under betyr at det vurderes slik at informanten anser hendelsen som viktig.

Myndighet/ bedrift:	Referansehendelser:				
	Damaskus 2006	Pakistan 2006	Pirat-Kapringer	22. juli	In Amenas
PST				X	X
E					(?)
FSA					
NSM				X	X
UD	X				X
Seksjon for sikkerhet og beredskap, UD					X
NSR					X
Kripos					
Statoil				X	X
Telenor Group				X	X
Telenor Norge AS[63]					

Tabell 2: Oversikt over hvilke referansehendelser informantene trekker frem som viktig i forhold til sikkerhetsrådgivning.

De tre første referansehendelsene har i følge informanten fra PST ikke påvirket deres sikkerhetsrådgivning i stor grad. PST er klar over hendelsene, og de har økt fokus på Telenor

[63] Telenor Norge AS ble ikke spurt om de tre første referansehendelsene. Da Telenor Norge har sin virksomhet i Norge ble intervjuet fulgt opp av et intervju med Telenor Group som har virksomhet i utlandet. Telenor Group er spurt om samtlige av de fem referansehendelsene.

pga. Muhammed-karikaturene. De har ikke endret sikkerhetsrådene eller hvordan de gir råd. Hvem de gir råd til endres hele tiden ut fra trussel, prioriteringer, hendelser og andre faktorer som for eksempel medieoppmerksomhet. Piratkapringene har ikke PST befattet seg særlig med. Informanten fra PST trekker frem at 22. juli har ført til at en anbefaling om robust og permanent grunnsikring. Samt at etter In Amenas har PST mer fokus på norske bedrifter med aktivitet i risikoområder og at In Amenas har aktualisert sikkerhetsrådgivning. Signalene fra overordnet myndighet oppleves som uklare og spørsmålet er hvem de skal gi råd og hvordan. De to hendelsene har ført til at rådgivningen får aktualitet, blir relevant og blir lyttet mer til. Sikkerhetsrådgivning blir mer etterspurt etter 22. juli og det blir også sett på terrortrusler. Risikoerkjennelsen og forståelsen er blitt bedre, men ikke god nok.

In Amenas har som oppgaven tidligere har beskrevet aktualisert sikkerhetsrådgivning fra E til bedrifter med virksomhet i utlandet. Utover det lar det seg vanskelig gjøre å si noe om endringer i forhold til de fem referansehendelsene. De fremkom heller ikke noe om endringer som følge av hendelsene for FSAs virksomhet i min kontakt med dem, verken ved deres eller Es virksomhet. I tabellen er det for E satt et spørsmålstegn i parentes på In Amenas-hendelsen. Dette på grunn av omtalen Es kontakt med næringslivet har fått etter hendelsen. E er som nevnt ikke informant i denne oppgaven.

Informanten fra NSM forteller at de følger med på det som skjer og alle reelle hendelser påvirker råd og veiledning vi gir til selskaper i Norge og selskaper med virksomhet i utlandet. Slik har de fem referansehendelsene påvirket utførelsen av deres sikkerhetsrådgivning, veiledning og dialog med selskapene. Spesielt har 22. juli hatt stor faglig betydning samt økt ressursbruk på råd og veiledning. Han sier videre at han tror at In Amenas ble en slags bekreftelse på det NSM hadde påpekt i mange år forut for 22. juli-hendelsen. Spesielt i forhold til kultur. Sikkerhetskulturbegrepet, som informanten jobber mest med i det daglige, er på mange måter løftet frem i Gjørv-rapporten. Det blir i følge han i veldig stor grad bekreftet gjennom det også Statoil sier om sin egen kultur i forhold til sikkerhet og hvem som har ansvaret for sikkerhet. Innen sitt eget fagfelt tror informanten at In Amenas bekreftet Gjørv-rapporten. Konkret innhold på råd og veiledning knyttet til reelle hendelser som nevnt i oppgaven, kan ikke beskrives nærmere da dette i følge informanten inneholder sikkerhetsgradert informasjon.

Informanten i UD trekker frem at det er et eget kapittel om samarbeid i Gjørv-rapporten som i stor grad omfatter internasjonalt samarbeid. Dette er i følge han på en måte Norges nasjonale antiterrorstrategi, som jo går mye bredere enn næringslivsbiten. Det bidro til at en fikk en økt oppmerksomhet på de utfordringene terrorisme utgjør. In Amenas som er mer innenfor UDs ansvarsområde, har ført til at en har sett på sikkerhetsrådgivning opp mot næringslivet og hvordan vi kan forbedre det. Evalueringsrapporten av norske myndigheters krisehåndtering ved In Amenas-hendelsen er sammenfallende med informantens uttalelse om å se etter mulige forbedringer (Utenriksdepartementet, 2013). I følge informanten fra Seksjon for sikkerhet og beredskap i UD var 22. Juli bestående av et dels IED-angrep[64], og dels et «Fedayeen»-angrep[65] (Utøya). En reel risiko for bedriftene, som bedriftene informeres om. In Amenas har ført til en ytterligere forbedret dialog med Statoil (og de øvrige større bedrifter som opererer i utlandet), samt et utvidet samarbeid med den britiske utenrikstjeneste særlig innenfor krisehåndtering. Ut over dette har ikke angrepet på Statoils anlegg i In Amenas medført spesielle endringer. Angrepene understreker imidlertid noe som UD i lengre tid har presisert: At norske bedrifter som opererer i utlandet må forholde seg gjeldende norske lovverk - som pålegger bedriften på selvstendig grunnlag å kartlegge all risiko forbundet med utførelse av arbeide, og på grunnlag av det iverksette nødvendige sikkerhetstiltak. For den restrisiko som bedriften aksepterer skal det utarbeides beredskapsplaner for å håndtere eventuelle hendelser. Denne konkrete hendelsen illustrerer dertil at det i mange tilfeller er nødvendig å iverksette omfattende tiltak selv om sannsynligheten for en hendelse i utgangspunktet vurderes som minimal. Hendelsen i Damskus i 2006 har blant annet ført til at en aktivt oppdaterer oversikten over norsk næringsliv i embetsdistriktet, slik at relevant informasjon kan distribueres fortløpende.

Informanten i NSR tror 22. juli det har gitt en endret forståelse fra myndighetene, for samarbeid på tvers av sektorene og det private næringsliv. Det tydeliggjør på en måte at dette klarer en ikke alene. Det er viktig å ikke fokusere på forrige hendelse. Dersom du har en god grunnsikring, kan du stå i mot mye. I forhold til In Amenas-hendelsen har NSR utvalget Grenseløse utfordringer, norske bedrifter med virksomhet utenlands. Der utveksles erfaringer, og det er utarbeidet en publikasjon som heter *Veileder for vurdering av*

[64] Improvised Explosive Device/improvisert bombe

[65] «Fedayeen, selvmordspatrulje, kommandogruppe. Uttrykket kommer opprinnelig fra et begrep innen sjiittisk islam; i moderne språkbruk betegner det geriljastyrker, særlig palestinske» (Gundersen, 2009).

sikkerhetsrisiko ved etablering i utlandet. Det har endret seg slik at det nå er mer fokus på sikkerhetsvurderinger, at du kanskje må gjøre helt andre sikkerhetsvurderinger ute enn hjemme. NSR har sett at norske virksomheter er utsatt for hendelser. Slike hendelser, inkludert hendelsene mot Telenor og ambassaden i Damaskus, førte til opprettelsen av utvalget Grenseløse utfordringer. Ikke spesielt de to hendelsene, men «slike» hendelser. Utvalget er opprettet på bakgrunn av behovet for sikkerhetsrådgivning til norske internasjonale selskaper. Dette har også økt dialogen mellom NSR og bedrifter. Alt som foregår ute på havet er i følge informanten utenfor NSRs mandat. Beredskapssekretariatet i Norges Rederiforbund (en av NSRs stiftere) tar seg av det. De fem referansehendelsene har utmerket seg på ulike måter. 22.7 har fått fokus på å tenke risiko og fysisk sikring her hjemme. In Amenas gitt fokus på å vurdere sikkerhetsrisikoen i utlandet. Ondsinnede tilsiktede hendelser kan man ikke sikre seg mot, men en kan i følge informanten i NSR gjøre noe med konsekvensene og slik redusere sårbarheten.

Informanten i Kripos, Næringslivskoordinatoren i NSR, mener 22. juli og In Amenas er et overordnet nivå som politiledelsen burde svare på. Hun har merket en endring i holdning til samarbeid med andre aktører i politiet. Videre forteller hun at næringslivet sier at det har vært en positiv utvikling der politiet er mer åpne for innspill og å gi informasjon de siste fem årene. Samtidig er det en lang vei å gå. Får vi en struktur på samarbeidet som er formalisert vil vi kunne svare opp rapportene. Ledelsen kunne blitt målt på samarbeid med andre aktører. Næringslivskoordinatorstillingen var ønsket fra NSR med tanke på informasjonsutveksling og det ble beskrevet en modell for samarbeid: Scottish Business Crime Resilient Center. Det handler om et samarbeid mellom politi, andre offentlig myndigheter og næringsliv som sitter i et senter i Skottland og utveksler informasjon. Nesten som et nasjonalt etterretnings- og analysesenter. Hun tenker det vil være løsningen på å ha en mer helhetlig tilnærming til næringslivet. At man kan få en pakke, dette er det PST, Økokrim, Kripos, NSM, NSR sier om hva som er trusler og utfordringer. I forhold til de tre andre referansehendelsene - har ikke informanten kjennskap til om de har endret noe på deres måte å kommunisere med omgivelsene på - på en strukturert, forutsigbar måte. Det betyr likevel ikke at Kripos ikke har gitt konkrete råd og veiledning, men dette er gjerne etter forespørsel.

Informanten i Statoil forteller at 22. juli Ikke nødvendigvis påvirket rådgivningen, men mer at de trengte å forsterke det som går på security i selskapet og bygge en bedre security-kultur. Security må styrkes, og Statoil er i følge han nødt til å forbedre kulturen. Ikke spesifikt i forhold til sikkerhetsrådgivning, men det er en del av bildet. I forhold til In Amenas ser Statoil at trusselbildet er veldig komplekst, skiftende, utfordrende. Ergo trenger Statoil i følge informanten best mulig informasjon for å klare å håndtere den. Sikkerhetsrådgivning er som han sier en del av dette. I følge informanten så blir det på den samme måten som ved 22. juli, og det har bare forsterket det Statoil allerede hadde sett og som de hadde begynt å jobbe med tidligere. Det ble gjort veldig mye i Statoil etter 22. juli når det gjelder security, og det ble bare forsterket og førte til en fortgang i det arbeidet da In Amenas-hendelsen fant sted. Rådgivning er en del av det, spesielt det som går på å skaffe seg best mulig kontroll på trusselbilde. De tre andre referansehendelsene har informanten bekjent ikke ført til noen endring i den rådgivning vi får fra myndighetene. Forbedring av kulturen og styrking av security som informanten i Statoil påpeker, samt opprettelsen av en egen sikringsavdeling i Statoil (Aadland, 2014) vil jeg si at må kunne kategoriseres under policyendring (Fimreite et al., 2014) i selskapet i etterkant av In Amenas.

Informanten i Telenor Group forteller at de som jobber med dette til daglig hadde nok det samme synet før. Det som er viktig er at slike hendelser, spesielt 22. juli og In Amenas, har skapt større forståelse i ledelsen. Slike hendelser øker kunnskapen, interessen og awarenes`en blant topplederne, konsernledelsen. Tror dette gjelder oss, Statoil, Yara osv. For Telenor var Muhammad-karikaturene den første tankevekkeren i følge informanten. Der så Telenor hvordan storpolitiske hendelser plutselig kunne påvirke dem. Danske tegninger førte til at to av Telenors butikker i Pakistan ble rasert som konsekvens av dette. I følge informanten trodde nok mange at Telenor var dansk. Karikaturtegningene viser at Telenor er sårbare for hendelser som de ikke er skyld i selv. Så kom In Amenas-hendelsen. Spesielt In Amenas har gjort det lettere å diskutere med myndighetene nå enn før. Informanten tror at begge parter har sett at de er avhengig av hverandre. Det har gitt en positiv boost for samarbeidet. Muhammad-karikaturene viser at Telenor er sårbare mange steder, at de må jobbe proaktivt, og sette inn tiltak i forkant. Hendelsene i Pakistan har endret litt for Telenors del. Dialogen med ambassaden i Pakistan er blitt bedre, men informanten tror nok dette først og fremst er på grunn av initiativ fra Telenor, ikke som følge av initiativ fra UD.

Denne hendelsen har nok ikke, slik informanten ser det, hatt noe innvirkning på dialogen mellom Telenor og myndighetene. Dialogen og samhandlingen mellom myndigheter og bedrifter er bedre i dag med tanke på deling av informasjon, dialog og råd. In Amenas har virkelig fått partene til å forstå at vi må samarbeide mer (en bekreftelse på dette), gjøre det sammen og ikke bare snakke om det- kan kalle det risikoerkjennelse. Hendelsen i Damaskus og piratkapringene har i følge informanten ikke ført til endringer.

For Telenors del ser ikke erfaringene fra Pakistan ut til å ha påvirket betydningen av de andre referansehendelsene på noen annerledes måte enn for Statoils del.

Opprettelsen av Felles kontraterrorsenter (FKS) for E og PST kan ikke direkte knyttes til sikkerhetsrådgivning. Samtidig kan dette føre til bedre samarbeid dem i mellom og bedre informasjon som igjen kan benyttes av bedriftene i deres egne vurderinger. Opprettelsen av FKS (februar 2014) ble gjort som en følge av anbefaling fra 22. juli-kommisjonen og er slik sett en endring som følge av 22. juli (og kanskje også påvirket av andre hendelser?). En av FKS sine oppgaver er å analysere terrortrusler mot norske interesser. Dette kan derfor sies være positivt for sikkerhetsrådgivningen og en følge av en av referansehendelsene (22. juli) jeg har brukt i oppgaven. Om det vil få betydning for sikkerhetsrådgivningen, og eventuelt hvilken effekt dette vil kunne få er vanskelig å si noe om.

Det kan som omtalt innledningsvis være lettere å huske de siste hendelsene og den eventuelle påvirkningen de hendelsene har ført til. Dette må tas med i vurderingen av svarene. Det er 22. juli og In Amenas som får mest omtale fra informantene. Da med unntak av informanten i Telenor Group som også trekker frem hendelsene mot deres butikker i Pakistan, uten at han tilskriver den noen nevneverdig betydning for sikkerhetsrådgivningen. Informanten i PST sier at de har økt fokus på Telenor etter Muhammed-karikaturene. Samt at informanten fra Seksjon for sikkerhet og beredskap i UD viser til at hendelsen i Damaskus 2006 førte til at en aktivt holder oversikt over norsk næringsliv i embetsdistriktet og derigjennom et bedre utgangspunkt for informasjonsdistribusjon til dem. At hendelsen som rammet UDs ambassade i Damaskus har påvirket dem på en eller annen måte kan ikke sies å være oppsiktsvekkende. 22. juli og In Amenas er foruten «nylige» hendelser, også hendelser som har fått stor medieomtale. Gjørv-rapporten har sett nærmere på norske styresmakter og politiet, PST, E, NSM og UD er blant de omtalte i rapporten. UD har evaluert norske

myndigheters krisehåndtering knyttet til In Amenas (Utenriksdepartementet, 2013) og Statoil har evaluert seg selv (Statoil ASA, 2013b). Den sistnevnte rapporten har i likhet med Gjørv-rapporten fått stor oppmerksomhet i media.

Forsvarsbygg opplyser i sin årsrapport for 2013 at de har hatt en økning i sin rådgivning knyttet til sikring av bygg på 74 prosent (Forsvarsbygg, 2014, s. 35). Økningen i rådgivningen kan bygge opp under det økte fokuset og bruken av sikkerhetsrådgivning som er fremkommet i denne oppgaven i etterkant av 22. juli og In Amenas. I deres brosjyre *For et tryggere Norge* vises det til 22. juli og betydningen av gjennomtenkte sikkerhetsløsninger (Forsvarsbygg, u.å.-a). Denne henvisningen er også sammenfallende med dette inntrykket.

Å huske endringer som følge av hendelser nærmere ti år tilbake i tid kan være krevende. Informantene er eksempelvis ikke blitt spurt om de arbeidet med fagfeltet i 2006. Dette kan også ha en betydning. På den andre siden vil det kunne sette informantene og virksomheten i et dårlig lys dersom hendelsene i 2006 førte til tilsvarende råd og endringsforslag som 22. juli og In Amenas uten at noe faktisk ble endret. Arbeidsgivers ansvar for egne ansatte (jf. arbeidsmiljøloven og internkontrollforskriften) og betydningen av bedrifters omdømme vil kunne påvirke informantenes svar. Det er mindre problematisk at 22. juli og In Amenas, hendelser med nærhet i tid, bekreftet tilsvarende utfordringer. Dette gjelder både i det statlige og det private. Til tross for fokus på permanent grunnsikring (22. juli) og mer samarbeid og forståelse for samarbeid mellom myndigheter og bedrifter (In Amenas) har ikke oppgaven avdekket det vi kan kalle *vannskiller* i synet og utøvelsen av sikkerhetsrådgivning. Av de fem referansehendelsene kan en likevel si at de to siste har hatt tilsynelatende størst betydning. Dette blir tydelig om en ser på tabell 2. At det er ferske hendelser med stor medieomtale har trolig en del å si for dette. Avslutningsvis er det nødvendig å presisere at det ikke er fremkommet informasjon som tyder på at det er tilbakeholdt informasjon, eller at informantene har fremstilt situasjonen som bedre enn det den faktisk er.

5. Avsluttende betraktninger og videre undersøkelser

5.1 Innledning

I denne delen av oppgaven oppsummeres oppgavens funn, og funnene ses i lys av tidligere forskning og teori. Jeg kommer også med forslag til tema som kan undersøkes nærmere.

5.1 Funn

Oppgavens fire problemstillinger er besvart i det foregående kapittelet. Problemstilling nr. 1: Hvordan bedriver norske myndigheter sikkerhetsrådgivning overfor store norske bedrifter med virksomhet i utlandet, og på hvilke områder gis det slik rådgivning? Med hensyn til denne første problemstillingen viser mine undersøkelser at myndighetene driver sikkerhetsrådgivning innen sine (ulike) arbeidsfelt, men at rådgivningen er av ulik karakter og fremstår som ikke-regulær. Rådgivningen er både av forebyggende karakter (definisjonens spor 1) og knyttet til spesifikke saker (definisjonens spor 2). Myndighetene produserer ulikt veiledende materiell, derav noen samarbeidsprodukter. Dette er en av flere informasjonskilder bedriftene benytter seg av i sine egne vurderinger, og kan derfor sies å være en del av den forebyggende rådgivningen (spor 1). Da flere av utgivelsene er (mer eller mindre) årlige kan de regnes som regelmessige. PSTs åpne trusselvurderinger, Es Fokus-rapporter, og NSMs rapport om sikkerhetstilstanden er eksempler på slike utgivelser (Etterretningstjenesten, 2014a; Nasjonal sikkerhetsmyndighet, 2014; Politiets sikkerhetstjeneste, 2014). NSRs stilling som kontaktpunkt og mellomledd mellom bedrifter og myndigheter, herunder det konsultative rådet, fremstår som en viktig aktør for formidling av informasjon/sikkerhetsrådgivning til bedriftene. Vertslandet er ansvarlig for sikkerheten for de som befinner seg på deres territorium, både forebygging og håndtering av trusler (Utenriksdepartementet, 2013, s. 6).

Problemstilling nr. 2: I hvilken grad er det kontakt mellom aktørene og hvorfor samarbeider de, hvilken type kontakt har de, og hvor hyppig er denne kontakten? Det viser seg at

kontakten mellom myndighetene og bedriftene er av varierende type og karakter, uten at det på bakgrunn av mine data lar seg gjøre å anslå hyppigheten på denne kontakten nærmere. Det kan stilles spørsmål med om ulikheten i kontakt kan tilskrives at samarbeid kan være person- og ikke funksjonsavhengig. Dette er et problem som er trukket frem av informanter i oppgaven. Kontakten mellom aktørene varierer fra å være direkte (eksempelvis én til én) til forskjellige typer åpen og upersonlig informasjon (internett/veiledere), samt fora med flere til stede (eksempelvis NSRs konsultative råd). Bedriftene ønsker et best mulig grunnlag for å gjøre egne vurderinger, mens myndighetene utfører oppgaver tilhørende deres arbeidsfelt. Hva en kan dele av informasjon og med hvem er en utfordring for myndighetene.

Problemstilling nr. 3: Er det noen aktører som samarbeider mer enn andre, og hvorfor er det eventuelt slik? Det viser seg at det er ulik kontakt mellom myndighetene, og mellom myndighetene og bedriftene. Det fremstår som at PST, E, UD og NSM har et velfungerende samarbeid, og bruk av liaisoner i UD virker å være positivt for deres samarbeid. Informasjonen fremkommet i intervjuene med Statoil og Telenor Group tyder på at bedrifter har ulik kontakt med PST, noe som kan være tilfelle også i deres kontakt med andre myndigheter. At en får informasjon via andre kan være en forklaring på manglende kontakt, noe som ikke nødvendigvis trenger å være noe problem.

Problemstilling nr. 4: Er det, på bakgrunn av de fem referansehendelsene, mulig å se endringer i sikkerhetsrådgivningen og dialogen mellom myndighetene og bedrifter? Referansehendelsen 22. juli ble trukket frem av flere, og In Amenas hadde i følge et flertall av informantene påvirket sikkerhetsrådgivningen i en eller annen form. Her kan det være flere faktorer som påvirker dette funnet: eksempelvis nærhet i tid, informanters hukommelse, og et ønske om ikke vise at problemer har vært kjent i lengre tid uten at noe er blitt gjort tidligere. Når det er sagt er dette to alvorlige hendelser som har preget de fleste norske borgere i en eller annen grad. Kombinert med stort mediefokus og uttalelser og fokus fra myndighetspersoner er det ikke unaturlig at hendelsene har påvirket sikkerhetsrådgivningen som bedrives fra myndigheter overfor bedriftene.

Sikkerhetsrådgivningen som gis av norske myndigheter er av varierende karakter og ikke regulær, noe jeg syns er svært interessant. Kombinert med uklarhet fremkommet i

datamaterialet mitt i forhold til hva som inngår i sikkerhetsrådgivning som begrep, hvem som skal gjøre hva, overfor hvem og på hvilken måte tyder slik jeg ser det på et behov for avklaringer og konkretisering av ansvar og samarbeid mellom myndighetene. Samarbeid myndighetene i mellom er et tema i 22. juli-rapporten (NOU 2012:14, 2012), og samarbeid med relevante myndigheter og organisasjoner er tema i In Amenas-rapporten (Statoil ASA, 2013b). Sikkerhetsrådgivningen fra myndighetene til bedrifter blir da aktualisert ved at den påvirkes av samarbeidet dem i mellom. Vertslandene har ansvar for sikkerheten på sitt territorium. Sikkerhetsrådgivning fra norske myndigheter er likevel en viktig del av bedriftenes sikkerhetsvurderinger, selv om bedriftene har ansvaret for sine ansattes arbeidsforhold. Gjennom sin rolle som mellomledd og kontaktpunkt mellom myndigheter og bedrifter fremstår NSR å være en betydningsfull aktør innen sikkerhetsrådgivningen. Deres målsetning om å være et single point of contact illustrerer slik jeg ser det hvor betydningsfull NSR vurderer kontakten mellom bedrifter og myndigheter.

5.2 Funnene satt i et videre perspektiv

Sikkerhetsrådgivning hører inn under det vi kan kalle samfunnssikkerhetsfeltet, et tverrfaglig område med tanke på aktører og metoder. Sikkerhet & beredskapsfiguren (figur 1) viser omfanget på en oversiktlig måte. Temaet sikkerhetsrådgivning er lite behandlet i faglitteraturen og det foreligger ikke en definisjon av begrepet. Oppgaven ble derfor innledet med en egen definisjon av begrepet: Råd og/eller informasjon som gis i den hensikt å bedre virksomheters (kontinuerlige) sikringsarbeid for slik og best mulig å kunne forebygge og/eller håndtere tilsiktede uønskede hendelser fra personer eller grupper. Sikkerhetsrådgivningen kan sies å ha to spor: 1) forebyggende råd, og 2) spesifikke råd knyttet mot sak eller hendelser.

Definisjonen utelater dermed beredskapsarbeid knyttet til eksempelvis naturkatastrofer og epidemier (safety). Det tas da et forbehold om at spredning av sykdommer kan være en bevisst handling og således en (ondsinnet og) tilsiktet handling. Definisjonen kan plasseres under security-feltet, et felt som kan synes mindre belyst og utforsket sammenlignet med safety-feltet. En skal være forsiktig med å forklare dette på en enkel måte, men denne

skjevheten, om en kan kalle det det, kan muligens tilskrives fokuset på å unngå uønskede hendelser i oljebransjen - safety-siden. Informanten fra PST uttalte i intervjuet at «Vi er veldig god på safety i Norge, og noe av grunnen til det er oljeindustrien». Denne uttalelsen er sammenfallende med dette inntrykket. Dagens fokus på tilsiktede handlinger, i særdeleshet terrortrusselen, vil kunne påvirke denne *fordelingen* av fokus.

Kunnskapen som er fremkommet i denne oppgaven vedrørende sikkerhetsrådgivning kan være et bidrag og/eller utgangspunkt for videre undersøkelser for å forebygge de tilsiktede handlingene som omtales i Norges Forskningsråds Program for samfunnssikkerhet (SAMRISK II) (Programplanutvalget, 2013, s. 5): *Forebygging av terrorisme og andre tilsiktede handlinger med stort skadepotensiale*[66]. Sikkerhetsrådgivning berører også andre prioriterte temaer, eksempelvis påvirkning av risikoforståelse og –erkjennelse.

Uttrykket i etterpåklokskapens lys kan være ubehagelig for de involverte partene. Med fakta på bordet vil en ofte finne svakheter med tidligere vurderinger og analyser, noe som også gjelder på security-feltet. Tidligere statsminister Kåre Willoch (Høyre) uttalte i forkant av fremleggelsen av 22. juli-rapporten at «…etterpåklokskapen er bedre enn ingen klokskap» (Vaaland, 2012)[67]. Overført til sikkerhetsrådgivningen jeg har undersøkt nærmere, et område innen forebygging av security-hendelser, tenker jeg at vi må bruke det som har fremkommet av informasjon og kunnskap i etterkant av alvorlige hendelser for å styrke sikkerhetsrådgivningen som allerede bedrives. Vi må lære av det som har skjedd, samtidig som vi ikke planlegger og tilpasser oss til det som har skjedd, men morgendagens trusler enten de er drevet av økonomiske, politiske eller ideologisk motiver. Sigve Indregard stiller i denne sammenhengen det betimelige spørsmålet: «…ender [vi] opp med systemer som forutser forrige terroraksjon [?]» (2013, s. 22).

5.3 Tilsvarende studie – samme resultat?

Som forsker må man være kritisk til sine funn (det ontologiske prinsipp). Hva som er «sannheten» kan endre seg som følge av revurderinger av egne og andres etablerte

[66] Ett av seks foreslåtte prioriterte hovedtemaer.
[67] Elektronisk unummerert artikkel.

forestillinger (Grønmo, 2004). Situasjonen kan også endre seg. Eksempelvis kan endringer i hvordan norske myndigheter skal bedrive sikkerhetsrådgivning føre til at svar på de samme spørsmålene jeg har benyttet meg av kan bli annerledes. En slik ulikhet i svarene kan da tilskrives endringer i det som gjøres i forhold til sikkerhetsrådgivning og ikke gjennomføringen av mine undersøkelser. Resultatet av undersøkelsene en har gjort er påvirket av konteksten undersøkelsen er gjennomført i og forskerens valg av metode og teori (det epistemologiske prinsipp). Forskerens forutinntatthet kan slik påvirke hva en ser etter og hvor en velger å fokusere.

Jeg kan ikke se at mine undersøkelser ikke skal kunne reproduseres av andre, men da med noen forbehold. For det første er mine funn knyttet til det utvalget jeg gjorde og oppgaven har ikke hatt som målsetning å bruke innsamlet data til generalisering. Når det er sagt mener jeg at jeg kan gi et bilde av hvordan sikkerhetsrådgivning bedrives av norske myndigheter overfor store norske bedrifter med virksomhet i utlandet. Reliabilitet er gjerne knyttet til muligheten til å reprodusere resultatene (Kvale et al., 2009, s. 250) og det vil her være mulig. For det andre er sikkerhetsrådgivning er et område som kan endre seg og det må man ta høyde for med tanke på en eventuell ny studie av det samme. For eksempel kan det tenkes at sikkerhetsrådgivning blir mer formalisert ved at det tydeliggjøres hvilke (n) myndighet (er) som skal ha dette ansvaret/oppgaven og overfor hvem det skal bedrives.

5.4 Videre forskning og utredning

I denne oppgaven som i andre dukker det opp områder en gjerne skulle sett nærmere på og undersøkt videre. Innledningsvis i arbeidsprosessen er gjerne problemstillinger å anse som vide og må derfor spisses og tilpasses det man ønsker å fremskaffe mer kunnskap om. Det kan være flere tema en ser at det kunne være interessant å studere mer inngående, og det er da det er nødvendig å holde «den røde tråden» og ikke «spore av». Å få lov til å foreslå og vise til områder en mener det er behov for å forske videre på kan derfor sies å være et privilegium når en ikke selv kan gjøre dette. I alle fall ikke i denne oppgaven. Oppgaven kan da være utgangspunkt for videre undersøkelser og ytterligere spørsmål knyttet til temaet enten det gjennomføres av en selv eller av andre. Det kan være tema en så vidt har vært

innom, det kan være tema som fortjener ytterligere undersøkelser og omtale, det kan være områder en ikke har berørt, eller kombinasjoner av dette.

Risikoforståelse og risikoerkjennelse er to begreper jeg har forklart innledningsvis i oppgaven. Gjennom arbeidet mitt ser jeg at det ville vært interessant å undersøke nærmere og analysert om sikkerhetsrådgivningen bidrar til økt risikoforståelse og –erkjennelse hos bedriftene ved å fokusere på aktuelle trusler og tiltak rettet mot truslene. Dette samsvarer også med - *Risiko, risikoforståelse og –erkjennelse* - som er et foreslått prioritert hovedtema i SAMRISK II (Programplanutvalget, 2013, s. 5). Dette er et interessant spørsmål fordi forståelse og erkjennelse av risiko øker evnen til å beskytte seg mot og håndtere aktuelle trusler. Spørsmålet (problemstillingen) kunne vært formulert slik som dette:

> Bidrar sikkerhetsrådgivningen fra myndighetene til økt risikoforståelse og risikoerkjennelse ved å fokusere på aktuelle trusler og tiltak rettet mot truslene?

En felles forståelse for begreper og situasjon er et godt (og kanskje nødvendig?) utgangspunkt for et vellykket samarbeid mellom myndigheter og bedrifter. Det har ikke kommet frem informasjon som tilsier at informantene stiller spørsmål ved informasjonen de får fra andre myndigheter eller bedrifter, men informantene er ikke spurt direkte om dette. Det er ikke trukket frem ved spørsmålene underveis i intervjuguiden, heller ikke ved spørsmålet «Er det noe du vil tilføye som jeg ikke har eller burde spurt om?» (appendiks nr. 1 og appendiks nr. 2). Standarden NS:5830 brukes blant annet av PST og UD ser i følge PST-hospitanten i UD[68] nærmere på metodebruk for deres ROS-analyser (risiko- og sårbarhetsanalyser), herunder hvordan en skal vektlegge sannsynligheten i en vurdering. PST-informanten understreker hvor vanskelig det er å si noe om sannsynligheten for tilsiktede hendelser. Han viser til ulik forståelse hos dem og Direktorat for samfunnssikkerhet og beredskap (DSB). Informanten henviser til Nasjonalt risikobilde 2013 der DSB har en matrise med sannsynlighet og konsekvens, noe som gjelder og passer bra for ulykker, men ikke for terror. Scenarioet terror var veldig lite sannsynlig, men med høy konsekvens. Når eksempelvis en direktør i et firma leser at terror har lav sannsynlighet da vil han gjerne ikke sikre seg mot det. Han understreker poenget med følgende uttalelse: «hvis han har noe som han vil beskytte som er veldig verdifullt for ham så bør han beskytte seg mot terror også

[68] Dette er ikke samme person som den nevnte PST-liaisonen. Den stillingen fylles av en annen person.

faktisk». Det som i In Amenas-rapporten kalles «low probability, high impact type of events» (Statoil ASA, 2013b, s. 52). Dette ville være et interessant område å undersøke videre. Her kan en også finne uenighet om hvem som skal drive med hvilke områder. PST-informanten mener at DSB ikke skal befatte seg med kontraterror, da det er andre fagmyndigheter som bør drive med det. Spørsmålet (problemstillingen) kunne vært formulert slik:

> Har norske myndigheter (og bedrifter?) tilsvarende forståelse av begrepene risiko/trusler/sårbarheter/verdier? Dersom nei, hvilken betydning har dette eventuelt for deres samarbeid?

I UDs evaluering kan vi lese at «PSTs hovedoppgave under krisehåndteringen var å søke å bringe klarhet i hvorvidt det var forbindelser mellom terrorangrepet i Algerie og personer i Norge, samt vurdere hvilke implikasjoner terrorangrepet kunne ha for det nasjonale trusselbildet» (Utenriksdepartementet, 2013, s. 28). I vår globaliserte verden er denne *overgangen* mellom Norge og utlandet interessant, og hvordan E og PST håndterer dette ville vært interessant å undersøke nærmere. Når tar eventuelt den andre tjenesten over «stafettpinnen» og hvilke muligheter er det for å formidle informasjon dem i mellom? Formidling av tidsriktig informasjon mellom PST og E, og analyse av terrortrusler mot norske interesser er blant FKS sine oppgaver (Bjørnland, 2014). Dette vil kunne påvirke sikkerhetsrådgivningen norske myndigheter bedriver overfor bedrifter. Dette ligger samtidig nært opp til utfordringen ved at myndigheter kan inneha informasjon de vet samarbeidspartnere ønsker, men ikke kan utveksle den pga. lov- og regelverk.

5.4 Betydning av funnene

Undersøkelsene mine er et bidrag til security-området innen samfunnssikkerhetsfeltet. Jeg har laget en definisjon av sikkerhetsrådgivning, et begrep jeg ikke har klart å finne noen definisjon på. Definisjonen jeg har utviklet kan sammen med mine funn danne utgangspunkt for videre forskning og undersøkelser. Det er enkelt å si seg enig i at norske myndigheter bør gjøre det de kan for å sikre norske bedrifters virksomhet i utlandet. Etter å ha gjennomført undersøkelsene mine er inntrykket at både myndighetene og bedriftene ønsker en mest

mulig velfungerende sikkerhetsrådgivning. Ressurser vil her som alltid være et av flere rammevilkår. En *samordnet* sikkerhetsrådgivning, om en kunne kalle det, med én ansvarlig og/eller koordinerende myndighet, kunne fange opp flere av utfordringene som er fremkommet i mitt datamateriale:

- Hvem er ansvarlig for sikkerhetsrådgivningen, hvordan skal det gjøres og overfor hvem?
- Formalisere kontakten mellom myndighetene knyttet til sikkerhetsrådgivningen, og avklare hvilken informasjon som kan deles og på hvilken måte.
- Ett kontaktpunkt der en kan henvende seg for denne typen rådgivning. Samtidig som en kan forutsette at en får den til enhver tid tilgjengelige og tidsriktige informasjon[69].

Sikkerhetsrådgivning bedrives av flere norske myndigheter, uten at det nødvendigvis blir korrekt å si at ansvaret er fordelt på flere myndigheter. Innen sivil beredskap har det «…langt på vei vært enighet om problemoppfatninger knyttet til fragmentering og manglende samordning, men samtidig har det vært betydelig uenighet om organisasjonsløsninger på feltet» (Fimreite et al., 2014, s. 37). Fraværet av en ansvarlig og/eller koordinerende myndighet når det gjelder sikkerhetsrådgivning gjør at dette feltet også har utfordringer knyttet til ansvar, sektortenkning, og samordning. Vertslandet har ansvaret for sikkerheten på sitt territorium, bedriftene har ansvar for sine ansatte i henhold til norsk lovgivning, og norske myndigheter bør tilstrebe å gi råd og formidle informasjon som kan benyttes av norske bedrifter med virksomhet i utlandet.

[69] Gradert informasjon vil naturligvis fortsatt holdes skjult, og bare kunne deles med de som er sikkerhetsklarert.

6. Litteraturliste

Aadland, C. (2014). - En hel organisasjon ble sterkt påvirket av angrepet i In Amenas. Sysla, 25. april 2014, from http://www.sysla.no/2014/04/25/oljeenergi/en-hel-organisasjon-ble-sterkt-pavirket-av-angrepet-i-in-amenas/

Agrell, W. (2005). *Förvarning och samhällshot*. Lund: Studentlitteratur.

Agrell, W., & Treverton, G. F. (2015). *National Intelligence and Science*. UK: Oxford University Press.

Ask, A. O. (2014). Privatsoldater dømt for massakre i rundkjøring. *Aftenposten, 24. oktober 2014*.

Bjørgo, T. (2005). *Root causes of terrorism: myths, reality and ways forward*. London: Routledge.

Bjørgo, T. (2014). Upublisert manuskript: How violent groups transform: A comparison of terrorism, organised crime and violent subcultures.

Bjørnland, B. (2014). Felles kontraterrorsenter. 5. juni 2014, from http://www.pst.no/blogg/felles-kontraterrorsenter/

Boin, A., & Smith, D. (2006). Terrorism and critical infrastructures: implications for public-private crisis management *In Public money & management* (Vol. 26(5), pp. 295-304). UK: Routledge.

Brenna, J. G., Norman, M. G., Jørstad, A., Sævereid, H. B., Jahren, A., Holm-Nilsen, S., & Byrkjedal, M. (2015). Dette er de terrormistenkte brødrene: Skal ha returnert fra Syria i sommer. *Verdens Gang*. from http://www.vg.no/nyheter/utenriks/terrorangrepet-mot-charlie-hebdo/dette-er-de-terrormistenkte-broedrene/a/23369724/

Dean, G., Fahsing, I. A., & Gottschalk, P. (2010). *Organized crime: policing illegal business entrepreneurialism*. Oxford: Oxford Univercity Press.

Den Nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora. (2006). *Forskningsetiske retningslinjer for samfunnsvitenskap, humaniora, juss og teologi*. Oslo: Forskningsetiske komiteer.

Dishman, C. (2005). The leadership nexus: When crime and terror converge (Vol. 28(3), pp. 237-252). Studies in conflict & terrorism.

Ege, R. T. (2015). Frykter at IS-pirater skal innta Middelhavet. Verdens Gang, 9. april 2015, from http://www.vg.no/nyheter/utenriks/is/frykter-at-is-pirater-skal-innta-middelhavet/a/23430821/

Ellingsen, E. B., & Zaman, K. (2006). Opprørt Stoltenberg ringte Pakistans statsminister. *Hentet 21. mars 2015*. http://www.vg.no/nyheter/utenriks/pakistan/opproert-stoltenberg-ringte-pakistans-statsminister/a/302302/

EOS-utvalget. (u.å.-a). EOS-tjenestene. Hentet 28. mars 2015, from http://eos-utvalget.no/norsk/tjenester/eos_tjenestene/

EOS-utvalget. (u.å.-b). Forsvarets sikkerhetsavdeling (FSA). Hentet 28. mars 2015, from http://eos-utvalget.no/norsk/tjenester/eos_tjenestene/forsvarets_sikkerhetsavdeling_fsa_/

Etterretningstjenesteloven. (1998). Lov om etterretningstjeneste av 20. mars 1998 nr. 5. https://lovdata.no/dokument/NL/lov/1998-03-20-11?q=lov+om+etterretningstjeneste

Etterretningstjenesten. (2014a). *Fokus 2014*.

Etterretningstjenesten. (2014b). Kontraterrorsenter i drift. Hentet 21. mars 2015, from http://forsvaret.no/aktuelt/arkiv/Kontraterrorsenter-i-drift

Etterretningstjenesten. (u.å.). Spørsmål og svar. Hentet 5. mars 2015, from http://forsvaret.no/fakta/organisasjon/Etterretningstjenesten/sporsmaal-og-svar

Etterretningstjenesten, Nasjonal sikkerhetsmyndighet, & Politiets sikkerhetstjeneste. (2013). *Trusler og sårbarheter 2013*. Departementenes servicesenter: Etterretningstjenesten, Nasjonal sikkerhetsmyndighet & Politiets sikkerhetstjeneste.

Fimreite, A. L., Langlo, P., Lægreid, P., & Rykkja, L. H. (2011). *Organisering, samfunnssikkerhet og krisehåndtering* (L. H. Rykkja Ed.). Oslo: Universitetsforlaget.

Fimreite, A. L., Langlo, P., Lægreid, P., & Rykkja, L. H. (2014). *Organisering, samfunnssikkerhet og krisehåndtering* (L. H. Rykkja Ed. 2. ed.). Oslo: Universitetsforlaget.

Fjelland, R. (1999). *Innføring i vitenskapsteori*. Oslo: Universitetsforlaget AS.

Forskningsrådet. (2011). Sluttrapport SAMRISK 2006-2011. Oslo: Norges forskningsråd.
Forsvaret. (2015). *Forsvarets årsrapport 2014: Verden i endring*. Oslo: Forsvaret.
Forsvarsbygg. (2014). *Forsvarsbygg årsrapport 2013*. Oslo: Forsvarsbygg.
Forsvarsbygg. (u.å.-a). *For et tryggere Norge*. Oslo: Kompetansesenter for sikring av bygg Forsvarsbygg.
Forsvarsbygg. (u.å.-b). Om Forsvarsbygg. Hentet 2. mars 2015, from http://www.forsvarsbygg.no/Om-Forsvarsbygg/
Gillham, B. (2005). *Research interviewing: the range of techniques*. Maidenhead: Open University Press.
Graf, C. (2013). Skremte bedrifter ber om terror-råd: Norske småbedrifter i utlandet kontakter myndighetene etter terrorangrepet i In Amenas. TV2.no, 31. januar 2013, from http://www.tv2.no/a/3978428
Grønmo, S. (2004). *Samfunnsvitenskapelige metoder*. Bergen: Fagbokforlaget.
Gundersen, D. (2009). Fedayeen. *Store norske leksikon*: Store norske leksikon.
Gundhus, H. I. (2009). *For sikkerhets skyld: IKT, yrkeskulturer og kunnskapsarbeid i politiet*. Oslo: Unipub.
Gundhus, H. O. (2005). Catching and targeting: Risk-based policing, local culture and gendered practices. *In Journal of Scandinavian studies in criminology and crime prevention* (Vol. 6(2), pp. 128-146).
Hansen, A. (2013). Kenyanske soldater har stormet Westgate. Dagbladet, 22. september 2013, from http://www.dagbladet.no/2013/09/22/nyheter/krig_og_konflikter/utenriks/terror/westgate/29405200/
Hegghammer, T. (2005). En oversikt over islamistiske terroristgrupper. In B. E. Rasch (Ed.), *Islamistisk terrorisme* (pp. 20-52). Oslo: Abstrakt forlag.
Hegghammer, T. (2013b). Should I stay or should I go? Explaning variation in western jihadists` choice between domestic and foreign fighting. *American political science review*.
Hoffman, B. (2006). *Inside terrorism*. New York: Columbia University Press.
Hovden, J. (1998). *Sikkerhetsforskning: en utredning for NFR*. Trondheim: NTNU.
Indregard, S. (2013). Kommentar: Spørsmålet er om vi ender opp med systemer som forutser forrige terroraksjon. *Morgenbladet*(22.-28. november 2013).
Instruks for Politiets sikkerhetstjeneste. (2005). Instruks for Politiets sikkerhetstjeneste av 19. august 2005. https://lovdata.no/dokument/INS/forskrift/2005-08-19-920?q=politiets+sikkerhetstjeneste
Instruks om Etterretningstjenesten. (2001). Instruks om Etterretningstjenesten av 31. august 2001. https://lovdata.no/dokument/INS/forskrift/2001-08-31-1012?q=instruks+om+etterretningstjeneste
Instruks om samarbeidet mellom E og PST. (2006). Instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste av 13. oktober 2006. https://lovdata.no/dokument/INS/forskrift/2006-10-13-1151?q=instruks+om+samarbeid+PST+og
Internkontrollforskriften. (1996). Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter av 6. desember 1996. https://lovdata.no/dokument/SF/forskrift/1996-12-06-1127?q=internkontrollforskriften
Iversen, B. (2006). Flere Telenor-butikker angrepet. *Bergensavisen, 14. februar 2006*. http://www.ba.no/nyheter/urix/article1954291.ece
Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser?: innføring i samfunnsvitenskapelig metode*. Kristiansand: Høyskoleforlaget.
Jakobsen, H. Ø. (2014). Et glimt av USA. *Morgenbladet, 25-31. juli 2014*.
Jarvis, L., & Holland, J. (2015). *Security: a critical introduction*. London: Palgrave Macmillan.
Johannessen, A., Tufte, P. A., & Christoffersen, L. (2010). *Introduksjon til samfunnsvitenskapelig metode*. Oslo: Abstrakt forlag.

Johansen, P. O. (1996). *Nettverk i gråsonen: et perspektiv på organisert kriminalitet*. Oslo: Ad notam Gyldendal.
Johnsen, A. B. (2014). Frankrike kuttet overvåkning av terror-brødrene. *Verdens Gang, 12. januar 2015*. http://www.vg.no/nyheter/utenriks/terrorangrepet-mot-charlie-hebdo/frankrike-kuttet-overvaakning-av-terror-broedrene/a/23372696/
Klassekampen. (2014). PST erkjenner at åpenhet om trusler er problematisk. *Klassekampen, 7. november 2014*. from http://www.klassekampen.no/article/20141107/NTBI/304864648
Kvale, S., Brinkmann, S., & Anderssen, T. M. R., Johan. (2009). *Det kvalitative forskningsintervju*. Oslo: Gyldendal akademisk.
Larsson, P. (2008). *Organisert kriminalitet*. Oslo: Pax.
Lia, B. (2005). *Globalisation and the future of terrorism: patterns and predictions*. London: Routledge.
Mathisen, P., & Høigaard, R. (2004). *Veiledningsmetodikk: en håndbok i praktisk veiledningsarbeid*. Kristiansand: Høyskoleforlaget.
Meld. St. 7 (2010-2011). (2010). *Kampen mot organisert kriminalitet: en felles innsats*. Oslo: Departementenes servicesenter.
Meld. St. 12 (2010-2011). (2011). *Bistand til nordmenn i utlandet*. Oslo: Departementenes servicesenter.
Meld. St. 21 (2012-2013). (2013). *Terrorberedskap: oppfølging av NOU 2012: 14 Rapport fra 22. juli-kommisjonen*. Oslo: Regjeringen.
Meld. St. 29 (2011-2012). (2012). *Samfunnssikkerhet*. Oslo: Regjeringen.
Mjaaland, O., & Wibe-lund, T. (2015). Derfor utfordrer soloterrorister Norge. *Verdens Gang, 17. februar 2015*. Hentet fra http://www.vg.no/nyheter/innenriks/terrorisme/derfor-utfordrer-soloterrorister-norge/a/23396801/
Nasjonal sikkerhetsmyndighet. (2009). *Veiledning i verdivurdering*. Kolsås: Nasjonal sikkerhetsmyndighet.
Nasjonal sikkerhetsmyndighet. (2010). *Veiledning i sikkerhetsadministrasjon*. Kolsås: Nasjonal sikkerhetsmyndighet.
Nasjonal sikkerhetsmyndighet. (2012). *Rapport om sikkerhetstilstanden 2012*. Kolsås: Nasjonal sikkerhetsmyndighet.
Nasjonal sikkerhetsmyndighet. (2014). *Sikkerhetstilstanden 2014*. Sandvika: Nasjonal sikkerhetsmyndighet.
Nasjonal sikkerhetsmyndighet. (2015). *Risiko 2015*. Sandvika: Nasjonal sikkerhetsmyndighet.
Nasjonal sikkerhetsmyndighet. (u.å.-a). *Kan du holde på en hemmelighet? [Brosjyre]*. Oslo: Nasjonal sikkerhetsmyndighet.
Nasjonal sikkerhetsmyndighet. (u.å.-b). Om NSM. Hentet 28. mars 2015, from http://www.nsm.stat.no/om-nsm/
Nasjonal sikkerhetsmyndighet, Politidirektoratet, & Politiets sikkerhetstjeneste. (2010). *En veiledning: Sikkerhets- og beredskapstiltak mot terrorhandlinger*. Oslo: Nasjonal sikkerhetsmyndighet, Politidirektoratet, Politiets sikkerhetstjeneste.
Norges Rederiforbund. (u.å.). Fortsatt behov for piratbekjempelse. Hentet 12. februar 2015, from http://www.rederi.no/nrweb/cms.nsf/%28$All%29/3B192BE5240FFD95C1257C5B00302A21
NOU 2000:24. (2000). *Et Sårbart samfunn: Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Oslo: Departementenes servicesenter, Informasjonsforvaltning.
NOU 2006:6. (2006). *Når sikkerheten er viktigst*. Oslo: Departementenes servicesenter, Informasjonsforvaltning.
NOU 2012:14. (2012). *Rapport fra 22. juli-kommisjonen*. Oslo: Departementenes servicesenter, Informasjonsforvaltning.
NRK. (2014). Terrorangrepet i In Aménas: Har plikt til å varsle. http://www.nrk.no/nyheter/1.11746299
Nærings- og Handelsdepartementet. (2003). *Kartlegging og utredning av former for offentlig privat samarbeid (OPS): - en KPMG-rapport til Nærings- og Handelsdepartementet*. Oslo: Nærings- og Handelsdepartementet.

Næringslivets sikkerhetsråd. (2011a). *Bakgrunnssjekk: en brukerveiledning*. Oslo: Næringslivets sikkerhetsråd.
Næringslivets sikkerhetsråd. (2011b). *En orientering om tiger kidnapping: Er du eller din virksomhet et attraktivt mål?* Oslo: Næringslivets sikkerhetsråd.
Næringslivets sikkerhetsråd. (2011c). *Veileder for vurdering av sikkerhetsrisiko ved etablering i utlandet*. Oslo: Næringslivets sikkerhetsråd.
Næringslivets sikkerhetsråd. (u.å.-a). Grenseløse utfordringer (NSRs utvalg for internasjonale sikkerhetsutfordringer). Hentet 10. februar 2015, from http://www.nsr-org.no/utvalg/grenseloese-utfordringer-nsrs-utvalg-for-internasjonale-sikkerhetsutfordringer-article143-134.html
Næringslivets sikkerhetsråd. (u.å.-b). Om NSR. Hentet 28. mars 2015, from http://www.nsr-org.no/om-nsr/
Næringslivets sikkerhetsråd. (u.å.-c). Spisskompetanse. Hentet 12. februar 2015, from http://www.nsr-org.no/utvalg/
Organization for Security and Co-operation in Europe. (u.å.). Public-private partnerships. from http://www.osce.org/atu/44852
Politiets sikkerhetstjeneste. (2007). *Politiets sikkerhetstjeneste: oppgaver og virksomhet*. Oslo: Politiets sikkerhetstjeneste.
Politiets sikkerhetstjeneste. (2012). *Åpen trusselvurdering 2012*. Oslo: Politiet sikkerhetstjeneste.
Politiets sikkerhetstjeneste. (2013). *Åpen trusselvurdering 2013*. Oslo: Politiets sikkerhetstjeneste.
Politiets sikkerhetstjeneste. (2014). *Åpen trusselvurdering 2014*. Oslo: Politiets sikkerhetstjeneste.
Politiets sikkerhetstjeneste. (2015). *Åpen trusselvurdering 2015*. Oslo: Politiets sikkerhetstjeneste.
Politiets sikkerhetstjeneste. (u.å.). Tryggleiksrådgivning. Hentet 4. februar 2015, from http://www.pst.no/oppgaver/tryggleiksradgiving/
Politiloven. (1995). Lov om politiet av 1. oktober 1995 nr. 16. https://lovdata.no/dokument/NL/lov/1995-08-04-53?q=politiloven
Programplanutvalget. (2013). Program for samfunnssikkerhet (SAMRISK II).
Rasch, B. E. (2005). Innledning. In B. E. Rasch (Ed.), *Islamistisk terrorisme* (pp. 9-19). Oslo: Abstrakt forlag.
Ravndal, D. (2009). Taliban-terrorister skulle angripe Telenor. *Verdens Gang, 24. august 2009*. Hentet 15. mars 2014, from http://www.vg.no/nyheter/utenriks/artikkel.php?artid=570758
Romarheim, A. G. (2012). Terrorismens tiår. *Internasjonal politikk, 2012(1)*.
Ruyter, K. W. (2003). Forskningsetikkens spede begynnelse og tilblivelse: beskyttelse av enkeltpersoner og samfunn. In K. W. Ruyter (Ed.), *Forskningsetikk: beskyttelse av enkeltpersoner og samfunn* (pp. 17-38). Oslo: Gyldendal akademisk.
Schmid, A. P. (2011). *The Routledge handbook of terrorism research*. London: Routledge.
Sikkerhetsloven. (1998). Lov om forebyggende sikkerhetstjeneste av 20. mars 2001. https://lovdata.no/dokument/NL/lov/1998-03-20-10?q=sikkerhetsloven
Simonsen, A. R. (2015a). Flere næringslivskontakter i politiet. *14. januar 2015*. from http://www.nsr-org.no/aktuelle-saker/flere-naeringslivskontakter-i-politiet-article568-110.html
Simonsen, A. R. (2015b). Sikkerhetsforum for norske internasjonale virksomheter. *18. mars 2015*. from http://www.nsr-org.no/aktuelle-saker/sikkerhetsforum-for-norske-internasjonale-virksomheter-article614-110.html
Spaaij, R. (2012). *Understanding lone wolf terrorism: global patterns, motivations and prevention*. Dordrecht: Springer.
Standard Norge. (2012). *Samfunnssikkerhet: beskyttelse mot tilsiktede uønskede handlinger: terminologi*. Lysaker: Standard Norge.
Statoil ASA. (2013a). Angrepet mot In Amenas: Norsk oversettelse av kapittel 1 (sammendrag): Statoil ASA.
Statoil ASA. (2013b). The In Amenas Attack: Statoil ASA.
Statoil ASA. (u.å.). Vår historie. Hentet 29. mars 2015, from http://www.statoil.com/no/about/history/pages/ourhistory.aspx

Steensæth, Y., Hellesøy, O. H., Skogstad, A., & Einarsen, S. (2000). *Det Gode arbeidsmiljø: krav og utfordringer : et festskrift til Odd H. Hellesøy* (A. Skogstad & S. Einarsen Eds.). Bergen: Fagbokforlaget.

Steiro, G. (2013). Opplagte terrormål. *Bergens Tidende, 13. september 2013*.

Stensvand, E. (2013). Sikkerhet som salsvare. *Hubro, 2(2013)*, 40-41.

Straffeloven. (1992). Almindelig borgerlig straffelov av 22. mai 1992. (Hentet 15. mars 2015). https://lovdata.no/dokument/NL/lov/1902-05-22-10?q=straffeloven

Strand, T. (2013). Frykter terror mot Statoil-anlegg: Forsvaret advarer Statoil om at det er en terrorfare mot selskapets kontorer og landanlegg. *Bergens Tidende, 14. september 2013*.

Sætre, S. (2015). - Hemmeligheter er en trussel mot demokratiet. *Morgenbladet, 2-8. januar 2015*.

Taghavi, M. (2010). Preparing against future terror attacks? A case of large UK firms. *International Journal of Arts and Sciences, 3(15)*, 381-393.

Telenor Group. (u.å.). Vår virksomhet - en verden av kommunikasjon. Hentet 29. mars 2015, from http://www.telenor.com/no/om-oss/var-virksomhet/

Thagaard, T. (2009). *Systematikk og innlevelse : en innføring i kvalitativ metode* (3. ed.). Bergen: Fagbokforlaget.

The Geneva Centre for the Democratic Control of Armed Forces. (u.å.). What is DCAF? , Hentet 17. mars 2015, from http://www.dcaf.ch/About-Us

The U.S. State Department`s Overseas Security Advisory Council. (u.å.). About OSAC. Hentet 17. mars 2015, from https://www.osac.gov/Pages/AboutUs.aspx

Tønnesen, T. H. (2008). Muhammad-karikaturene som motiv for terroranslag: En oppdatering. Foredrag 11. juni 2008, NUPI. *Forsvarets Forskningsinstitutt,* (hentet 12.10.2014). http://www.ffi.no/ny/Prosjekt/Terra/Publikasjoner/Documents/Muhammad_karikaturene_Foredrag.pdf

United States. (2004). *Patterns of Global Terrorism 2003*. Retrieved from http://www.state.gov/documents/organization/31912.pdf.

Utenriksdepartementet. (2013). *Terrorangrepet på gassproduksjonsanlegget i In Amenas: Evaluering av norske myndigheters krisehåndtering*. Oslo: Utenriksdepartementet.

Utenrikstjenesteloven. (2002). Lov om utenrikstjensten av 1. september 2002. https://lovdata.no/dokument/NL/lov/2002-05-03-13?q=lov+om+utenrikstjeneste

Vaaland, T. Ø. (2012). Refseren: tidligere statsminister Kåre Willoch mener etterpåklokskapen er bedre enn ingen klokskap. *Morgenbladet, 3-9. august 2012*. from http://morgenbladet.no/samfunn/2012/refseren#.VTck1pOK-fw

Veum, E., & Olsson, S. V. (2013). E-tjenesten: - Økende trussel for norske selskaper. Hentet 22. august 2014, from http://www.nrk.no/verden/okende-trussel-for-norske-selskaper-1.10900906

Vikøren, B. M. (u.å.). Joint venture. *Store norske leksikon*. Hentet 15. mars 2014, from http://snl.no/joint_venture

Wermdalen, H., & Nilsson, K. (2013). *Säkerhetsboken*. Stockholm: Security Manager.

Østensen, Å. G. (2011a). In from the cold? Self-legitimating the market for private security. *23, No. 3*.

Østensen, Å. G. (2011b). *UN Use of private military and security companies: Practices and policies*. Genève: DCAF.

7. Appendiks

7.1 Appendiks nr. 1: Intervjuguide myndigheter

I denne masteroppgaven vil jeg se på hvordan norske myndigheter bedriver sikkerhetsrådgivning (formidler sikkerhetsråd). Hvordan og gjennom hvem yter norske myndigheter denne sikkerhetsrådgivningen, og hvordan formidles dette til bedriftene? Hva slags trusler er det fokus på i denne eventuelle rådgivningen? Hva får bedriftene ut av denne informasjonen, og hvem går bedriftene til for å innhente informasjon på eget initiativ?

Nærmere bestemt: Hvordan bedriver norske myndigheter sikkerhetsrådgivning til større norske bedrifter med næringsvirksomhet i utlandet, med tanke på at de skal bli bedre rustet mot den trusselen terrorister og/eller tilsvarende andre ondsinnede aktører kan representere. Bidrar myndighetenes sikkerhetsrådgivning til risikoforståelse og risikoerkjennelse? I hvilken grad har ulike hendelser påvirket bedriftenes sikkerhetsmessige bevissthet, og utveksler de og myndighetene på noen måte erfaringer til vanlig og etter spesielle hendelser?

Informasjon/formaliteter

Samtykke: Frivillig deltakelse med mulighet til å trekke seg på et hvilket som helst tidspunkt.

Anonymitet: Det er kjent hvilke offentlige myndigheter og bedrifter jeg prater med. I utgangspunktet åpenhet om hvem jeg intervjuer. Personnavn kan holdes anonyme, men arbeidssted holdes kjent.

Lydopptak: Spørre om informanten tillater bruk av lydopptak under intervjuet. Ønsker informanten å lese gjennom resymeet før bruk? Eventuelt bare direkte sitater? Lydopptakene og resyme destrueres etter at masteroppgaven er sensurert.

Innledning

1. Gir dere sikkerhetsråd, og hvorfor gir dere slike råd?
    a. Hva er hjemmelen til dette?
    b. Hvilken betydning legger dere i sikkerhetsrådgivning?
    c. Hvordan bedriver dere sikkerhetsrådgivning?
    d. Hvilke trusler fokuseres det på i rådgivningen?
    e. Produserer dere rådgivende materiell (veiledere etc.) som bedriftene kan nyttiggjøre seg av?

Informasjonsutveksling og samarbeid

2. Hvordan deles informasjon mellom myndighetene og bedriftene, og hvordan syns dere dette fungerer?
    a. Hvem eller hva initierer kontakten?
2. Mottar dere informasjon fra andre norske myndigheter (eller utenlandske) som dere videreformidler eller benytter dere av ved sikkerhetsrådgivningen?
    a. Hvordan fungerer denne informasjonsutvekslingen?
    b. Hvorfor formidler dere informasjon i stedet for at informasjonen gis direkte fra dem?
3. Gir dere informasjon til andre myndigheter i forbindelse med sikkerhetsrådgivning?
    a. I så fall, hvorfor gir dere ikke informasjonen direkte til bedriftene?
4. Er det utfordringer ved informasjonsutvekslingen mellom myndighetene eller mellom myndighetene og bedriftene, i så fall hvilke?
5. Er det noen dere ønsker å samarbeide med som dere ikke samarbeider med i dag, i så fall hvem og hvorfor?
    a. Er det noen som vil samarbeide med dere som dere ikke har samarbeid med?
6. Er det noe dere ønsker å endre i denne forbindelse og hvorfor?

Risiko- og trusselforståelse

7. Hvilken definisjon har dere av risiko, trussel og sårbarhet?

Før og etter terrorangrepet 22. juli

8. Har terrorangrepet 22. juli og den etterfølgende Gjørv-rapporten ført til endringer i deres syn på og måten dere utøver sikkerhetsrådgivning? Hvorfor/hvorfor ikke?

Før og etter terrorangrepet i In Amenas

9. Har terrorangrepet mot In Amenas og den etterfølgende evalueringsrapporten ført til endringer i deres syn på og måten dere utøver sikkerhetsrådgivning? Hvorfor/hvorfor ikke?
10. Kan du si noe om de to overnevnte hendelsene har medført ulik påvirkning på sikkerhetsrådgivningen?

Avsluttende spørsmål

11. Er det noe du vil tilføye som jeg ikke har eller burde spurt om?

Avslutning

Takke for at informanten tok seg tid til intervjuet.

Gjenta avtalen en inngikk ved starten av intervjuet vedrørende anonymitet, bruk av materialet (tilgjengelig resyme til gjennomlesning/sitatsjekk) og frivillighet. Lydopptaket og det skriftlige destrueres etter sensur på oppgaven.

Spørre om det er ok med eventuelle oppklarende spørsmål fra meg i ettertid om det skulle bli behov for det pr e-post eller telefon.

Oppfølgingsspørsmål sendt ut i etterkant pr e-post:

12. Har anslagene mot Telenors butikker i Pakistan i 2005 ført til endringer i sikkerhetsrådgivningen dere gir til store norske bedrifter med virksomhet i utlandet og dialogen med dem? Hvis ja, forklar på hvilken måte.

13. Har anslaget mot den norske ambassaden i Damaskus i 2006 ført til endringer i sikkerhetsrådgivningen dere gir til store norske bedrifter med virksomhet i utlandet og dialogen med dem? Hvis ja, forklar på hvilken måte.
14. Har piratkapringer de siste årene i Adenbukta og omkringliggende områder, mot norsk og utenlandsk skipsfart, ført til endringer i sikkerhetsrådgivningen dere gir til store norske bedrifter med virksomhet i utlandet og dialogen med dem? Hvis ja, forklar på hvilken måte.

7. 2 Appendiks 2: Intervjuguide bedrifter

I denne masteroppgaven vil jeg se på hvordan norske myndigheter bedriver sikkerhetsrådgivning (formidler sikkerhetsråd). Hvordan og gjennom hvem yter norske myndigheter denne sikkerhetsrådgivningen, og hvordan formidles dette til bedriftene? Hva slags trusler er det fokus på i denne eventuelle rådgivningen? Hva får bedriftene ut av denne informasjonen, og hvem går bedriftene til for å innhente informasjon på eget initiativ?

Nærmere bestemt: Hvordan bedriver norske myndigheter sikkerhetsrådgivning til større norske bedrifter med næringsvirksomhet i utlandet, med tanke på at de skal bli bedre rustet mot den trusselen terrorister og/eller tilsvarende andre ondsinnede aktører kan representere. Bidrar myndighetenes sikkerhetsrådgivning til risikoforståelse og risikoerkjennelse? I hvilken grad har ulike hendelser påvirket bedriftenes sikkerhetsmessige bevissthet, og utveksler de og myndighetene på noen måte erfaringer til vanlig og etter spesielle hendelser?

Informasjon/formaliteter

Samtykke: Frivillig deltakelse med mulighet til å trekke seg på et hvilket som helst tidspunkt.

Anonymitet: Det er kjent hvilke offentlige myndigheter og bedrifter jeg prater med. I utgangspunktet åpenhet om hvem jeg intervjuer. Personnavn kan holdes anonyme, men arbeidssted holdes kjent.

Lydopptak: Spørre om informanten tillater bruk av lydopptak under intervjuet. Ønsker informanten å lese gjennom resymeet før bruk? Eventuelt bare direkte sitater? Lydopptakene og resyme destrueres etter at masteroppgaven er sensurert.

Innledning

1. Mottar dere sikkerhetsrådgivning?
2. Kan du si hvorfor dere eventuelt mottar sikkerhetsråd?
3. Hvordan mottar dere sikkerhetsrådgivning?

4. Hvem mottar dere sikkerhetsrådgivning fra?
    a. Har dere kontaktperson (er) hos de (myndighetene eller andre) dere får sikkerhetsrådgivning fra?
    b. Får dere rådgivning i fellesskap med andre bedrifter eller via andre bedrifter?
5. Hvilken betydning legger dere i sikkerhetsrådgivning?
6. Hvilke trusler fokuseres det på i rådgivningen?
7. Nyttiggjør dere dere av rådgivende materiell fra norske myndigheter eller andre, og eventuelt hvordan?
8. Hva får dere ut av denne sikkerhetsrådgivningen/informasjonen?
9. Hvem henvender dere dere til dersom dere innhenter informasjon på eget initiativ?

Informasjonsutveksling og samarbeid

10. Er det noen dere ønsker å ha kontakt med i forbindelse med sikkerhetsrådgivning som dere ikke har kontakt med i dag, i så fall hvem og hvorfor?
    a. Er det noen som vil ha kontakt med dere i denne sammenhengen som dere ikke har kontakt med i dag?
11. Er det utfordringer ved informasjonsutvekslingen mellom myndighetene og dere, i så fall hvilke?
12. Hvordan deles informasjon mellom aktørene og hvordan syns dere dette fungerer?
13. Er det noe dere ønsker å endre i denne forbindelse og hvorfor?

Risiko og trusselforståelse

14. Hvilken definisjon har dere av risiko, trussel og sårbarhet?
15. Er det en reell risikoerkjennelse når risiko, sårbarhet og trusler omtales i rapporter/dokumenter dere benytter dere av?
16. Påvirker sikkerhetsrådgivningen dere mottar bedriftens risikoforståelse og risikoerkjennelse, og hvis ja på hvilken måte?

Før og etter terrorangrepet 22. juli

17. Har terrorangrepet 22. juli og den etterfølgende Gjørv-rapporten ført til endringer i bedriftens syn på og benyttelse av sikkerhetsrådgivning fra norske myndigheter eller andre? Hvorfor/hvorfor ikke?

Før og etter terrorangrepet i In Amenas

18. Har terrorangrepet mot In Amenas og den etterfølgende evalueringsrapporten ført til endringer i bedriftens arbeid med og syn på og benyttelse av sikkerhetsrådgivning fra norske myndigheter eller andre? Hvorfor/hvorfor ikke?
19. Kan du si noe om de to overnevnte hendelsene har medført ulik påvirkning på sikkerhetsrådgivningen dere mottar?

Avsluttende spørsmål

20. Er det noe du vil tilføye som jeg ikke har eller burde spurt om?

Avslutning

Takke for at informanten tok seg tid til intervjuet.

Gjenta avtalen en inngikk ved starten av intervjuet vedrørende anonymitet, bruk av materialet (tilgjengelig resyme til gjennomlesning/sitatsjekk) og frivillighet. Lydopptaket og det skriftlige destrueres etter sensur på oppgaven.

Spørre om det er ok med eventuelle oppklarende spørsmål fra meg i ettertid om det skulle bli behov for det pr e-post eller telefon.

Oppfølgingsspørsmål sendt ut i etterkant pr e-post:

21. Har anslagene mot Telenors butikker i Pakistan i 2005 ført til endringer i sikkerhetsrådgivningen dere mottok/mottar fra norske myndigheter og dialogen med dem (Næringslivets Sikkerhetsråd (NSR) inkludert)? Hvis ja, forklar på hvilken måte.

22. Har anslaget mot den norske ambassaden i Damaskus i 2006 ført til endringer i sikkerhetsrådgivningen dere mottok/mottar fra norske myndigheter og dialogen med dem (NSR inkludert)? Hvis ja, forklar på hvilken måte.
23. Har piratkapringer de siste årene i Adenbukta og omkringliggende områder, mot norsk og utenlandsk skipsfart, ført til endringer i sikkerhetsrådgivningen dere mottok/mottar fra norske myndigheter og dialogen med dem (NSR inkludert)? Hvis ja, forklar på hvilken måte.

Antall ord: 34 016 (kun oppgaveteksten)