FFI-rapport 2014/00948

Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet

Ingvill Moe Elgsaas og Hege Schultz Heireng

FFI Forsvarets forskningsinstitutt

Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet

Ingvill Moe Elgsaas og Hege Schultz Heireng

Forsvarets forskningsinstitutt (FFI)

4. september 2014

FFI-rapport 2014/00948

Oppdrag 388301

P: ISBN 978-82-464-2424-8
E: ISBN 978-82-464-2425-5

Emneord

Forebyggende sikkerhet

Sikkerhetsloven

Årsaker

Sikkerhetstilstanden

Nasjonal sikkerhetsmyndighet

Godkjent av

Monica Endregard	Prosjektleder
Janet Martha Blatny	Avdelingssjef

Sammendrag

Nasjonal sikkerhetsmyndighet (NSM) har i en årrekke rapportert at Norges sikkerhetstilstand er lite tilfredsstillende, og i de senere år har gapet mellom truslene vi står overfor og tiltakene som er ment å beskytte oss mot dem økt. Denne rapporten kartlegger og vurderer årsakene til at norske virksomheter ikke ivaretar den forebyggende sikkerheten på en tilfredsstillende måte. En bedre forståelse av årsakene kan bidra til å styrke virksomhetenes oppfølging av eget sikkerhetsarbeid, og derav samfunnets totale evne til å oppdage og reagere på sårbarheter og sikkerhetstruende hendelser.

Det har blitt gjennomført en håndfull delanalyser, designet for å ta høyde for at årsaker konseptualiseres og presenteres ulikt i forskjellige kretser. Eksempelvis, den faglige debatten om det forebyggende sikkerhetsarbeidet kan tenkes å avvike fra den allmenntilgjengelige debatten i media. Viktige kilder inkluderer NSMs rapporter om sikkerhetstilstanden, og et utvalg av tilsynsrapporter som beskriver avvik og observasjoner NSM har avdekket gjennom sin tilsynsvirksomhet. Prosjektets medarbeidere har også deltatt på tilsyn som observatører for å samle inn empiri til denne studien. I tillegg har vi gjennomført intervjuer med relevante aktører. Det har videre blitt gjennomført en medieanalyse av i overkant av 200 nyhetssaker for å fange opp mediedebatten rundt forebyggende sikkerhet. Til slutt har det blitt gjennomført en analyse av forholdet mellom sektorovergripende lovgivning for forebyggende sikkerhet (sikkerhetsloven) og sektorspesifikt lovverk innen samme tema. Som metodisk fremgangsmåte har dokumentanalyse og kvalitativ innholdsanalyse blitt benyttet i de totalt fem delanalysene.

For å bedre det forebyggende sikkerhetsarbeidet på en helhetlig og hensiktsmessig måte må norske virksomheter arbeide både kortsiktig og langsiktig med å bedre sikkerheten. På den ene siden bør det fokuseres på det området hvor vi faktisk kan utgjøre en forskjell på *kort sikt*. Eksempelvis bør det fokuseres mer på dokumentasjon av det forebyggende sikkerhetsarbeidet, for å sikre etterprøvbarhet og bevare kontinuiteten i sikkerhetsarbeidet når kritisk sikkerhetspersonell skiftes ut. Det bør også innarbeides bedre rutiner for rapportering og håndtering av sikkerhetstruende hendelser, gjennomføres øvelser innen forebyggende sikkerhet, arbeides for å øke ansattes forståelse om viktigheten av sikkerhetsklarering og autorisasjonssamtaler, og utvikle rutiner for å sikre kontinuerlig kontrollaktivitet i virksomheten. Slike tiltak kan på kort sikt styrke sikkerhetstilstanden i de fleste virksomheter underlagt sikkerhetsloven.

Samtidig må det arbeides *langsiktig* med å rette opp i fundamentale årsaker, som for eksempel å bedre «sikkerhetskulturen» i virksomheten. Men det ligger i selve begrepet «kultur» at dette ikke er noe som kan endres raskt på. Ledere må engasjere seg mer i sikkerhetsarbeidet og ha tettere dialog med sikkerhetsorganisasjonen. Dette er helt avgjørende for å sikre at det bevilges ressurser som tar høyde for det aktuelle risikobildet. Økt fokus på sikkerhet på ledelsesnivå kan dessuten bidra positivt ved å øke sikkerhetsbevisstheten i virksomheten totalt sett. Det sentrale fremover blir å se årsakskompleksiteten som en helhet og tillegge alle områdene tilstrekkelig vekt.

English summary

The Norwegian National Security Authority (NSM) has for several years reported that the state of affairs in Norway's security systems is unsatisfactory. In latter years, the gap between security threats and the protective security measures aiming to protect our society has increased. This report sets out to chart the underlying causes why Norwegian state agencies and companies fail to safeguard their protective security. The end goal is to contribute towards Norwegian companies' improved efforts to safeguard their own protective security, and, in turn, to make a contribution towards betterment of Norwegian society's overall ability to detect vulnerabilities and adequately respond to security threats.

We have carried out a number of analyses designed to account for the complexity of underlying causes, which may well be conceptualised and presented differently in various milieus (e.g. the academic debate on protective security vs. media coverage). Important sources for this study include annual reports on the state of affairs in Norway's security systems published by the NSM and a selection of reports from NSMs inspection activities that relay the state of protective security measures in the agencies and companies in question. The researchers have also observed inspections as a source of further empirical evidence for current project. This has been supplemented with semi-structured interviews. The project also included a media analysis of upwards of 200 relevant news stories. Finally, the project also compared the Norwegian Security Act (Law on the Protective Security Services) and laws that regulate protective security in specific sectors.

Norwegian state agencies and companies must undertake both short- and long-term measures to improve their protective security in a comprehensive and timely manner. On the one hand, focus should be directed on areas where security measures can make differences in *the short term*. For example, documentation of protective security measures will ensure verifiability and continuity when key security personnel leave. Other measures that should be established include better procedures for reporting and dealing with security-threatening events, exercises to test their security plans, and efforts to improve employee understanding of the importance of security clearance and authorization. In addition, the agencies and companies should also adequately control and revise their protective security system. These measures should strengthen the security systems in most agencies and companies subject to the Norwegian Security Act in the short term.

Simultaneously, *long-term* work must be done to correct the fundamental causes of the unsatisfactory security systems, such as improving the «security culture» in agencies and companies. However, the very concept of «culture» cannot be changed quickly. Leaders should be more involved in safeguarding the protective security, and cooperate closely with the security organization. This is essential to ensure that resources are distributed according to the needs of the risk situation. Involving leaders can also contribute positively, by increasing security awareness overall. Going forward, the key will be to see the causal complexity as a whole and ensure sufficient coverage of all areas.

Innhold

Forord

Denne rapporten er en del av forskningsprosjektet «Sikkerhetstilstanden – årsaker, konsekvenser og virkemidler» (SÅKOV). SÅKOV-prosjektet består av i alt fire delaktiviteter som tar for seg forskjellige problemstillinger knyttet til sikkerhetstilstanden i Norge. Forsvarsdepartementet (FD) ga Nasjonal sikkerhetsmyndighet (NSM) i oppdrag å gjennomføre SÅKOV-prosjektet, og NSM har inngått samarbeid med Forsvarets forskningsinstitutt (FFI) om gjennomføringen av prosjektets første delaktivitet. Første aktivitet kartlegger «Årsaker til mangelfull sikkerhetstilstand» (ÅMS) og ble i hovedsak gjennomført i perioden oktober 2012-desember 2013. Rapporten presenterer relevante funn og forslag til videre arbeid for å bedre sikkerhetstilstanden i Norge. Forfatterne retter en stor takk til alle intervjuobjekter og virksomheter som har bidratt med verdifullt datamateriale og til NSM for tilrettelegging og oversendelse av relevant dokumentasjon.

Hege Schultz Heireng og Ingvill Moe Elgsaas

Kjeller, juni 2014

1 Innledning

Nasjonal sikkerhetsmyndighet (NSM) har i en årrekke rapportert at Norges sikkerhetstilstand er utilfredsstillende. I de senere år har NSM også observert at gapet mellom truslene vi står overfor og tiltakene som er ment å beskytte oss mot dem øker.[1] På bakgrunn av denne utviklingen er det utformet et prosjekt som tar for seg forskjellige problemstillinger knyttet til sikkerhetstilstanden: «Sikkerhetstilstanden – årsaker, konsekvenser og virkemidler» (SÅKOV). SÅKOV-prosjektet har som mål å styrke virksomhetenes oppfølging av eget sikkerhetsarbeid slik at de kan forbedre den generelle sikkerhetstilstanden på en helhetlig og hensiktsmessig måte og derved styrke samfunnets evne til å oppdage og reagere på sårbarheter og sikkerhetstruende hendelser. Denne studien presenterer SÅKOV-prosjektets første aktivitet: «Årsaker til mangelfull sikkerhetstilstand» (ÅMS).[2]

Bakgrunnen for denne studien er direkte knyttet til sikkerhetstilstanden. I det som følger vil vi derfor introdusere sikkerhetstilstanden (del 1.1) ved å definere hva som menes med begrepet «sikkerhetstilstand» (del 1.1.1) før vi presenterer hvordan Norges sikkerhetstilstand er blitt vurdert de siste årene (del 1.1.2). Deretter følger en presentasjon av forskningsdesign (del 1.2) og kilder (del 1.3). I kapittel 2 presenterer vi regelverket for og organisasjonen av det forebyggende sikkerhetsarbeidet hhv. del 2.1 og 2.2. Lesere som allerede er kjent med denne tematikken henvises direkte til analysedelen i kapittel 3 og 4. Kapittel 3 presenterer analysefunnene med fokus på årsaker som gjør seg gjeldende i mange virksomheter og som, ved utbedring, kan ha en betydelig innvirkning på sikkerhetstilstanden generelt så vel som i den enkelte virksomhet. Kapittel 4 konkluderer og gir anbefalinger om hvordan norske virksomheter kan arbeide kortsiktig og langsiktig med å bedre sikkerhetstilstanden.

1.1 Sikkerhetstilstanden

1.1.1 Risikobildet og forebyggende sikkerhet

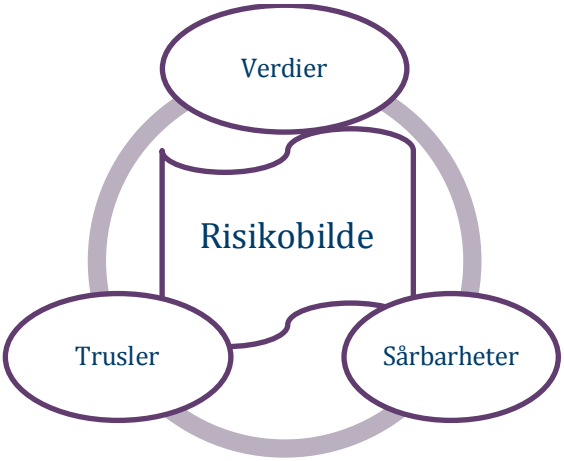
Først kan det være nyttig å presentere de mest sentrale definisjonene innen fagfeltet. *Sikkerhetstilstand* er et sammensatt begrep som består av to hovedkomponenter: *risikobilde og forebyggende sikkerhet*. Vi vil her introdusere disse to komponentene og deres bestanddeler.

[1] Se blant annet: Rapport om sikkerhetstilstanden 2012 (NSM 2012) og Rapport om sikkerhetstilstanden 2011 (NSM 2011). Se for øvrig del 1.1.2 for en oppsummerende diskusjon av NSMs rapporter om sikkerhetstilstanden fra 2003-2012.

[2] SÅKOV-prosjektet består av i alt fire delaktiviteter. Delaktivitet I omhandler «Årsaker til mangelfull sikkerhetstilstand (ÅMS)», delaktivitet II vurderer «Hva mangelfull forebyggende sikkerhet koster samfunnet (SIKKOST)», delaktivitet III vurderer «Verktøy som kan bidra til å øke sikkerhetsbevisstheten (VERKØRS)», og delaktivitet IV ser på «Veileder i sikkerhetsadministrasjon (VESI)».

Ifølge Norsk Standard[3] kan *risikobilde* defineres som en «tidsbegrenset beskrivelse av en entitets risiko».[4] Selv om standarden oppgir innledningsvis at *entitet* her brukes som et samlebegrep (fysisk objekt, et individ, en organisasjon, en stat osv.) kreves ytterligere definisjoner for å belyse hovedkomponenten i risikobilde, nemlig «risiko». Norsk Standard definerer *risiko* som «forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet ovenfor den spesifiserte trusselen».[5] Denne definisjonen drar frem tre viktige komponenter: «trussel», «verdi» og «sårbarhet». En *trussel* defineres som en «mulig uønsket handling som kan gi negativ konsekvens for en entitets sikkerhet».[6] *Verdi* defineres som en «ressurs» som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen».[7] *Sårbarhet* defineres som «manglende evne til å motstå en uønsket hendelse eller å opprette en ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning».[8]

Med andre ord, *Norges risikobilde er en tidsbegrenset beskrivelse av forholdet mellom samfunnets verdier, trusler mot dem og verdienes sårbarheter ovenfor disse truslene i en gitt periode.* Forholdet mellom verdier, trusler og sårbarheter refereres til som «risikotrekanten» (Figur 1.1. nedenfor) og brukes i dag som rammeverk for NSMs vurderinger av Norges risikobilde opp mot deres årlige vurdering av sikkerhetstilstanden.[9]



Figur 1.1 Risikobilde: Verdier, trusler og sårbarheter.

[3] NSMs foreløpig siste rapport om sikkerhetstilstanden (2012) bruker aktivt definisjoner fra Norsk Standard. For å støtte opp om en mest mulig samkjørt terminologi har vi også valgt å bruke definisjoner fra Norsk Standard i denne rapporten.
[4] Standard Norge, 2012, «Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi» (NS 5830:2012). 2.34.
[5] Standard Norge, 2012, «Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi» (NS 5830:2012). 2.33.
[6] Ibid. 2.21
[7] Ibid. 2.18.
[8] Ibid. 2.31.
[9] NSM, Rapport om sikkerhetstilstanden 2012. s. 5.

Forebyggende sikkerhet er, i likhet med risikobilde, sammensatt av flere bestanddeler. Vi kan her med fordel sitere sikkerhetslovens definisjon av forebyggende sikkerhetstjeneste som:

> «planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet».[10]

Denne definisjonen knytter forebyggende sikkerhet opp mot risikobildet og introduserer to nye elementer: «forebyggende sikkerhetstiltak» (også «sikringstiltak») som søker å fjerne eller redusere risiko og «sikkerhetstruende virksomhet» (også «tilsiktede uønskede handlinger»). *Sikkerhetstruende virksomhet* refererer til «forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet».[11] I de senere år har det blitt vanlig å bruke formuleringen *tilsiktede uønskede handlinger* som Norsk Standard definerer som uønskede hendelser «som forårsakes av en aktør som handler med hensikt» og «som kan utsette en verdi for uønsket påvirkning» (eksempelvis i form av ødeleggelse, kompromittering eller forstyrrelse).[12] Likeledes bruker man i dag ofte «sikringstiltak» for forebyggende sikkerhetstiltak. *Sikringstiltak* refererer til «tiltak for å redusere risiko forbundet med tilsiktede uønskede handlinger».[13] (Disse endringene i terminologi er i hovedsak formelle og ikke substansielle. Vi gjengir den terminologien som er brukt i kildene, det vil si, forebyggende sikkerhetstiltak og sikringstiltak vil bli brukt noe om hverandre og det samme gjelder sikkerhetstruende virksomhet og tilsiktede uønskede handlinger.)

Sikringstiltak deles ofte inn i tre kategorier: menneskelige, organisatoriske og teknologiske. *Menneskelige sikringstiltak* er «tiltak som påvirker persepsjon, vurderingsevne, kunnskap, adferd og reell evne til å bruke teknologiske sikringstiltak og følge organisatoriske tiltak».[14] *Organisatoriske sikringstiltak* er «tiltak i form av skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, rutiner, adferd og/eller anvendelse av andre sikringstiltak».[15] *Teknologiske sikringstiltak* deles inn i tre kategorier: *fysisk sikringstiltak,* det vil si «fysisk barriere som hindrer eller forsinker uønsket adgang til verdier»; *elektronisk sikringstiltak,* det vil si «tiltak som bruker elektronisk utstyr og løsninger for å støtte, supplere eller erstatte fysiske sikringstiltak»; og *logisk sikringstiltak,* det vil si «tiltak for sikring av informasjon som lagres eller overføres elektronisk».[16] De forebyggende sikringstiltakene er *defensive* og tar sikte på å fjerne eller redusere risiko ved å *minske sårbarhetene* verdiene våre har overfor truslene mot dem.

Sikkerhetslovens definisjon av sikkerhetstruende virksomhet (sitert ovenfor) setter denne i forbindelse med spionasje, sabotasje eller terror. Sikkerhetsloven definerer *spionasje, sabotasje* og *terrorhandlinger* som henholdsvis: «innsamling av informasjon ved hjelp av fordekte midler i

[10] LOV 1998-03-20-10 Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), § 3.
[11] Ibid.
[12] NS 5830:2012. 2.3 og 2.4.
[13] Ibid. 2.8.
[14] Ibid. 2.15.
[15] Ibid. 2.14.
[16] Ibid. 2.10-2.13.

etterretningsmessig hensikt», «tilsiktet ødeleggelse, lammelse eller driftsstopp av utstyr, materiell, anlegg eller aktivitet, eller tilsiktet uskadeliggjøring av personer, utført av eller for en fremmed stat, organisasjon eller gruppering» og «ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer eller eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål».[17] Slik virksomhet rettet mot norske verdier utgjør en trussel mot Norges sikkerhet – særlig dersom den rettes mot kritiske verdier og deres sårbarheter. Spionasje, sabotasje og terrorhandlinger kan også være reelle trusler for virksomheter som ikke er underlagt sikkerhetsloven. For eksempel: private forretningsvirksomheter kan utsettes for industrispionasje og/eller industrisabotasje og virksomheter med høy symbolverdi (eller ganske enkelt høy synlighet) kan risikere å bli utvalgt som terrormål.

Planlegging, tilrettelegging, gjennomføring og kontroll av de forskjellige sikringstiltakene utgjør den forebyggende sikkerheten og er avgjørende for at våre verdier beskyttes mot de truslene vi står overfor. Planleggingen, tilretteleggingen, gjennomføringen og kontroll i virksomheten utføres i hver enkelt virksomhet, det kan være statlige eller private virksomheter. NSM er selv tilsynsmyndighet for det forebyggende sikkerhetsarbeidet i de av virksomhetene som er underlagt sikkerhetsloven, det vil si «den forbyggende sikkerhetstjenesten». (Mer om sikkerhetsloven, dens virkeområde og annen sikkerhetsrelatert lovgivning er gitt i kapittel 2.) Basert på disse tilsynene samt annen innhentet informasjon vurderer NSM tilstanden på det forebyggende sikkerhetsarbeidet opp mot deres årlige vurdering av sikkerhetstilstanden.

Figur 1.2 Forebyggende sikkerhet: organisatoriske-, menneskelige- og teknologiske tiltak.

Når vi nå har introdusert de to komponentene, risikobilde og forebyggende sikkerhet, som til sammen utgjør sikkerhetstilstanden «i teorien», samt at vi også har presentert en mengde sentrale definisjoner, vil vi her rette oppmerksomheten over på empirien – på hvordan Norges sikkerhetstilstand er blitt vurdert i de senere år og frem til i dag (2012).

[17] LOV 1998-03-20-10 Lovom forebyggende sikkerhetstjeneste (sikkerhetsloven). § 3.

1.1.2 Sikkerhetstilstanden i Norge, 2003-2012

Som allerede er blitt nevnt så utarbeider NSM årlig en rapport om sikkerhetstilstanden.[18] NSMs rapporter om sikkerhetstilstanden baseres på materiale fra en rekke kilder. Blant sentrale bidragsytere er Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten (E-tjenesten) som begge utarbeider vurderinger av trusler mot Norge og norske interesser.[19] NSM drar også nytte av andre kilder som Kripos og ØKOKRIM.[20] I tillegg tilvirker NSM egen empiri gjennom sine aktiviteter, herunder tilsyn med forbyggende sikkerhetstjeneste i virksomheter som er underlagt sikkerhetsloven. Den første rapporten utkom i 2003 («Risikovurdering 2003»), samme året som NSM ble opprettet som et selvstendig direktorat (se del 2.2). Den foreløpig siste rapporten i rekken utkom våren 2014, men dette forskningsprosjektets varighet medførte at den siste rapporten som inngår i våre analyser er rapporten fra 2012 («Rapport om sikkerhetstilstanden 2012»). Som det fremkommer av de siterte titlene har rapportserien utviklet seg over tid. Fokuset har gradvis beveget seg fra en hovedvekt på risikobildet, supplert med generell informasjon om forebyggende sikkerhetsarbeid, og over til mer utfyllende vurderinger av risikobildet og det forebyggende sikkerhetsarbeidet samt en vurdering av den resulterende sikkerhetstilstanden.[21] Vi vil her i korte trekk presentere noen av hovedtemaene og utviklingen som beskrives i NSMs rapporter om sikkerhetstilstanden (risikovurderingene) fra 2003 og frem til og med 2012.

«Risikovurdering 2003» tar for seg de mest sentrale temaene innen sikkerhetstilstand: risikobildet, sikkerhetsmessig verdi, sikkerhetstrusselen, sårbarhet og forebyggende sikkerhetstiltak. Rapporten retter særlig oppmerksomhet på sikkerhetstrusselen og på informasjons- og kommunikasjonsteknologi (IKT) sikkerhet. NSM drar frem hvor viktig det er å ha inngående kjennskap til trusselen – hva *trusselaktører* fokuserer på, hvilke metoder de bruker og hvilke kapasiteter og intensjoner de har. Sentrale kategorier trusselaktører inkluderer: nasjoner som driver etterretningsvirksomhet i og mot Norge (statlige aktører), terroraktører og kriminelle. NSM lister en rekke «plattformer» som gjerne benyttes for å innhente informasjon i etterretningssammenheng, herunder ambassadepersonell, teknisk avlytting og personkontakt.[22] Rapporten lister også en rekke områder hvor trusselaktører har drevet aktiv etterretning i og mot Norge: vår utenriks- og sikkerhetspolitikk; Forsvaret; vår virksomhet i utlandet; personell og beslutningstakere; industri, forskning og teknologi; kritisk infrastruktur; objekter med symbolverdi og farlig materiell m.fl.[23]

NSM drar også frem sikkerhetsmessige utfordringer knyttet til vår økende avhengighet av IKT. Rask teknologisk utvikling og utbredt bruk av IKT systemer gjør informasjonssystemene sårbare.

---

[18] Rapportene er titulert «Risikovurdering» for 2003-2007 og «Rapport om sikkerhetstilstanden» f.o.m. 2009. I 2008 utkom det ikke en separat ugradert rapport men de samme problemstillingene ble presentert i en lignende publikasjon titulert «Hovedpunkter fra NSMs årlige Rapport om sikkerhetstilstanden» samt undertittelen «Tilstanden i virksomhetene 2008» i NSMs årsmelding for det samme året.

[19] PSTs trusselvurderinger er tilgjengelige via tjenestens nettsider (www.pst.no) og E-tjenestens «FOKUS» er tilgjengelige vis Forsvarets nettsider (www.forsvaret.no).

[20] NSM, 2012 «Rapport om sikkerhetstilstanden 2012», s. 8.

[21] Rapportene er tilgjengelige på NSMs nettsider (https://www.nsm.stat.no) under publikasjoner/rapporter.

[22] NSM, 2003, «Risikovurdering 2003», s. 12.

[23] Ibid. s. 11.

NSM nevner i den forbindelse at det kan være vanskelig å begrunne satsning på sikkerhet i et kortsiktig økonomisk perspektiv (særlig med tanke på kompleksiteten som kreves og hvor fort utviklingen går).[24] Samtidig rapporterer NSM at angrep mot nettopp informasjonssystemer i vinnings hensikt er et økende samfunnsproblem.[25] Denne første rapporten i rekken av NSMs vurderinger av sikkerhetstilstanden maler et bilde med forbedringspotensial. I forordet til rapporten heter det at «det er en kjensgjerning at forebyggende sikkerhetstjeneste i dag i mange virksomheter ikke gis den nødvendige prioritet».[26] Avslutningsvis skriver NSM at de gjennom sin virksomhet har avdekket ulike former for sikkerhetsmangler og at NSMs anbefaling er «at sikkerhetslovens regler følges opp i større grad enn det som synes å ha vært tilfelle hittil».[27]

I NSMs «Risikovurdering 2004» er det spesielt to temaer som blir viet oppmerksomhet, NSMs oppgaver og rolle og risikovurdering. Vi vil i denne studien presentere regelverket for og organisasjonen av forebyggende sikkerhet i Kapittel 2 og kommer derfor ikke til å gå inn på NSMs oppgaver og rolle her. Når det gjelder risikovurdering så går rapporten i detalj på begrepene «sikkerhet» og «risiko». *Sikkerhet* omfatter sikkerhetstruende hendelser av kvalitativ forskjellig art dvs. både tilsiktede handlinger (jf. «security» på engelsk) og tilfeldige handlinger (jf. «safety» på engelsk). Det er sikkerhet i betydningen tilsiktede handlinger («security») som faller inn under sikkerhetsloven og NSMs myndighet, men rapporten hevder at overgangen mellom de to typene sikkerhet er flytende og at konsekvensene av tilsiktede og tilfeldige handlinger kan være like.[28] *Risiko* presenteres som et sammensatt begrep som består av komponentene «sannsynlighet» og «konsekvens».[29] Å analysere risiko forbundet med tilsiktede handlinger basert på disse to begrepene er noe NSM selv nå har gått bort fra. I dag bruker NSM den definisjonen av risiko som er oppgitt i Norsk Standard (NS 5830:2012) og som vi har gjengitt i 1.1.1 ovenfor. Rapporten er sparsommelig på detaljer vedrørende den forbyggende sikkerheten og selve sikkerhetstilstanden. NSMs oppfatning av disse kan derimot leses mellom linjene i anbefalingene som gis: forebyggende sikkerhet må bringes inn på et tidligere stadium (for eksempel ved oppføring av store vitale bygninger og ved installering av store informasjonssystemer), det er behov for en holdningsendring (spesielt blant brukere av store, elektroniske informasjonssystemer) og det er viktig at sikkerhetsarbeidet foregår kontinuerlig slik at det bygges opp en kultur hvor sikkerhet tas alvorlig.[30] Med andre ord, forbedring utbedes.

NSMs «Risikovurdering 2005» gjentar tidligere advarsler mot etterretningsaktivitet, som fortsatt eksisterer «i form av tradisjonell, statsinitiert spionasje», og terroraktører.[31] Når det gjelder sårbarheter nevnes spesifikt vår avhengighet av internett, navigasjonssystemer og elektroniske informasjonssystemer som alle tre kan påvirkes negativt på forskjellige måter (for eksempel ved bruk av tjenestenektangrep, jammeutstyr og avlesning).[32] Rapporten presenterer resultater fra en

[24] Ibid. s. 22-23.
[25] Ibid. s. 14.
[26] Ibid. s. 4.
[27] Ibid. s. 29.
[28] NSM, 2004, «Risikovurdering 2004». s. 4.
[29] Ibid. s. 4-5.
[30] Ibid. s. 14.
[31] NSM, 2005 «Risikovurdering 2005». s. 2.
[32] Ibid. s. 4.

spørreundersøkelse gjennomført av NSM. Spørreundersøkelsen viser at: ved sikkerhetsgradering (se 2.1.1) er virksomheters *tidligere* praksis til en viss grad førende, noe som kan vanskeliggjøre at sikkerhetsgraderingene gjenspeiler *samtidig* risikobilde; virksomheter ser ikke ut til å evaluere egne sikkerhetstiltak i særlig grad; flere virksomheter gjennomfører ikke autorisasjonssamtaler (se 2.1.1); sikkerhetsorganisasjonen nedprioriteres ofte i omstillingsfaser.[33] NSM bemerker at forebyggende sikring mot for eksempel terrorhandlinger kan forbedres ved å utvide sikkerhetslovens virkeområde til å omfatte flere virksomheter samt at Norge på det nåværende tidspunkt ennå ikke har en egen «Computer Emergency Response Team» (CERT) for å koordinere svar på IT-angrep.[34] (NorCert ble opprettet året etter, mer om dette i Kapittel 2.)

Selv om NSMs rapporter om sikkerhetstilstanden (risikovurderingene) for årene 2003-2005 ikke kan regnes som særlig «lystig» lesning synes det som at NSMs «Risikovurdering 2006» markerer en forverring. NSM siterer PSTs vurdering av etterretningstrusselen mot norske interesser som «betydelig» og skriver at:

> «en betydelig etterretningstrussel er en alvorlig tilstand som må spore til en målrettet innsats for å beskytte sikkerhetsgradert og annen sensitiv informasjon. NSMs erfaring er at flere virksomheter ikke i tilstrekkelig grad tar hensyn til at etterretningstrusselen er betydelig».[35]

Rapporten dedikeres så i sin helhet til fem konkrete områder «hvor sikkerhetsarbeidet i mange virksomheter har et forbedringspotensial»: verdivurdering, øvelse, sikkerhetsadministrasjon (se 2.1.1), IKT-sikkerhet og sikkerhetskultur. Sistnevnte plukker opp tråden fra anbefalingene i rapporten av 2004 og utdyper at riktige holdninger og motivasjon er forutsetninger for at sikkerhetsarbeidet skal lykkes og for at effekten av de ulike tiltakene vil bli redusert dersom det ikke etableres en god sikkerhetskultur.[36]

NSMs «Risikovurdering 2007» repeterer mange allerede velkjente temaer, herunder at det norske samfunn står overfor betydelige risikoer i form av sabotasje og terror, og særlig spionasje. Økende sårbarheter i et stadig mer IKT-avhengig samfunn er et annet velkjent og sentralt tema. NSM trekker særlig frem økende bruk av *botnet*[37] og *phishing*[38] for økonomisk vinning og av *tjenestenektangrep*[39] i forbindelse med politiske eller religiøse konflikter.[40] Rapporten av 2007 gir

[33] Ibid. s. 6.
[34] Loc.cit.
[35] NSM, 2006, «Risikovurdering 2006». s. 3-4.
[36] Ibid. s. 8.
[37] Et *botnet* er et nettverk av datamaskiner som er blitt infisert av skadevare (malicious software, eller «malware» i forkortet form). *Bot* kommer av robot og referer til at de infiserte maskinene gjennomfører automatiserte oppgaver over internett uten eiers viten og vilje (de blir også kalt zombier). microft.com/security, What is a botnet?
[38] *Phishing* er en form for svindel hvor man via e-post blir forsøkt lurt til å oppgi personopplysninger til uvedkommende. merriam-webster.com/dictionary/phishing
[39] *Tjenestenektangrep* (denial of service, DoS) er en angrepsmetode som brukes mot datasystemer over et nettverk. Tjenestenektangrep forsøker, som navnet tilsier, å gjøre sette datasystemer ute av stand til å utføre sine tjenester. compnetworking.about.com, DoS - Denial of Service.

til forskjell fra den foregående både ris og ros. Selv om NSM etterlyser bedre koordinering blant virksomheter når det gjelder verdivurdering rapporterer direktoratet også at de har sett «en positiv trend med hensyn til fokus på verdivurdering i året som er gått».[41] Et nytt tema av året er kostnader knyttet til sikkerhetsbrudd. NSM vedgir at opprettelse av nødvendige sikkerhetstiltak er en langvarig prosess men advarer mot å unnlate å overholde forpliktelser (slik som å rapportere om grove sikkerhetsbrudd) i frykt for ekstrautgifter.[42] NSM retter også oppmerksomheten mot kostnader tilknyttet brudd på sikkerheten og at denne kan vurderes på ulike måter. For eksempel: sikkerhetsgradert informasjon i hendene på en «motstander» kan innebære redusert sikkerhet, sikkerhetsbrudd kan nødvendiggjøre kostbare utbedringer og de kan føre til tap av tillit og renommé.[43]

I «Tilstanden i virksomhetene 2008» og «Hovedpunkter fra NSMs Rapport om sikkerhetstilstanden» (2007/2008) fortsetter fokuset på trusler og sårbarheter i det digitale rom. NSM beskriver særlig utfordringer knyttet til fenomener som «hacktivism» (politisk motivert dataangrep) og bruk av ondsinnet programvare. Utviklingen innen ondsinnet programvare vurderes som særlig bekymrende: «Utfordringen er så stor at selv sikkerhetsbevisste virksomheter vil kunne oppleve å bli utsatt for alvorlige dataangrep».[44] Også dette året deler NSM ut både ris og ros, men mest ris. NSM observerer at arbeidet med forebyggende sikkerhetstjeneste som regel er godt i de virksomheter der dette arbeidet er lederforankret og systematisk, men der dette mangler blir ofte resultatet tilfeldig og personavhengig.[45] Gjennom sin tilsynsaktivitet har NSM avdekket «grunnleggende mangler i virksomhetenes forebyggende sikkerhetsarbeid. Dette gjelder både kunnskaper, prioritering, forankring og styring».[46] Under overskriften «en urovekkende utvikling» konstaterer NSM at: «Aktiviteten til utenlandske staters etterretningstjenester mot Norge og norske interesser er høy […] Det forebyggende defensive sikkerhetsarbeidet holder ikke følge med dette».[47]

NSMs «Rapport om sikkerhetstilstanden 2009» tar bladet fra munnen og presenterer NSMs overordnede vurdering av sikkerhetstilstanden i Norge som «ikke tilstrekkelig» sett i forhold til dagens trusselbilde.[48] Rapporten adresserer så en rekke helt sentrale områder hvor det forbyggende sikkerhetsarbeidet ikke er tilfredsstillende, dette inkluderer: manglende lederengasjement, mangelfull organisering, mangelfull kompetanse og bevissthet, med flere. Særlig interessant er observasjonen at selv om majoriteten av alle cyberangrep går mot sårbarheter hvor det finnes sikkerhetsoppdateringer og andre sikkerhetstiltak er likevel mange mindre sofistikerte angrep vellykkede da vedlikehold ikke blir ivaretatt og tilgjengelige oppdateringer ikke blir benyttet.

---

[40] Ibid. ss.15-16.
[41] NSM, 2007, NSMs Risikovurdering. s. 6-7.
[42] NSM, 2007, «Risikovurdering 2007». s. 12.
[43] Loc. cit.
[44] NSM, 2007/2008, «Hovedpunkter fra NSMs årlige Rapport om sikkerhetstilstanden». s. 4.
[45] Ibid. s. 2.
[46] NSM, 2008, «Tilstanden i virksomhetene 2008» i NSMs «Årsmelding 2008». s. 8.
[47] Ibid. s. 7.
[48] NSM, 2009, «Rapport om sikkerhetstilstanden 2009». (Uten sidetall.)

I «Rapport om sikkerhetstilstanden 2010» rapporteres det at gapet mellom trusselaktørenes kapasiteter og mottiltakene i virksomhetene har økt og at sikkerhetstilstanden i Norges dermed forverres.[49] NSM påpeker mangler når det gjelder verdiforståelse, oversikt over egen sikkerhetstilstand, kompetanse, osv. I «Rapport om sikkerhetstilstanden 2011» melder NSM at sikkerhetstilstanden i Norge blir stadig svekket. Risikoforståelsen knyttet til spionasje, sabotasje og terror er fortsatt for lav og viktige tiltak som risikovurderinger, kompetanseheving, rapportering og sikkerhetsrevisjon blir ikke gjennomført».[50] Kort fortalt oppsummeres situasjonen som følger:

- Verdiene våre øker i volum og betydning i takt med samfunnsutviklingen og økt produksjon av informasjon.
- Truslene mot skjermingsverdig informasjon øker og skjerpes i takt med nyvinninger innen IKT. Nyvinningene tillater trusselaktører å bli mer selektive når det gjelder utvelgelse av mål og å bli mer effektive med hensyn til gjennomførelse.
- Stadig nye sårbarheter oppdages og kan utnyttes.
- Tiltak som reduserer sårbarhetene er utilstrekkelige i utgangspunktet og holder ikke tritt med trusselutviklingen.[51]

Den siste i rekken av NSMs årlige rapporter om sikkerhetstilstanden som inngår i våre analyser er rapporten fra 2012. Dens hovedkonklusjon er at:

> «Sikkerhetstilstanden for 2012 er ikke tilfredsstillende. De sikkerhetsmessige utfordringene som er skissert vil fortsette, og øke i omfang. Dette begrunnes med markante sårbarheter i teknologiske, organisatoriske og menneskelige forhold. Det er registrert økt uønsket aktivitet mot viktige norske verdier. Sikkerhetsarbeidet i virksomhetene utvikles ikke tilstrekkelig for å møte et stadig mer komplekst risikobilde».[52]

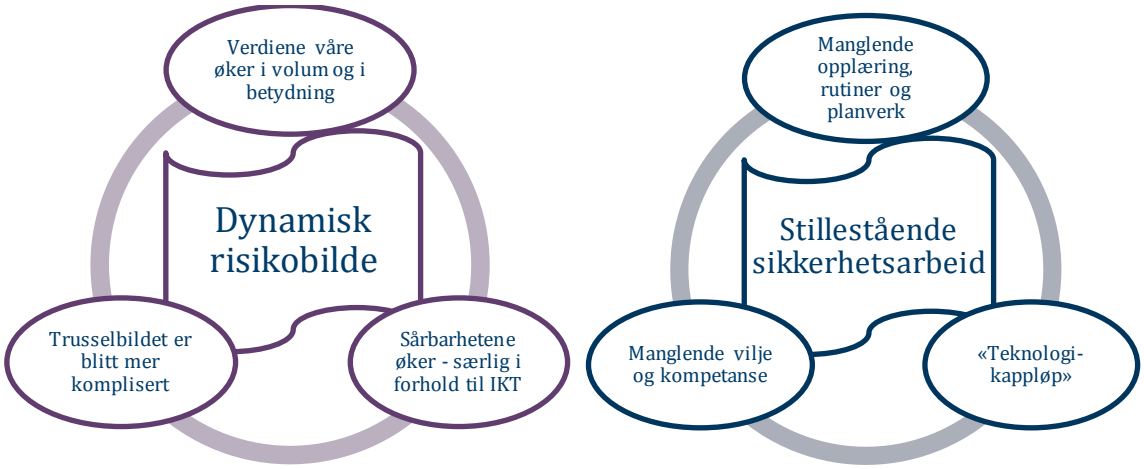
De sikkerhetsmessige utfordringene som er skissert inkluderer at:

- Norge og norske interesser daglig utsettes for uønsket ulovlig etterretning fra andre stater.
- Risikoen for at virksomheter som av hensyn til rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser er underlagt sikkerhetsloven[53] blir utsatt for uønsket kriminell aktivitet via internett eller mot deres sikkerhetsgraderte systemer er økende.
- Det er et pågående digitalt «kappløp» mellom de som jobber med forebyggende sikkerhetstiltak og de som forsøker å utnytte sårbarheter for digitale angrep.
- Mørketallene for innrapporterte sikkerhetstruende hendelser anses å være store; dette til tross for at antallet innrapporterte hendelser har økt de siste årene.

[49] NSM, 2010, «Rapport om sikkerhetstilstanden 2010». s. 2.
[50] NSM, 2011, «Rapport om sikkerhetstilstanden 2011». s. 4.
[51] Loc. cit.
[52] NSM, 2012, Rapport om sikkerhetstilstanden 2012, s. 3.
[53] LOV 1998-03-20-10 Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven).

Når det gjelder attraktive mål og metoder så er situasjonen langt på vei den samme i dag som i tidligere år. Den økende uønskede aktiviteten mot norske interesser retter seg i stor grad mot et knippe aktiviteter som er særlig interessante for trusselaktører. Dette gjelder særlig forsvarsindustrien, olje- og gassektoren, luft- og romfartsindusti og andre typer høyteknologisk industri samt Forsvaret. I tillegg er politiske beslutningstakere særlig utsatt for etterretningsaktivitet.[54] Metodene som brukes inkluderer bruk av teknologi så vel som sosial manipulasjon.[55]

Som en illustrasjon av sikkerhetstilstanden og dens utvikling i de senere år kan de to figurene av risikobilde og forebyggende sikkerhet som ble presentert i 1.1.1 ovenfor «fylles ut» slik:



Figur 1.3 Norges sikkerhetstilstand (2003-2012)

Det er dette bildet av sikkerhetstilstanden, her oppsummert i Figur 1.3, som danner bakteppet for SÅKOV-prosjektet og forskningsaktiviteten ÅMS. I denne studien søker vi å belyse de bakenforliggende årsakene til at sikkerhetstilstanden er utilfredsstillende og sikkerhetsarbeidet er stillestående og ikke holder tritt med utviklingene i risikobildet.

1.2 Forskningsdesign

For å besvare denne studiens forskningsspørsmål på en tilfredsstillende måte har vi besluttet å diversifisere vår analyse ved å sammenstille en håndfull delanalyser. Disse delanalysene er designet for å ta høyde for at årsaker konseptualiseres og presenteres ulikt i forskjellige kretser og media, og at det derfor kan være vanskelig å fremskaffe en bred og mest mulig representativ oversikt over de mest sentrale årsakene til at vi har en utilfredsstillende sikkerhetstilstand i Norge. Eksempelvis, den faglige debatten om det forebyggende sikkerhetsarbeidet kan tenkes å avvike fra den allmenntilgjengelige debatten i massemedia. På samme vis kan det tenkes at spørsmål omkring konkrete sikringstiltak og diskusjoner vedrørende de juridiske rammene rundt, belyser vidt forskjellige svakheter som kan være interessante for denne studien. Denne studien sammenstiller derfor flere delanalyser som alle tar for seg den samme problemstillingen, men som tilnærmer seg den på ulikt vis og basert på forskjellig kildemateriale. Vi vil her presentere

[54] NSM, 2012, Rapport om sikkerhetstilstanden, s. 3.
[55] Ibid. s. 9.

hver av disse delanalysene, men først vil vi gi en kort presentasjon av to sentrale metoder som, mer eller mindre eksplisitt, brukes i hver av de totalt fem delanalysene: dokumentanalyse og kvalitativ innholdsanalyse.

Dokumentanalyse

Dokumentanalyse er en kvalitativ forskningsmetode som går ut på å systematisk gjennomgå eller evaluere dokumenter. Dokumentene undersøkes og tolkes for å trekke frem mening, for å oppnå bedre forståelse og for å utvikle empirisk kunnskap omkring forskningsspørsmålet.[56] Glenn Bowen har laget en liste over metodens fordeler og ulemper, herunder: dokumentanalyse er en effektiv metode fordi den baseres på et utvalg av materiale heller enn innsamling av materiale; dokumenter er ikke reaktive, det vil si de er stabile og blir ikke påvirket av forskning noe som igjen betyr at de uforandrede dokumentene kan gjennomgås gjentatte ganger ved behov; på den andre siden så er dokumenter forfattet med en hensikt annen enn den forskeren har og inneholder derfor ikke nødvendigvis den informasjonen forskeren kunne trenge for å besvare forskningsspørsmålet.[57] Den eneste måten å minimere ulempen det siste punktet medfører er å studere forskjellige typer dokumenter fra forskjellige kilder slik vi har valgt å gjøre med våre fem delanalyser. Bowen gir også følgende beskrivelse av dokumentanalyse: dokumentanalyse involverer skimming (overflatisk gjennomgang), lesning (nøye gjennomgang) og fortolkning. Denne iterative prosessen kombinerer elementer fra innholdsanalyse og tematisk analyse.

En innholdsanalyse går ut på å organisere informasjon i kategorier som er relatert til forskningsspørsmålet. Tematisk analyse defineres som en form for mønstergjenkjennelse, en prosess som innebærer en nøye og fokusert lesning og gjennomgang av materialet.[58] Innholdsanalyse og tematisk analyse benyttes til en viss grad i alle de fem delanalysene. I tillegg benytter denne studien innholdsanalyse mer formelt (eksplisitt) i to av analysene (nr. 2 og nr. 5).

Innholdsanalyse

En innholdsanalyse går som sagt ut på å organisere informasjon i kategorier som er relatert til forskningsspørsmålet. Metoden er fleksibel i den forstand at en innholdsanalyse kan gjennomføres på ulike medier og etter ulike standarder. Noe forenklet kan det sies at innholdsanalysen er en metode som ligger mellom tekstanalyse (semiotikk) på den ene siden og diskursanalyse på den andre siden og som dekker hele spekteret mellom de to. Innholdsanalyser kan være kvantitative eller kvalitative alt ettersom hva det er som studeres og hvilket kildemateriale som er tilgjengelig. Innholdsanalyser kan kombineres med tekstanalyser eller med diskursanalyser, og da det ikke er enighet om akkurat hvor «delelinjene» går kan en og samme analyse plasseres noe ulikt på «skalaen» også. Metoden blir brukt noe ulikt i de forskjellige delanalysene i denne studien. I hovedsak er dette en ulikhet som gjør seg gjeldende i hvilken grad metoden brukes eksplisitt eller implisitt. Med få unntak vil denne studiens analyser være å regne for kvalitative innholdsanalyser.

[56] Bowen, Glenn A. 2009, Document Analysis as a Qualitative Research Method, Qualitative Research Journal, vol. 9, no. 2, s. 27.
[57] Ibid. s. 31.
[58] Ibid. s. 32.

Vurderinger av sikkerhetstilstanden (delanalyse nr. én)

Den første av denne studiens delanalyser er en analyse av NSMs rapporter om sikkerhetstilstanden (risikovurderinger). Disse publikasjonene utgjør en sentral komponent i denne studiens kontekst, men de er også første steget på veien til å finne årsakene til hvorfor vi har en utilfredsstillende sikkerhetstilstand. Denne delanalysen består derfor av en grundig sammenlignende lesning av NSMs 10 rapporter om sikkerhetstilstanden (2003-2012) for å danne et bilde av *utviklingen i sikkerhetstilstanden over tid*; for å forstå *forholdet mellom eksterne og interne årsaker* til at sikkerhetstilstanden er som den er; for å se *i hvilken grad NSM selv adresserer årsaker* og evt. hvilke årsaker; og, sist men ikke minst, for å opparbeide en oversikt over *søkeord som kan hjelpe oss å fange opp mediedebatten* rundt forebyggende sikkerhet. (Mer om det siste punktet nedenfor.)

Avvik og observasjoner i tilsynsrapporter (delanalyse nr. to)

I den andre analysen ser vi nærmere på hvilke feil og mangler som forekommer i virksomhetene, på symptomene til de årsakene vi er ute etter. Denne analysen baseres på et utvalg av 11 tilsynsrapporter fra 10 virksomheter. Disse rapportene gjengir funn NSM har gjort ved tilsyn i forskjellige virksomheter i ulike sektorer. Hensikten med denne analysen er å danne oss et bedre bilde av hvilke feil og mangler som forekommer og hvilke feil og mangler som er de mest vanlige på tvers av virksomheter og sektorer. I tillegg til gjennomgang av de 11 tilsynsrapportene har vi samlet alle registrerte avvik i en database som vi har brukt for å kategorisere avvikene. Denne analysen opplyser om hvor i de forebyggede sikringstiltakene de mest allmenne årsakene ligger (altså hvilken kategori) samtidig som at den gir innblikk i konkrete feil og mangler i virksomhetene hvor tilsynene er blitt gjennomført.

Avvikene kategoriseres på følgende måte:[59]

Kategorier av avvik med definisjoner og eksempler					
Menneskelige avvik	**Organisatoriske avvik**	**Teknologiske avvik**			Annet
		Fysiske avvik	Elektroniske avvik	Logiske avvik	
Avvik i en persons eller i en liten gruppe personers adferd og/eller kompetanse.	Avvik i skriftlige eller muntlige beskrivelser, vurderinger og beslutninger som regulerer ledelse, organisering, prosesser, analyser, rutiner, adferd, og/eller anvendelse av andre sikringstiltak.	Avvik ved fysiske barrierer som hindrer eller forsinker uønsket adgang til verdier. F. eks. dører, låser, gjerder eller naturgitte forhold.	Avvik i elektronisk utstyr og løsninger som brukes for å støtte/supplere/erstatte fysiske sikringstiltak. F. eks. automatisk innbruddsalarmanlegg, TV-overvåkning eller automatisk adgangskontroll.	Avvik i den teknologiske sikringen av informasjon som lagres eller overføres elektronisk. F. eks feil og mangler i IKT-programvare, brannmur eller antivirusprogrammer	
Menneskelige/organisatoriske avvik					
Avvik i en persons eller i en liten gruppe personers adferd og/eller kompetanse som følge av organisatoriske avvik, eller som burde vært forhindret av organisatoriske sikringstiltak.					

Figur 1.4 Kategorier av avvik med definisjoner og eksempler.

I tillegg til de tre kategoriene, *menneskelige, organisatoriske og teknologiske avvik* som gjenspeiler de forskjellige typene sikringstiltak har vi valgt å også inkludere en «blandet kategori»: *menneskelige/organisatoriske avvik*. Dette er fordi tilsynsrapportene i mange tilfeller beskriver ett tilfelle av et avvik. Det er uvisst om det her dreier seg om et enkelttilfelle eller om det er et eksempel på hvordan noe gjøres generelt i virksomheten. I flere tilfeller dreier det seg også om avvik som i utgangspunktet synes som menneskelig svikt, men som vi mener burde vært forhindret dersom de organisatoriske sikringstiltakene hadde fungert tilfredsstillende. Vi kan ikke med sikkerhet kategorisere disse avvikene som enten menneskelige eller organisatoriske. Vi synes også at den resulterende blandede kategorien fanger opp et viktig moment i og med at avvikene som faller inn under denne kategorien illustrerer den nære sammenhengen mellom organisatoriske og menneskelige faktorer.

Deltagende observasjon og intervjuer (delanalyse nr. tre)

Den tredje analysen nærmer seg empirien enda mer enn den forrige ved at vi gjennom deltakelse på tilsyn i virksomheter og intervjuer samler inn vårt eget materiale. Som det ble nevnt i forbindelse med dokumentanalysemetoden ovenfor så går den ut på å velge hvilke dokumenter man skal studere heller enn å samle inn materiale selv. Gjennom deltakende observasjon og semi-strukturerte intervjuer (med intervjuguide) supplerer vi på med dokumenter som vi selv forfatter, i form av notatene våre; det vil si, dokumenter som er forfattet med den hensikt å besvare nettopp vårt forskningsspørsmål. Grunnen til at vi regner dette for en separat analyse og ikke slår den

[59] Kategoriene er utviklet basert på relevante definisjoner i NS 5830:2012 av *sikringstiltak* (2.8), *teknologisk sikringstiltak* (2.10, 2.11, 2.12, 2.13), *organisatorisk sikringstiltak* (2.14) og *menneskelig sikringstiltak* (2.15).

sammen med delanalyse nr. 2 er at vi i dette tilfellet fikk en mye rikere kontekstualisering av prosessene, og mange av funnene i denne analysen stammer fra praktisk læring som vi selv har oversatt til tekstformat ved å notere ned observasjoner så vel som uttalelser. Disse dokumentene er ikke direkte sammenlignbare med tilsynsrapportene i delanalyse nr. 2, særlig da resultatene av de tilsynene hvor vi har vært observatører heller ikke foreligger i skrivende stund.

Sammenligning av regelverk (delanalyse nr. fire)

På samme vis som vi bruker dokumentanalyse for å avdekke status og trender i vurderingene av sikkerhetstilstanden i delanalyse nr. en, bruker vi også samme metode for å forstå det juridiske rammeverket som setter betingelser for det forebyggende sikkerhetsarbeidet. Til forskjell fra delanalyse nr. én så fokuserer denne analysen på forholdet mellom forskjellige lovverk heller enn utviklingen over tid. Det vi i hovedsak ser på her er forholdet mellom den sektorovergripende lovgivningen for forebyggende sikkerhet (sikkerhetsloven) og sektorspesifikt lovverk på samme tema. Sistnevnte er for stort et tema til å ta for seg her så vi har derfor valgt ut en sektor, olje- og energisektoren, som vi presenterer som et eksempel på sektorlovgivning. Analysen ser også på intern konsistens innen de forskjellige lovverkene, (u)tvetydighet og i hvilken grad kravene er operasjonalisert.

Kvalitativ innholdsanalyse av media (delanalyse nr. fem)

Den siste delanalysen er den som i høyest grad benytter seg av innholdsanalysemetoden som analyseverktøy. Dette dreier seg om en analyse av media - et område som ikke er ukjent for kvalitative innholdsanalyser. Analysen gjennomføres over flere steg: tidsavgrensning, utvelgelse av media, utvelgelse av artikler, utvikling av kodebok, klassifisering av innhold i henhold til kategoriene i kodeboken, og analyse av resultatene.

Når det gjelder tidsavgrensning så vil vi dekke stort sett den samme perioden som vi har tilgjengelige rapporter om sikkerhetstilstanden (2003-2012), samtidig som at vi gjerne vil inkludere mest mulig oppdatert materiale. Tidsperioden vi bruker er fra og med 1. januar 2003 og til og med 31. juli 2013. Da dekning av hele mediedebatten er altfor stort et tema for denne studien så vi oss nødt til å velge ut noen medier. Hensikten vår la her strenge føringer på hvilke medier vi kunne velge da vi var avhengige av elektronisk tilgang og søkemuligheter. Vi konsulterte også Gallup sin toppliste over antall unike brukere på forskjellige nettsteder. Vi endte opp med å velge ut VG og NRK sine nettarkiver.

For å finne de relevante nyhetssakene innen VG og NRKs nettarkiver benyttet vi oss av målrettet utvelgelser (*relevance sampling* eller *purposive sampling*).[60] Målrettet utvelgelse er ikke basert på sannsynlighet, utvalget som gjøres er ikke ment å representere universet av nyhetssaker (mediedekningen generelt), men i stedet å representere akkurat den delen av mediedekningen som omhandler forebyggende sikkerhet. Måten vi har valgt å gjøre dette på er å bruke søkeord som vi

[60] Krippendorf, Klaus, 2013 (3rd ed.), Content Analysis: An Introduction to its Methodology, SAGE Publications, s. 120-121.

har samlet fra og med den første delanalysen for å identifisere nyhetssaker som omhandler den relevante tematikken. Søkeordene vi bruker er som følger:

Sikkerhet/tryggleik[61]
Samfunnssikkerhet/samfunnstryggleik
Forebyggende sikkerhet/førebuande tryggleik
Trussel/ trugsel
Sårbarhet/sårbarheit
Risiko
Etterretning
Spionasje
Sabotasje
Terrorisme
Sikringstiltak

Ikke alle treffene vi fikk på disse søkeordene var relevante, og vi opplevde at mye av den spesialiserte debatten omkring forebyggende sikkerhet falt utenom. Vi supplerte derfor utvelgelsen med følgende mer spesialiserte søkeord:

Sikkerhetskultur/tryggleikskultur
Sikkerhetsloven/tryggleikslova
Sikkerhetstilstand/tryggleikstilstand
Sikkerhetspersonell/tryggleikspersonell
Forebyggende sikkerhetstjeneste/førebuande tryggleiksteneste
Nasjonal sikkerhetsmyndighet/Nasjonal tryggleiksmyndigheit
Sikkerhetsadministrasjon/tryggleiksadministrasjon
Informasjonssikkerhet/informasjonstryggleik
Objektsikkerhet/objekttryggleik
Risikoforståelse/risikoforståing
Risikobilde/risikobilete
Risikoerkjennelse/risikoerkjenning
Risikovurdering
Systemsikkerhet/systemtryggleik
Fysisk sikring
Skjermingsverdig informasjon
Skjermingsverdig objekt

Alle artiklene ble samlet i et mediearkiv.

Videre så utviklet vi en kodebok med de kategoriene vi er ute etter og underkategorier for informasjonen vi er ute etter (se Figur 1.5 nedenfor). Kodeboken inneholder åtte kategorier som dekker forskjellige tematikker som direkte eller indirekte gir oss opplysninger om

[61] Vi tilpasser søkene for å fange opp bøyde former der dette ikke var en funksjon i søkemotoren.

sikkerhetstilstanden og årsaker til denne: anledning for nyhetssaken, sikkerhetstilstanden, trusler, sårbarheter, verdier, årsaker, NSM, kostnader.[62] Hver av kategoriene har én, to eller tre nivåer avhengig av kompleksiteten. Eksempelvis, når det gjelder sikkerhetstilstanden så registrerer vi i henhold til kodeboken om den er omtalt i nyhetssaken eller ikke (1. nivå), i tilfelle omtale så registreres det om denne er eksplisitt eller implisitt (2. nivå), deretter registreres det om sikkerhetstilstanden omtales i nøytralt, positivt eller negativt ordelag (3. nivå). I tillegg så inkluderer denne kodeboken åpne kommentarfelt for at vi skal kunne registrere eksempler osv. som er av interesse for denne studien.

Før vi klassifiserte innholdet i alle artiklene i et medie-arkiv operasjonaliserte vi kodeboken (se Vedlegg A).

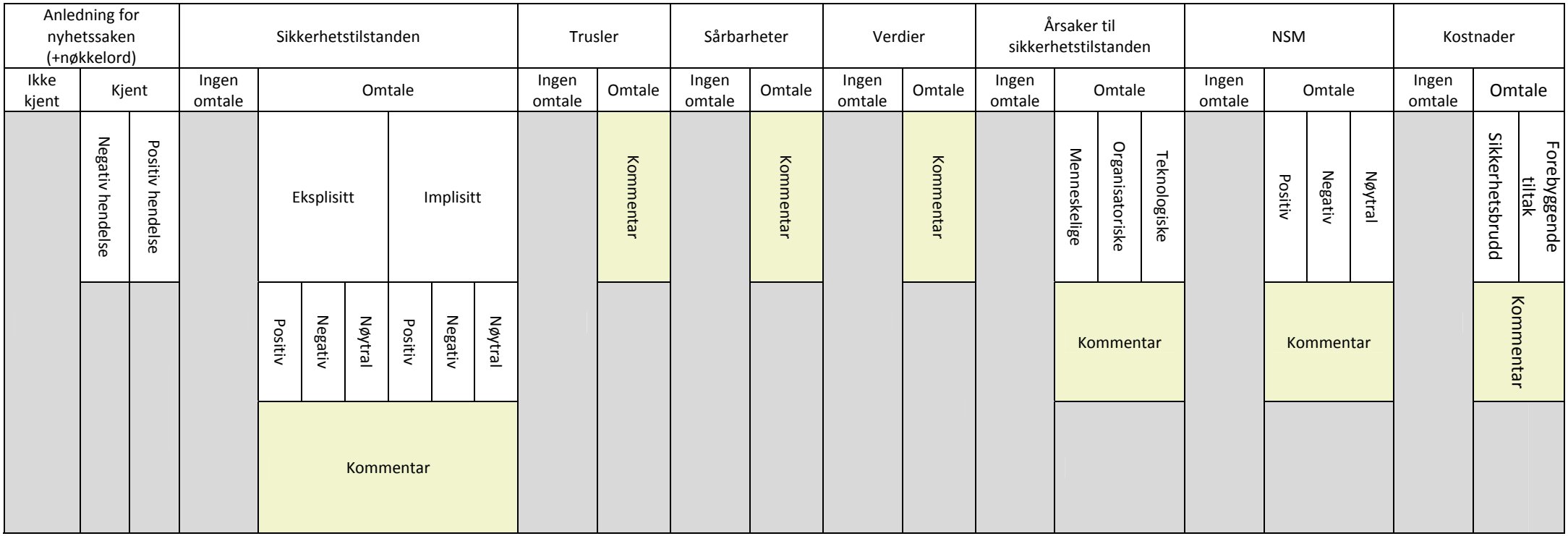
Selve klassifiseringen av innhold i henhold til kategoriene i kodeboken og utfylling av kommentarfeltene ble gjennomført ved manuell gjennomgang av alle artiklene i mediearkivet. Underveis luket vi ut de artiklene som ble fanget opp av søkeordene men som ikke faktisk omhandlet forebyggende sikkerhet.

Grunnen til at vi har valgt å inkludere en relativt omfattende medieanalyse innenfor rammene av denne studien, er at vi ønsker å differensiere kildematerialet, og at vi søker å måle pulsen på den norske befolknings oppfatninger og holdninger til forebyggende sikkerhet og til sikkerhetstilstanden, som et supplement til delanalysene som konsentrerer seg på «bransjen» og de som er direkte involvert i det forebyggende sikkerhetsarbeidet. Tanken bak er at nyhetssakene fungerer både som refleksjon av samfunnets holdninger (media gir publikum det det vil ha) og som folkeopplysning (media påvirker opinionen). Begge deler er av interesse for denne studien og særlig som rammeverk for de holdninger og «instrukser» som finner og gis innen forebyggende sikkerhet.

[62] Kostnadskategorien er inkludert med tanke på en fremtidig aktivitet i SÅKOV-prosjektet og kommer ikke til å behandles i denne studien som sådan.

Kodebok for kvalitativ innholdsanalyse av artikler samplet fra massemedia

8 dimensjoner (hovedkategorier) med 1-3 nivåer.



Figur 1.5 Kodebok for kvalitativ innholdsanalyse av massemedia.

1.3 Kilder

Denne rapporten er basert på materiale fra en rekke forskjellige kilder fra Norges lover og forskrifter til oppslag i massemedia. Viktige kilder inkluderer Norges offentlige utredninger (NOU-er), NSMs rapporter om sikkerhetstilstanden og andre publikasjoner, samt informasjon fra virksomheter som er underlagt sikkerhetsloven. En annen sentral kilde er et utvalg av tilsynsrapporter som beskriver avvik og observasjoner NSM har avdekket gjennom sin tilsynsvirksomhet. Prosjektets medarbeidere har også selv vært med på tilsyn som observatører i forbindelse med innsamling av empiri til denne studien. I tillegg har vi deltatt på sikkerhetskonferanser og gjennomført intervjuer med relevante aktører.

Anonymisering av kilder og rapportering av funn

Da sikkerhetstilstanden i Norge og i den enkelte virksomhet er sensitiv informasjon vil vi i denne studien ikke identifisere virksomhetene som er representert i vårt utvalg av tilsynsrapporter eller hvilke virksomheter vi selv har observert. Vi navngir heller ikke intervjuobjektene våre. Det følger av sakens natur at vi i høyest mulig grad anonymiserer hvor konkret informasjon kommer fra. Kravet om anonymisering er derimot ikke uforenlig med denne studiens problemstilling og målsetting. SÅKOV-prosjektets mål om å bidra til å styrke den generelle sikkerhetstilstanden på en helhetlig og hensiktsmessig måte kan best etterleves ved å fremheve nettopp årsaker til mangelfull sikkerhetstilstand som gjør seg gjeldende i de aller fleste virksomheter. Alle funn og observasjoner som presenteres i denne studien omhandler årsaker som gjør seg gjeldende i mange virksomheter; og som, ved utbedring, kan bidra til å styrke sikkerhetstilstanden i Norge så vel som i den enkelte virksomhet. Årsaker som gjør seg gjeldende i én eller noen få virksomheter vil ikke bli omtalt i denne rapporten.

Note om sitater

Som her forklart så legger vi i denne studien stor vekt på anonymisering av kilder. Vi mener likevel at vi med fordel kan illustrere sentrale poeng ved hjelp av sitater fra intervjuobjekter. Vi gjør dette med det forbehold at vi har oppfattet intervjuobjektene riktig, særlig i de situasjonene hvor vi som observatører ikke hadde anledning til å stille oppfølgnings- eller oppklaringsspørsmål til intervjuobjektene. For øvrig gjelder det også her at vi bare inkluderer sitater som illustrerer årsaker som gjør seg gjeldende i mange virksomheter og at vi utelater informasjon som muligens kunne gi en pekepinn om hvem intervjuobjektene er eller hvilke virksomheter de arbeider i.

2 Forebyggende sikkerhet – regelverk og organisasjon

Dette kapittelet tar for seg regelverket for og organisasjonen av det forebyggende sikkerhetsarbeidet i Norge. Kapittelet er inndelt i to deler. Del 2.1 presenterer relevante lover og forskrifter. Denne presentasjonen retter fokus på sikkerhetsloven med forskrifter (del 2.1.1) og den presenterer lover som gjelder spesifikt for olje- og energisektoren som eksempel på sektorlovgivning (del 2.1.2). Del 2.2 presenterer hvordan det forebyggende sikkerhetsarbeidet er organisert. Presentasjonen tar for seg organiseringen av den forebyggende sikkerhetstjenesten (del 2.2.1) og olje- og energisektorens beredskapsorganisasjon (del 2.2.2). Lesere som allerede er kjent med denne tematikken henvises direkte til analysedelen (kapittel 3 og 4) som belyser årsakene til at vi har en dårlig sikkerhetstilstand i Norge.

2.1 Regelverket

Flere av Norges lover vedrører sikkerhet i og for det norske samfunn. Dette bør ses i sammenheng med at *sikkerhet* er et bredt begrep som favner mange forskjellige prosesser. Som et resultat av store endringsprosesser i det internasjonale samfunn over de senere år så er også dagens sikkerhetsbegrep bredere enn noen gang og omfatter territoriell, økonomisk, sosial, politisk og økologisk sikkerhet.[63] I tillegg til at sikkerhetsbegrepet omfatter mange forskjellige områder så innebærer det også eskaleringspotensial; det vil si, sikkerheten skal ivaretas ved kriser og krig så vel som i fredstid.

2.1.1 Sikkerhetsloven med forskrifter

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)[64] har som sitt formål:

> «å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, ivareta den enkeltes rettssikkerhet, og trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste».[65]

Sikkerhetsloven ble vedtatt 20. mars 1998 og trådte i kraft 1. juli 2001.[66] Den erstattet da en rekke fagspesifikke instrukser som kun gjaldt for statsforvaltningen.[67] Sikkerhetsloven ble vedtatt i kjølvannet av skarp kritikk rettet mot de såkalte «hemmelige tjenestene» (se del 2.2 nedenfor) og etter lang tid med «et klart uttrykt behov for bedre samordning og klargjøring av regelverket for forebyggende sikkerhet».[68]

[63] Gahr Støre, Jonas, 2012, Suverenitet, stabilitet og samarbeid. Norsk sikkerhetspolitikk i en brytningstid. Sikkerhetspolitisk linjetale, 16. mai 2012.
[64] LOV 1998-03-20-10 Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven).
[65] Sikkerhetsloven, § 1.
[66] LOV 1998-03-20-10 Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). Tilgjengelig via www.lovdata.no (Sist åpnet 5. april 2013.)
[67] NOU 2006:6. Når sikkerheten er viktigst, 7.1.
[68] NSM, i. d. «Historikk». (Lenke i referanselisten.)

Sikkerhetsloven har et bredt virkeområde og gjelder for (1) forvaltningsorganer, (2) leverandører av varer eller tjenester til et forvaltningsorgan i forbindelse med sikkerhetsgraderte anskaffelser, og (3) ethvert annet rettssubjekt som eier, har kontroll over eller fører tilsyn med skjermingsverdige objekter eller som gis tilgang til sikkerhetsgradert informasjon av et forvaltningsorgan, etter bestemmelse av Kongen.[69] I loven heter det at den gjelder for Svalbard og Jan Mayen i den utstrekning Kongen bestemmer.[70] Inntil nylig forelå det ingen bestemmelse om lovens gyldighet for disse områdene av norsk territorium. I mars 2013 ble det fremmet forslag om at loven skulle gjøres gjeldende også for Svalbard og Jan Mayen[71] og dette ble fastsatt i mai.[72]

Som forvaltningsorgan regnes alle statlige og kommunale organer.[73] En sikkerhetsgradert anskaffelse innebærer at leverandøren av varen/tjenesten vil kunne få tilgang til skjermingsverdig informasjon eller objekt eller anskaffelsen av andre grunner må sikkerhetsgraderes.[74] Et «annet rettssubjekt» kan være alt fra offentlig næringsvirksomhet til foreninger og enkeltpersoner. Organer og andre rettssubjekt som er underlagt sikkerhetsloven blir i loven kalt virksomheter og en «virksomhet» defineres nettopp i kraft av å være underlagt sikkerhetsloven.[75] For å unngå ambivalens som følge av den mindre spesialiserte og mer allmenne bruken av «virksomhet» presiserer denne studien at det er virksomheter som er underlagt sikkerhetsloven det er snakk om når dette ellers ikke fremkommer av teksten. (Det er dog verdt å merke seg at annen litteratur kan rette seg etter sikkerhetslovens spesialiserte bruk av «virksomhet».)

Alle virksomheter som er underlagt sikkerhetsloven plikter å utøve *forebyggende sikkerhetstjeneste*, det vil si: planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet.[76] Sikkerhetsloven presenterer en rekke fagområder som skal inngå i den forebyggende sikkerhetstjenesten: informasjonssikkerhet, objektsikkerhet, personellsikkerhet og sikkerhetsgraderte anskaffelser.

Informasjonssikkerhet. Informasjon som må beskyttes av sikkerhetsmessige hensyn skal sikkerhetsgraderes i henhold til følgende kategorier og kriterier:[77]

> «STRENGT HEMMELIG nyttes dersom det kan få helt avgjørende skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.

[69] Sikkerhetsloven § 2.
[70] Ibid.
[71] FD, 8. mars 2013. Sikkerhetsloven foreslås utvidet til Svalbard og Jan Mayen.
[72] FOR 2013-05-31-558 Forskrift om sikkerhetslovens anvendelsesområde på Svalbard og Jan Mayen.
[73] Sikkerhetsloven gjelder ikke for Riksrevisjonen, Stortinget og dets organer, men den gjelder derimot for domstolene (med særregler iht. LOV-1915-08-13-5 Lov om domstolene (domstolloven) og LOV-1981-05-22-25 Lov om rettergangsmåten i straffesaker (straffeprosessloven).
[74] Sikkerhetsloven § 3.17.
[75] Ibid. § 3.6.
[76] Ibid. § 3.1.
[77] Sikkerhetsloven § 11.

> HEMMELIG nyttes dersom det alvorlig kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
>
> KONFIDENSIELT nyttes dersom det kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
>
> BEGRENSET nyttes dersom det i noen grad kan medføre skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende».[78]

Hvordan sikkerhetsgradert informasjon skal beskyttes er detaljert i Forskrift om informasjonssikkerhet som trådte i kraft samtidig med sikkerhetsloven i juli 2001.[79] Viktige temaer som omhandles i forskriften inkluderer blant annet oppbevaring, deling, journalføring, tilintetgjøring, evakuering av sikkerhetsgradert informasjon og krav til sikkerhetsdokumentasjon.

Objektsikkerhet. Objekter som må beskyttes av sikkerhetsmessige hensyn skal klassifiseres i henhold til følgende kategorier:[80]

> «MEGET KRITISK nyttes dersom det kan få helt avgjørende skadefølger for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse av uvedkommende.
>
> KRITISK nyttes dersom det alvorlig kan skade rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse av uvedkommende.
>
> VIKTIG nyttes dersom det kan skade rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser om objektet får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse av uvedkommende».[81]

Hvordan sikkerhetsgraderte objekter skal beskyttes er detaljert i Forskrift om objektsikkerhet som trådte i kraft 1. januar 2011.[82] Forskriften tar blant annet opp spørsmålet om forholdet til

[78] Sikkerhetsloven § 11.
[79] FOR 2001-07-01-744.
[80] Sikkerhetsloven § 17.
[81] Sikkerhetsloven § 17.
[82] FOR 2010-10-22-1362.

sektorlovgivning og sektormyndigheter, tiltak for å beskytte objektene mot etterretningsvirksomhet osv.

Personellsikkerhet. For å beskytte skjermingsverdig informasjon og objekter skal personer som har tjenstlig behov for tilgang til disse autoriseres (alle grader) og evt. sikkerhetsklareres (for tilgang til informasjon gradert Konfidensielt eller høyere).[83] Krav og prosedyrer vedrørende personellsikkerhet er presentert i Forskrift om personellsikkerhet som trådte i kraft 1. juli 2001.[84] Viktige temaer i denne forskriften er krav om klarering og autorisasjon og personkontroll.

Sikkerhetsgraderte anskaffelser. Ved anskaffelser som innebærer at leverandøren av varen eller tjenesten vil kunne få tilgang til skjermingsverdig informasjon eller objekt eller at anskaffelsen av andre grunner må sikkerhetsgraderes må det inngås en sikkerhetsavtale mellom anskaffelsesmyndigheten og leverandøren. I tilfeller der leverandøren kan få tilgang til informasjon gradert Konfidensielt eller høyere kreves det også leverandørklarering.[85] Krav og rutiner ved sikkerhetsgraderte anskaffelser er presentert i Forskrift om sikkerhetsgraderte anskaffelser som av 1. juli 2001.[86]

Sikkerhetsadministrasjon. I tillegg til de fire fagspesifikke forskriftene finnes det en forskrift til sikkerhetsloven som gjelder på tvers av de forskjellige fagområdene, Forskrift om sikkerhetsadministrasjon som også trådte i kraft 1. juli 2001.[87] I forskriften defineres sikkerhetsadministrasjon som:

> «internkontroll ved gjennomføring av systematiske tiltak for å sikre at virksomhetens aktiviteter planlegges, organiseres, utføres og revideres i samsvar med krav fastsatt i og i medhold av sikkerhetsloven».[88]

Forskriften spesifiserer at den gjelder sikkerhetsadministrasjon for å motvirke sikkerhetstruende virksomhet som spionasje, sabotasje og terrorhandlinger og videre at en virksomhets sikkerhetsadministrasjon skal samordne og ses i sammenheng med forhold som skal motvirke andre tilsiktede hendelser (som alminnelig vinningskriminalitet og skadeverk) og utilsiktede hendelser (som naturkatastrofer og ulykker).[89]

Bestemmelsene som er nedfelt i sikkerhetsloven med forskrifter utgjør grunnsikringen overfor trusler mot Norges selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Alle virksomheter som er underlagt sikkerhetsloven plikter å etterleve disse bestemmelsene og til å implementere sikringstiltak utover disse minimumskravene i henhold til kontinuerlige risikovurderinger som tar hensyn til lokale forhold av sikkerhetsmessig betydning. Risikovurderingene skal også søke å avdekke overflødige og unødvendig overlappende

[83] Sikkerhetsloven § 19.
[84] FOR 2001-6-29-722.
[85] Sikkerhetsloven §§ 27-28.
[86] FOR 2001-7-1-753.
[87] FOR 2001-6-29-723.
[88] Ibid. § 1-2.1.
[89] Ibid. § 1-1.

sikkerhetstiltak samt å finne frem til mer kostnadseffektive tiltak som kan erstatte eksisterende tiltak.[90]

Sikkerhetsloven er et eksempel på en sektorovergripende lov da den gjelder for virksomheter som hører til forskjellige sektorer; private virksomheter så vel som offentlige og både sivile og militære. I tillegg finnes det bestemmelser i sektorlovgivningen som gjelder for det forebyggende sikkerhetsarbeid innen den enkelte sektor. For å illustrere forholdet mellom den sektorovergripende og den sektorspesifikke lovgivningen vil vi her kort presentere lovgiving om forebyggende sikkerhet som gjelder spesifikt for olje- og energisektoren. Som nevnt i 1.1.2 i kapittel 1 er dette en sektor som regnes som særlig utsatt for uønsket aktivitet.[91]

2.1.2 Sektorlovverk: olje- og energisektoren

Olje- og energidepartementet (OED) har det overordnede ansvaret for petroleumsvirksomhet på norsk sokkel og for kraftforsyningen.[92] Vi vil her presentere de mest sentrale lover og forskrifter som legger føringer for det forebyggende sikkerhetsarbeidet innen petroleumsvirksomheten og kraftforsyningen.

Petroleumsvirksomheten på norsk sokkel. Petroleumsvirksomheten reguleres gjennom Lov om petroleumsvirksomhet (petroleumsloven) av 29. november 1996.[93] Lovens kapittel 9 omhandler krav til sikkerhet, herunder opprettelse av sikkerhetssoner rundt og over innretninger, stansing av petroleumsvirksomheten ved fare- og ulykkessituasjoner, og beredskap mot bevisste anslag. § 9-3 om beredskap mot bevisste handlinger stadfester at:

> «Rettighetshaver[94] skal iverksette og opprettholde sikringstiltak for å bidra til å hindre bevisste anslag mot innretninger samt til enhver tid ha beredskapsplaner for slike anslag. Rettighetshaver skal stille innretninger til disposisjon for offentlige myndigheter til øvelser og i nødvendig grad delta i slike øvelser. Departementet kan gi pålegg om gjennomføring av tiltak […]».[95]

Utover dette fokuseres det på beredskap med sikte på fare- og ulykkessituasjoner, det vil si situasjoner som kan føre til tap av menneskeliv, personskade, forurensing eller store materielle skader.[96] Sikring mot sabotasje, spionasje/etterretning og terrorvirksomhet nevnes ikke spesifikt i loven. Sikkerhetstrussel nevnes kun i forbindelse med Kongens myndighet til å gi immunitet og særlige privilegier til utenlandske statsmenn, i forbindelse med tiltak for å forebygge og gripe inn overfor ulovlige handlinger som innebærer en sikkerhetstrussel for petroleumsvirksomheten.[97]

---

[90] Ibid. § 4-2.
[91] NSM, 2012, Rapport om sikkerhetstilstanden, s. 3.
[92] OED, i/d, Beredskap i enrgisektoren. (regjeringen.no)
[93] LOV 1996-11-29-72.
[94] Fysisk eller juridisk person eller personer som etter loven (eller tidligere lovgivning) innehar tillatelse til å undersøke, utvinne, transportere, eller utnytte petroleum. Ibid. § 1-6.
[95] Ibid. § 9-3.
[96] Ibid. § 9-2.
[97] Ibid. § 10-15.

Petroleumsloven har et klart fokus på HMS og økonomiske verdier. Som det fremkommer i kapittel 10 om alminnelige bestemmelser: «Petroleumsvirksomheten skal ivareta hensynet til sikkerhet for personell, miljø og de økonomiske verdier innretninger og fartøyer representerer, herunder driftstilgjengelighet».[98] Dette fokuset er også retningsgivende for det oppdraget som gis rettighetshavere som er pålagt «å påse at virksomheten kan utøves på forsvarlig måte i samsvar med gjeldende lovgivning og under ivaretakelse av hensynet til *god ressursforvaltning, helse, miljø og sikkerhet*» (uthevelse lagt til).[99]

Selv om fokus synes å være på HMS og «safety» og ikke i særlig grad på «security» er det verdt å nevne at § 9-3 som er sitert ovenfor er en tilføying av 2003,[100] en tilføying som supplerer fokuset på utilsiktede uønskede hendelser med bevisste handlinger. Vi har her bemerket at sabotasje, spionasje, etterretning og terrorvirksomhet ikke nevnes i loven. Denne typen trusler var likevel et fremtredende tema i departementets lovforslag om endring i petroleumsloven og en ny § 9-3:

> «Departementet ser behov for å styrke beredskapen for produksjons- og forsyningssikkerheten på sokkelen. [...] Det foreslås lovfestet at rettighetshaver til enhver tid skal ha beredskapsplaner for bevisste anslag. Disse planene må omfatte tiltak som rettighetshaver skal iverksette for å bidra til å hindre drifts- og leveringsbrudd i en slik situasjon. Tidligere var det faren for krig som utgjorde den relevante trussel. I dag er det faren for bevisste skadehandlinger som terroraksjoner, spionasje, sabotasje og ulike former for krigslignende handlinger rettet mot virksomheten, som er mest fremtredende».[101]

For å sikre forsyningen av petroleum og petroleumsprodukter kan importører og produsenter av petroleumsprodukter og biodrivstoff pålegges å opprette lager av disse produktene i henhold til Lov om beredskapslagring av petroleumsprodukt.[102] OED kan innkreve gebyr ved brudd på loven og pålegg gitt i henhold til loven på opptil 10 millioner per vedtak.[103] Detaljene rundt lagringsplikten er beskrevet i Forskrift om beredskapslagring av petroleumsprodukt.[104] Kort oppsummert plikter produsenter og importører av petroleumsprodukter å holde et beredskapslager som tilsvarer Norges normalforbruk for 20 dager. Formålet er å sikre forsyningen til det norske markedet skulle leveransene bli forstyrret eller som tilskudd til en samordnet krisehåndtering innen rammene av Det internasjonale energibyrået.[105] De lagringspliktige selskapene plikter å opplyse om import, salg og lagerholdning samt å innrapportere oversikt over lagerholdet fire ganger årlig sammen med en erklæring om at lagringsplikten er oppfylt.[106]

---

[98] Ibid. § 10-1.
[99] Ibid. § 10-2.
[100] LOV 2003-27-06-68. Lov om endring i lov 29. november 1996 nr. 72 om petroleumsvirksomhet.
[101] Ot. prp. nr. 46 (2002-2003), 2.6 Beredskap mot bevisste anslag (Ny § 9-3).
[102] LOV 2006-08-18-61, § 1.
[103] Ibid. § 2.
[104] FOR 2006-09-01-1019.
[105] OED, 2007, Beredskapslagring av petroleumsprodukter.
[106] Ibid.

Kraftforsyningen. Kraftforsyningen reguleres gjennom Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven) av 29. juni 1990.[107] Lovens kapittel 9 omhandler beredskap, herunder kraftforsyningens beredskapsorganisasjon, beredskapstiltak og informasjonssikkerhet. (Førstnevnte punkt vil bli behandlet under 2.2 nedenfor.) I § 9-2 heter det at:

> «Den som helt eller delvis eier eller driver anlegg eller system som er eller kan bli av vesentlig betydning for produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, plikter å sørge for effektiv sikring og beredskap og iverksette tiltak for å forebygge, håndtere og begrense virkningene av ekstraordinære situasjoner […] og for å gjenopprette normal situasjon. Beredskapsmyndigheten kan gi forskrift eller treffe enkeltvedtak om beredskapstiltak for å forebygge, håndtere eller begrense virkningene av ekstraordinære situasjoner […]».

> «Den som pålegges beredskapstiltak plikter å gjennomføre tiltaket for egen regning og risiko. Når det anses nødvendig kan beredskapsmyndigheten uten hensyn til tidligere pålegg treffe vedtak om at nye eller endrede beredskapstiltak skal settes i verk».[108]

Når det gjelder informasjonssikkerhet så fastsetter loven at alle enheter som inngår i kraftforsyningens beredskapsorganisasjon (se 2.2. nedenfor) «skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen. Enhetene skal kartlegge hvilken informasjon som er sensitiv, hvor den befinner seg og hvem som har tilgang til den. Det skal etableres effektiv avskjerming og beskyttelse av sensitiv informasjon. Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen».[109]

I tillegg til Energilovens bestemmelser om forebyggende sikkerhet og beredskap finnes det en egen forskrift på temaet, Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften).[110] Denne relativt nye forskriften, av 7. desember 2012, tar blant annet for seg klassifisering og sikringstiltak, informasjonssikkerhet og beskyttelse av driftskontrollsystemer.

Ifølge Beredskapsforskriften plikter den som eier eller driver et anlegg, system eller annet som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting i ekstraordinære situasjoner, å sikre det mot uønskede hendelser og handlinger, herunder adgang for uvedkommende.[111] Videre heter det at:

---

[107] LOV 1990-06-29-50.
[108] Ibid. § 9-2.
[109] Ibid. § 9-3.
[110] FOR 2012-12-07-1157.
[111] Med anlegg menes «bygg og andre ressurser». Ibid. § 5-1.

«Det er den enkelte virksomhets ansvar å planlegge, gjennomføre og vedlikeholde sikringstiltak etter anleggets eller systemets type, oppbygging og funksjon. Alle anlegg m.m. som nevnt i første ledd skal holdes i funksjonsdyktig stand og skal så langt som mulig virke etter sin hensikt under ekstraordinære forhold. Det skal særlig tas hensyn til ekstraordinære forhold som:
- uvær og annen naturgitt skade
- brann og eksplosjoner
- alvorlig teknisk svikt
- innbrudd, hærverk, sabotasje og andre kriminelle handlinger».[112]

I likhet med sikkerhetslovens bestemmelser for skjermingsverdige objekter så skal anlegg m.m. som er av vesentlig betydning for kraftforsyningen klassifiseres. Her benyttes klasse 1-3, hvorav klasse tre inneholder de anleggende som er av størst betydning for kraftforsyningen. Klassene defineres ved å liste typene/kapasitetene de omfatter, eksempelvis:[113]

«Klasse 1 omfatter:
a. Kraftstasjon med samlet installert generatorytelse på minst 25 MVA.
b. Transformatorstasjon med samlet hovedtransformatorytelse på minst 10 MVA.
[...]
Klasse 2 omfatter:
a. Kraftstasjon med samlet installert generatorytelse på minst 100 MVA og kraftstasjoner på minst 100 MVA plassert i dagen.
b. Transformatorstasjon med samlet hovedtransformatorytelse på minst 50 MVA og høyeste spenningsnivå på minst 30 kV.
[...]
Klasse 3 omfatter:
a. Kraftstasjon i fjell med samlet installert generatorytelse på minst 250 MVA.
b. Transformatorstasjon med samlet hovedtransformatorytelse på mer enn 100 MVA og bygget for et høyeste spenningsnivå på minst 200 kV og transformering til sekundært spenningsnivå i nett på minst 30 kV.
[...]»[114]

Beredskapsforskriften fastsetter at alle anlegg som er klassifisert skal prosjekteres, plasseres, utføres, utrustes, sikres, driftes og holdes i stand slik at risiko for skade, havari og funksjonssvikt og andre uønskede hendelser og handlinger blir minst mulig.[115] Krav til sikringstiltak for de forskjellige klassene presentes (§§ 5-4 - 5-6) og detaljeres videre i vedlegg til forskriften, en til hver av klassene (Vedlegg 1-3).

I forlengelsen av Energilovens bestemmelser om informasjonssikkerhet og beskyttelse av sensitiv informasjon presenterer Beredskapsforskriften en rekke regler og prosedyrer for hvordan denne informasjonen skal beskyttes, herunder sikkerhetsinstruks, anskaffelser og personkontroll (se

[112] Ibid. § 5-1.
[113] Ibid. § 5-2.
[114] Flere eksempler innenfor de ulike klassene listes opp i § 5-2.
[115] Ibid. 5-3.

kapittel 6.) I likhet med klassene for viktige anlegg m.m. defineres sensitiv informasjon ved eksempler i § 6-2:

> «Med sensitiv informasjon menes spesifikk og inngående opplysninger om energiforsyningen som kan brukes til å skade anlegg eller påvirke funksjoner som har betydning for energiforsyningen, herunder:
>
> a. Alle system som ivaretar viktige driftskontrollfunksjoner, herunder også nødvendig hjelpeutstyr som samband.
> b. Detaljert informasjon om energisystemet, herunder enlinjeskjema, med unntak av enlinjeskjema for mindre viktige produksjonsanlegg.
> c. Detaljert informasjon om klassifiserte transformatorstasjoner med tilhørende koblingsanlegg, herunder anleggets oppbygning og drift.
> [...]» [116]

Når det gjelder beskyttelse av driftskontrollsystemer fastsetter forskriften at alle virksomheter med driftskontrollsystemer skal sørge for at disse til enhver tid virker etter sin hensikt og at de skal beskytte systemene mot alle typer uønskede hendelser, herunder mot alle typer uautorisert tilgang for å hindre misbruk og spredning av skadelig programvare og lignende.[117] Viktige temaer som behandles i den forbindelse men som vi ikke går inn på her inkluderer kontroll med brukertilgang og utstyr, håndtering av feil, sårbarheter og sikkerhetsbrudd osv.

Også her er sabotasje den eneste eksplisitt nevnte typen sikkerhetstruende virksomheten den forebyggende sikkerheten søker å forebygge. Likevel synes det forebyggende sikkerhetsarbeidet å være langt mer tilstedeværende i regelverket for kraftforsyningen enn det som var tilfelle i regelverket for petroleumsvirksomheten.

En umiddelbar observasjon hva gjelder sektorregelverket er at det finnes betydelig variasjon selv innenfor den ene sektoren som vi her har brukt som eksempel, og at det derfor vil være naturlig at forholdet mellom sikkerhetsloven og sektorregelverket vil fremstå som ulikt avhengig av hvilket område av sektorregelverket man ser på. Vi vil komme tilbake til dette i kapittel 3 (3.2.8 om mangler i regelverket). Her vil vi nå rette fokus på organisasjonen av det forebyggende sikkerhetsarbeidet.

Andre relevante regelverk

Beredskapsloven, eller Lov om særlige rådgjerder under krig, krigsfare og liknende forhold, gjelder hvis Norge skulle være i krig, om krig truer eller om rikets selvstendighet eller sikkerhet er i fare.[118] Andre relevante lover inkluderer Lov om forsvarshemmeligheter,[119] Lov om oppfinnelser av betydning for rikets forsvar[120] og Lov om kommunal beredskapsplikt, sivile

[116] Flere eksempler listes opp i § 6-2.
[117] Ibid. § 7-1.
[118] LOV-1950-12-15-7 Lovom særlige rådgjerder under krig, krigsfare og liknende forhold.
[119] LOV 1914-08-18-03 Lovom forsvarshemmeligheter.
[120] LOV 1953-06-26-8 Lovom oppfinnelser av betydning for rikets forsvar.

beskyttelsestiltak og Sivilforsvaret (Sivilbeskyttelsesloven).[121] Sivilbeskyttelsesloven har som formål å beskytte liv, helse, miljø, materielle verdier og kritisk infrastruktur ved bruk av ikke-militær makt når riket er i krig, når krig truer, når rikets selvstendighet og sikkerhet er i fare, og ved uønskede hendelser i fredstid (§ 1).

For å håndtere krisesituasjoner har vi et Nasjonalt beredskapssystem (NBS) som består av et Sivilt beredskapssystem (SBS) og et Beredskapssystem for forsvarssektoren (BFF). NBS ble innført i 2005 og er harmonisert med NATOs Crisis Response System (NCRS). Terroranslagene mot World Trade Center og Pentagon i 2001 synliggjorde behovet for et beredskapssystem som kan håndtere hendelser i alle deler av krisespekteret, tettere samarbeid mellom militær og sivil sektor og en lavere terskel for å ta systemet i bruk. NBS er Regjeringens krisehåndteringsverktøy og inneholder konkrete forhåndsplanlagte tiltak og handlemåter som kan iverksettes ved kgl. res. eller av ansvarlig statsråd for å forebygge eller redusere skadeomfanget ved kriser, som for eksempel naturkatastrofer og terroranslag eller ved krig.[122]

Videre finnes en rekke lover og forskrifter som tar for seg HMS-hensyn innen for eksempel strålevern, industrivern, arbeidsmiljø, brann- og eksplosjonsfare etc. Det er i hovedsak dette regelverket vi forbinder med sikkerhet i fredstid, det vil si sikkerhet i betydningen «safety» heller enn «security». Selv om HMS er et mer fremtredende tema i en normaltilstand uten krig og i stor grad også uten kriser så er «security» aspektet likevel en relevant problemstilling og det er her sikkerhetsloven med forskrifter kommer inn i bildet.

2.2 Organisasjonen

Som presentert innledningsvis i 1.2 så finnes det en rekke forskjellige lover som omhandler sikkerhet. Vi vil her holde oss til de mest sentrale delene av regelverket som omhandler forebyggende sikkerhet som presentert i den foregående delen, det vil si, den forebyggede sikkerhetstjenesten (2.2.1) og olje- og energisektorens beredskapsorganisasjon representert ved kraftforsynings beredskapsorganisasjon (2.2.2).

2.2.1 Den forebyggende sikkerhetstjenesten

Den forebyggende sikkerhetstjenesten kan med fordel inndeles i tre nivåer: overordnede myndighetsorganer, virksomheter som er underlagt sikkerhetsloven og sikkerhetsorganisasjonen i disse virksomhetene. Her følger en presentasjon av disse tre nivåene.

2.2.1.1 Overordnede myndighetsorganer

Nasjonal sikkerhetsmyndighet. Da sikkerhetsloven trådte i kraft i 2001 opprettet den en funksjon, Nasjonal sikkerhetsmyndighet. NSM fikk da ansvaret for å koordinere de forebyggende sikkerhetstiltakene og å kontrollere sikkerhetstilstanden. NSM ble også utøvende organ i forholdet til andre land og organisasjoner.[123] Først ble denne funksjonen lagt til Forsvartes

[121] LOV-2010-06-25-45 Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven).
[122] NOU 2006:6, Når sikkerheten er viktigst, 11.6.2.5 Kriseledelse ved terror- og sabotasjesituasjoner.
[123] Sikkerhetsloven, § 8.

Overkommando/Sikkerhetsstaben (FO/S). 1. januar 2003 ble NSM opprettet som et selvstendig direktorat slik vi kjenner det i dag. NSM ivaretar en rekke sentrale oppgaver innen den forebyggende sikkerhetstjenesten, herunder: å føre tilsyn med sikkerhetstilstanden i virksomhetene som er underlagt sikkerhetsloven og å gi informasjon, råd og veiledning.[124] NSM gjennomfører revisjoner basert på standarden ISO 19011:2002. Hensikten med revisjonene er å vurdere om tilsynsobjektene beskytter skjermingsverdig informasjon og skjermingsverdige objekter i samsvar med bestemmelsene gitt i eller i medhold av sikkerhetsloven. I hovedsak gjennomfører NSM tilsyn med virksomheters styringssystem og ett eller flere av fagområdene personellsikkerhet, dokumentsikkerhet, informasjonssystemsikkerhet, fysisk sikring, kryptosikkerhet, kurerposttjeneste og sikkerhetsgraderte anskaffelser. Tilsynsområdet er nylig utvidet til også å gjelde objektsikkerhet. Lengden på tilsynet avhenger av størrelsen på virksomheten og antallet fagområder som skal revideres, men tilsynet pågår gjerne over flere dager. Resultater fra intervjuer og stikkprøver hos virksomhetene danner grunnlag for å skrive revisjonsbevis. Endelig avvik og observasjoner gjøres tilgjengelig gjennom NSMs tilsynsrapporter.

Samme år som NSM ble opprettet som et direktorat kom også Forskrift om fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet.[125] Forskriften stadfester at:

1. «Justisministeren har et overordnet ansvar for den forebyggende sikkerhetstjeneste i sivil sektor.
2. Forsvarsministeren har et overordnet ansvar for den forebyggende sikkerhetstjeneste i militær sektor.
3. Nasjonal sikkerhetsmyndighet skal på Justisministerens og Forsvarsministerens vegne ivareta de utøvende funksjoner for den forebyggende sikkerhetstjeneste.
4. Forsvarsdepartementet gis det administrative ansvaret for Nasjonal sikkerhetsmyndighet.
5. Forsvarsdepartementet gis forvaltningsansvaret for lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven)».[126]

Forsvarsdepartementet (FD) og Justis- og beredskapsdepartementet (JD). FD og JD har altså det overordnede ansvaret for den forebyggende sikkerhetstjenesten i hhv forsvarssektoren og sivil sektor. NSM har en dobbel rapporteringslinje og rapporterer til JD på sivile anliggende og til FD hva angår militære anliggende. Selve forvaltningsansvaret for sikkerhetsloven ligger hos FD som også har det administrative ansvaret for NSM.

NSM, FD og JD rapporterer til to organer i tillegg til Regjeringen; Riksrevisjonen og Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjenestene (EOS-utvalget). Riksrevisjonen er Stortingets revisjons- og kontrollorgan. Dens oppgave er å undersøke om Stortingets krav til og mål for forvaltningen etterleves gjennom regnskapsrevisjon,

[124] Ibid. § 9.
[125] FOR 2003-07-04-900.
[126] Ibid. Artikkel I.

forvaltningsrevisjon og selskapskontroll. Riksrevisjonen har med andre ord ikke ansvar for revisjon og kontroll av det forebyggende sikkerhetsarbeidet som sådan, det er den forebyggende sikkerhetstjenestens organisasjon som faller inn under Riksrevisjonens ansvars- og virkeområde.

EOS-utvalget er ansvarlig for kontroll av all etterretnings-, overvåknings- og sikkerhetstjeneste i sivil og militær forvaltning. Disse tjenestene utøves i dag av NSM, PST, E-tjenesten og Forsvarets sikkerhetsavdeling (FSA). PST, E-tjenesten og FSA er ansvarlige for hver sitt fagområde hhv. nasjonal etterretning, utenlands etterretning og forebyggende sikkerhet i Forsvaret. Sammen med NSM utgjør de EOS-tjenestene - også kjent som de «hemmelige tjenestene». EOS-utvalget ble opprettet i 1996 etter at Stortinget året for vedtok Lov om kontroll med EOS-tjenestene (EOS-loven).[127]

EOS-utvalgets kontroll av EOS-tjenestene har som formål å kartlegge om og forebygge at tjenestenes aktiviteter øver urett mot noen eller utilbørlig skader samfunnet og videre å påse at aktivitetene holdes innenfor rammen av relevante lover og regelverk.[128] Med dette formål for øye skal utvalget føre regelmessig tilsyn med tjenestene, undersøke alle klager fra enkeltpersoner og organisasjoner, og på eget initiativ ta opp saker EOS-utvalget selv regner som viktige og saker som er gjenstand for offentlig kritikk.[129] Minimumsantallet inspeksjoner i de forskjellige tjenestene er fastsatt i EOS-instruksen.[130] For NSMs vedkommende heter det at tilsynsvirksomheten skal omfatte minst kvartalsvise inspeksjoner.[131]

2.2.1.2 Virksomheter underlagt sikkerhetsloven

Som det ble beskrevet i 2.1.1 ovenfor er det tre kategorier virksomheter som er underlagt sikkerhetsloven, (1) forvaltningsorganer, (2) leverandører ved sikkerhetsgraderte anskaffelser og (3) andre rettssubjekter etter særskilt vedtak. Vi vil her gi en kort presentasjon av hver av disse kategoriene og noen av deres virksomheter.

Forvaltningsorganer. Den første av de tre kategoriene virksomheter som er underlagt sikkerhetsloven er forvaltningsorganene. Det vil si alle organer som er en del av statsforvaltningen, fylkesforvaltningen og kommuneforvaltningen. Dette inkluderer FD og JD på lik linje med alle andre departementer. Det samme gjelder deres underliggende etater herunder NSM som sammen med Forsvaret, Forsvarets forskningsinstitutt (FFI) og Forsvarsbygg (FB) er en av FDs underliggende etater. Det vil si at FD og JD befinner seg på to steder samtidig i den forebyggende sikkerhetstjenestens hierarkiske struktur: som en av de mange virksomhetene som er underlagt sikkerhetsloven og som NSM fører tilsyn med, og som de to departementene som har det overordnede ansvaret for den forebyggende sikkerhetstjenesten i hhv. forsvarssektoren og sivil sektor. I tillegg til disse to rollene har FD, som nevnt, også det administrative ansvaret for NSM.

[127] LOV 1995-02-02-7
[128] Ibid. § 2.
[129] Ibid. § 3.
[130] FOR 1995-05-30-4295. Instruks om kontroll med etterretnings-, overvåknings- og sikkerhetstjenste.
[131] Ibid. § 11.

Leverandører ved sikkerhetsgraderte anskaffelser. Denne kategorien inkluderer alle virksomheter som gjennom leveranser til forvaltningen får tilgang til skjermingsverdig informasjon eller objekter. De fleste sikkerhetsgraderte anskaffelser i Norge finner sted i militær sektor med Forsvaret eller andre etater under FD som anskaffelsesmyndighet. Langt færre avtaler om sikkerhetsgraderte anskaffelser blir inngått i sivil sektor. I sivil sektor er det i hovedsak innen justissektoren, statlig eiendomsforvaltning og offentlige anskaffelser av foto- og kartmateriell at det gjennomføres sikkerhetsgradert anskaffelser.[132]

Andre rettssubjekter underlagt sikkerhetsloven etter særskilt vedtak. Den tredje og siste kategorien virksomheter som er underlagt sikkerhetsloven er de som er underlagt loven ved enkeltvedtak. Dette fordi de eier, har kontroll over eller fører tilsyn med skjermingsverdige objekter eller fordi de får tilgang til sikkerhetsgradert informasjon av et forvaltningsorgan. Per i dag (april 2013) gjelder dette følgende virksomheter:

- NSB AS
- CargoNet AS (inngår i NSB-konsernet)
- ROM Eiendom AS (inngår i NSB-konsernet)
- Flytoget AS
- Posten Norge AS
- Telenor ASA
- Ventelo Networks AS
- Avinor AS
- Norsk senter for informasjonssikring (NorSIS)
- Næringslivets sikkerhetsråd (NSR)
- Aerospace Industrial Maintenance Norway (AIM Norway)
- Det kongelige hoff

Selv om det ikke er veldig mange virksomheter som hører til denne kategorien så er dette en kategori som har vokst kraftig de siste årene. Til sammenligning var det kun NSB AS, CargoNet AS, Posten Norge AS, Telenor ASA og NorSIS som var listet under denne kategorien i NOU-en «Når sikkerhet er viktigst» i 2006.[133]

2.2.1.3 Sikkerhetsorganisasjonen i virksomhetene

Virksomheter som er underlagt sikkerhetsloven plikter å opprette en sikkerhetsorganisasjon som står i forhold til virksomheten og å avsette de nødvendige ressursene til dette formålet.[134] Virksomhetens leder har ansvaret for å utpeke en Sikkerhetsleder (SL) med stedfortreder og et tilstrekkelig antall personer i forhold for å ta vare på virksomhetens sikkerhetsbehov og de forskjellige fagområdene som er relevante for virksomhetens aktiviteter. Sikkerhetslederen og de

[132] FD, Høringsbrev av 15. november 2012, Forslag til ny forskrift om forsvars- og sikkerhetsanskaffelser.
[133] NOU 2006:6. Det kan forøvrig bemerkes at NOU-en ikke inkluderte Avinor AS i denne listen fordi Avinor ble regnet som et forvaltningsorgan, dette til tross for at selskapet ble omorganisert fra å være en statlig forvaltningsbedrift til å bli et aksjeselskap allerede i 2003.
[134] Forskrift om sikkerhetsadministrasjon, § 2-1 og 2-5.

andre i sikkerhetsorganisasjonen skal koordinere, gi råd og kontrollere sikkerheten blant de foresatte og den enkelte medarbeider.[135]

Virksomhetene som har kryptomateriell plikter å etablere en kryptosikkerhetsorganisasjon i henhold til Forskrift om informasjonssikkerhet. Kryptosikkerhetsorganisasjonen skal minst bestå av en Kryptosikkerhetsleder med stedfortreder og en kryptoforvalter med stedfortreder. Det skal også etableres en ordning for henting og levering av kryptomateriell med kurerpost. Personellet i kryptosikkerhetsorganisasjonen skal ha den nødvendige faglige kompetansen, de skal ha den nødvendige myndigheten i virksomheter og skal kunne ivareta funksjonen i minst ett år. Det presiseres videre at personellet ikke skal pålegges andre oppgaver i den utstrekning at det fratar dem muligheten til å ivareta funksjonen i samsvar med de gjeldende sikkerhetsbestemmelsene.[136] Forøvrig er NSM selv nasjonal distribusjonsmyndighet for kryptomateriell, leverandør av kryptosikkerhetstjenester og produsent av kryptonøkler.[137]

Virksomheter som har informasjonssystemer som behandler sikkerhetsgradert informasjon plikter å etablere en datasikkerhetsorganisasjon. Denne organisasjonen skal ha tilstrekkelig myndighet, kompetanse og ressurser til å ivareta sikkerheten i systemene og skal minst bestå av en Datasikkerhetsleder (DSL) med stedfortreder.[138]

Virksomhetens sikkerhetsorganisasjon skal være i stand til å håndtere generelle og tverrfaglige sikkerhetsmessige problemstillinger.[139] Virksomhetens leder skal så langt det er mulig fordele oppgaver og ansvar slik at muligheten for at enkeltpersoner kan undergrave sikkerheten i virksomheten er minst mulig. Utøvende og kontrollerende oppgaver innen sikkerhet skal fordeles på forskjellige medarbeidere.[140] Sikkerhetsleder skal ha direkte tilgang til virksomhetens leder i viktige sikkerhetssaker. I virksomheter med kryptosikkerhetsleder eller en klareringsansvarlig skal disse også ha direkte tilgang til virksomhetens leder. Lederen kan bestemme at dette også skal gjelde for ansvarlige for andre fagområder.[141]

[135] Ibid. § 2-5.
[136] Forskrift om informasjonssikkerhet, § 7-6.
[137] Ibid. § 7-2.
[138] Forskrift om informasjonssikkerhet, § 5-14.
[139] Forskrift om sikkerhetsadministrasjon, § 2-5.
[140] Ibid. § 2-4.
[141] Ibid. § 2-5.

Figur 2.1 Sikkerhetsorganisasjonen. Eksempel på en mulig sikkerhetsorganisasjon i en virksomhet med kryptomateriell og informasjonssystemer som behandler sikkerhetsgradert informasjon.

I Forskrift om sikkerhetsadministrasjon fastsettes det videre at enhver foresatt i virksomheten har ansvar for sikkerheten innen sitt ansvars- og myndighetsområde og for å påse at deres underordnedes adferd bidrar til å ivareta sikkerheten i virksomheten.[142] Det er den enkelte medarbeiders ansvar, det være seg faste eller midlertidig ansatte eller innleid personell, å medvirke til en effektiv sikkerhetstjeneste. Dette innebærer blant annet å kjenne til virksomhetens sikkerhetsorganisasjon og å rapportere om sikkerhetstruende hendelser til sin nærmeste overordnede, virksomhetens leder eller den lederen har bemyndiget.[143]

Det overordnede ansvaret for den forebyggende sikkerhetstjenesten ligger hos virksomhetens leder som også er ansvarlig for den forebyggende sikkerhetstjenesten i underliggende virksomheter.[144]Ansvarsforholdet strekker seg også til leverandører og sikkerhetsorganisasjonen er blant de kriterier som vurderes opp mot en leverandørklarering for en potensiell leverandør.[145]

2.2.2 Olje- og energisektorens beredskapsorganisasjon

Petroleumsloven gir ingen særlige føringer for en organisasjon som skal ivareta forebyggende sikkerhet eller beredskapsarbeid. Lovens krav til ressursforvaltning og HMS ivaretas gjennom de ordinære virksomhetsorganisasjonene med Petroleumstilsynet som tilsynsorgan for HMS og beredskap. Vi vil her fokusere på kraftforsyningens beredskapsorganisasjon som i tillegg til beredskap også har ansvar for forebyggende sikkerhetsarbeid innen kraftsektoren.

[142] Ibid. § 2-2.
[143] Ibid. § 2-3.
[144] Ibid. § 2-1.
[145] Forskrift om sikkerhetsgraderte anskaffelser, § 3-1.

Ifølge Energiloven skal kraftforsyningen ha en beredskapsorganisasjon, Kraftforsyningens beredskapsorganisasjon (KBO), bestående av:

> «de enheter som eier eller driver anlegg eller annet som har vesentlig betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme. Beredskapsmyndigheten kan ved forskrift eller enkeltvedtak fastsette hvilke enheter som skal inngå i KBO».[146]

Alle enhetene i KBO videre sørger for at virksomheten er innrettet på en slik måte og med slike ressurser som er nødvendig for å ivareta ansvar og oppgaver etter kapittel 9 i Energiloven.[147] Videre heter det at:

> «Beredskapsmyndigheten skal samordne beredskapsarbeid og utpeke en den samlede ledelse i KBO. I ekstraordinære situasjoner som kan skade eller hindre produksjon, omforming, overføring, omsetning eller fordeling av elektrisk energi eller fjernvarme, kan KBO pålegges oppgaver og plikter. Det samme gjelder i ekstraordinære situasjoner hvor skade eller hindring som nevnt i første punkt har oppstått. Beredskapsmyndigheten kan under beredskap og i krig underlegge kraftforsyningen KBO. Kraftforsyningen plikter å følge de pålegg som gis og gjennomføre de tiltak som kreves».[148]

Beredskapsforskriften utdyper videre organisering av KBO som bestående av KBO-enhetene, kraftforsyningens distriktssjefer (KDS), beredskapsmyndigheten og (under beredskap og krig også) kraftforsyningens sentrale ledelse (KSL).[149] Beredskapsmyndigheten står for inndeling i distrikter og utpeking av KDS med stedfortredere. KDS skal bidra med tilrettelegging for hensiktsmessig samarbeid om forebygging og håndtering av ekstraordinære situasjoner.

Beredskapsorganisasjonen fortsetter også innenfor virksomhetene som plikter å opprette følgende funksjoner: en beredskapsleder som utpekes av virksomhetens leder og som sørger for nødvendig planlegging og utøvelser av beredskapsarbeidet, en beredskapskoordinator som skal fungere som kontaktpunkt til beredskapsmyndigheten og en IKT-sikkerhetskoordinator som skal være faglig kontaktpunkt til beredskapsmyndigheten innen IKT-sikkerhet.[150]

[146] Energiloven, § 9-1.
[147] Ibid.
[148] Ibid.
[149] Beredskapsforskriften, § 3-1 og 3-5.
[150] Ibid. § 2-2.

3 Hvilke årsaker ligger til grunn for Norges mangelfulle sikkerhetstilstand?

Gjennom de fem delanalysene har vi samlet inn materiale fra forskjellige kilder som belyser årsakene til at vi har en dårlig sikkerhetstilstand i Norge. Vi skiller mellom eksterne og interne årsaker. *Eksterne årsaker* er faktorer som ligger utenfor vår innflytelse og som vi vanskelig kan utbedre, men som vi like fullt må være bevisst. *Interne årsaker* er faktorer som vi selv har muligheten til å påvirke, eksempelvis gjennom å styrke det forebyggende sikkerhetsarbeidet. Aller først gis en kort beskrivelse av eksterne årsaker (kapittel 3.1.), før vi retter blikket mot de interne årsakene (kapittel 3.2.) som tillegges mest vekt i denne analysen.

3.1 Eksterne årsaker

Sikkerhetstilstanden er et resultat av risikobildet og det forebyggende sikkerhetsarbeidet. At vi i denne studien fokuserer på det forebyggende sikkerhetsarbeidet har sin naturlige forklaring i at det er her vi har mulighet til å forbedre sikkerhetstilstanden. Trusselbildet er til en viss grad avhengig av hvordan vi som nordmenn oppfører og uttaler oss, men i det store og hele så er trusselbildet utenfor vår kontroll. Det vil ikke si at endringer i trusselbildet ikke er å regne som årsaker for hvorfor vi har en dårlig sikkerhetstilstand i Norge. Tvert imot, mye av den negative utviklingen henger sammen med trusselbildet. Likevel, slike eksterne årsaker kan ikke enkelt utbedres. Nedenfor gis en kort presentasjon av trusselbildets bidrag til at sikkerhetstilstanden er slik den er.

Verdiene våre. I takt med samfunnsutviklingen blir verdiene våre stadig flere og stadig mer avhengig av hverandre. Utstrakt bruk av IKT står sentralt i denne utviklingen. Samfunnet vårt er på mange måter et informasjonssamfunn og det er mye man kan utrette, også i negativ forstand, ved å kombinere informasjon og noen tastetrykk.

Trusselbildet. Utviklingen i det globale samfunnet har ført til at trusselbildet har blitt stadig mer komplisert; det blir mindre oversiktlig og mindre forutsigbart. Dette vanskeliggjør oppgaven med å gjøre seg kjent med trusselen og trusselaktørene for å kunne motvirke dem. Inntil helt nylig var et terrorangrep på norsk jord en fjern forestilling for mange. Dette gjenspeilet seg i det forebyggende arbeidet som er blitt kritisert i etterkant av 22. juli 2011.

Sårbarheter. De økende verdiene og det uforutsigbare trusselbildet gjør oss sårbare. Vi har mer å beskytte samtidig som at de vi skal beskytte oss mot blir vanskeligere å identifisere og kan gjennomføre aksjoner også fra den andre siden av kloden.

I 2013 gav E-tjenesten, PST og NSM ut en samordnet vurdering som oppsummerer følgende: «Norge har mange vitale verdier og interesser som må beskyttes. Erfaring forteller oss at trusselaktører har intensjon om og evne til å utnytte eksisterende og potensielle sårbarheter ved verdier og funksjoner gjennom et bredt spekter av metoder og virkemidler».[151]

[151] E-tjenesten, PST og NSM, 2013, Trusler og sårbarheter 2013, Samordnet vurdering fra E-tjenesten, PST og NSM, s. 14.

3.2 Interne årsaker

For at vi skal ha en tilfredsstillende sikkerhetstilstand må sikringstiltakene til enhver tid ta høyde for sårbarhetene. Det er på dette området vi selv har muligheten til å påvirke sikkerhetstilstanden ved å styrke oppfølgingen av det forebyggende sikkerhetsarbeidet. I det som følger vil vi presentere et utvalg av årsaker til at vi har en utilfredsstillende sikkerhetstilstand i Norge. Årsakene som presenteres her er blitt identifisert i de fem delanalysene vi har gjennomført. Vi har gjort vårt utvalg basert på følgende kriterier: årsakene er *allmenngyldige* og de er *konkrete*. Med allmenngyldig mener vi at dette er årsaker som går igjen i et stort antall virksomheter og at vi har funnet empiri på dem i flere av de fem delanalysene. At årsakene er konkrete er viktig med tanke på forbedringspotensialet. Vi har valgt å presentere årsaker som kan adresseres direkte uten at de trenger å bli operasjonalisert på noe vis. Dette er et bevisst valg som vi mener supplerer senere års fokus på «sikkerhetskultur» som årsaken til hvorfor vi har en utilfredsstillende sikkerhetstilstand her til lands. Selv om sikkerhetstilstanden utvilsomt er nært forbundet med sikkerhetskulturen vår, så er *sikkerhetskultur* i seg selv et komplekst og abstrakt konsept som krever klare definisjoner for flere omfattende begreper for å kunne brukes opp mot en styrking av det forebyggende sikkerhetsarbeidet.[152] I denne studien retter vi fokus på konkrete årsaker som ikke krever konseptuell avgrensning og som på sikt kan påvirke vår sikkerhetskultur til det bedre.

3.2.1 Generelle funn fra tilsynsrapporter og medieanalysen

Analysen av tilsynsrapportene avslører at de aller fleste avvikene NSM avdekker i virksomheter kan kategoriseres som *organisatoriske*. Selv der NSM dokumenterer kun ett tilfelle av et avvik, så er avvikets natur ofte slik at de organisatoriske rammene i virksomheten, dersom de hadde vært tilfredsstillende, skulle ha avverget det. De samme avvikene går ofte igjen i mange virksomheter, og relaterte avvik går igjen i en og samme virksomhet. Dette understreker viktigheten av å ha det organisatoriske grunnlaget for det forebyggende sikkerhetsarbeidet på plass.

Menneskelige avvik	Menneskelige/ organisatoriske avvik	Organisatoriske avvik	Teknologiske avvik
17	20	205	13
Totale avvik: 255. (Fordelt på 11 tilsynsrapporter.)			

Figur 3.1 Kategorisering av avvik i tilsynsrapportene[153]

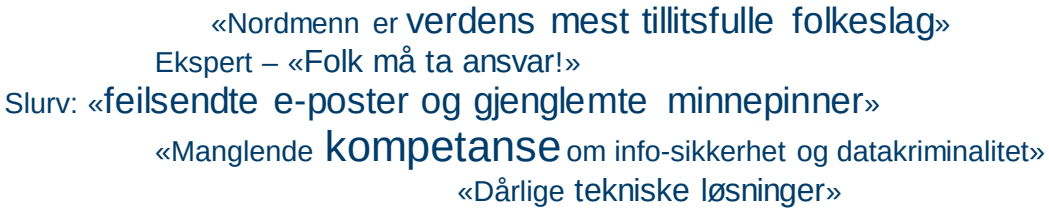
Studien finner kun få eksempler på feil og mangler hva gjelder *teknologiske* avvik. Dette til tross for at den teknologiske utviklingen regnes som en sentral medvirkende årsak til økt sårbarhet i samfunnet. Dette peker til den største sårbarheten ved selve de teknologiske tiltakene, de er avhengige av de menneskelige og organisatoriske tiltakene for å kunne leve opp til sitt potensiale. Det er menneskene som oppfatter, vurderer og lærer når og hvordan man skal bruke de forskjellige teknologiske tiltakene. Mennesker kan bevisst eller ubevisst undergrave verdien av de teknologiske tiltakene. Eksempelvis nytter det lite å investere i et nytt adgangskontrollsystem

[152] Jf. følgende definisjon av kultur som «ideer, verdier, regler og normer som et menneske overtar fra den foregående generasjonen, og som man forsøker å bringe videre – ofte noe forandret – til neste generasjon.» Kleiven, R. et. al. 1995, I samfunnet. Samfunnslære for videregående skole.

[153] Se Figur 4 (s.18) for definisjoner av kategoriene.

dersom ansatte holder døren åpen for hverandre, og en programoppdatering er ikke verdt pengene som ble investert i å utvikle den, dersom den ikke installeres.

Medieanalysen av i overkant av 200 nyhetssaker understøtter funnet om at organisatoriske årsaker er sentrale. Likevel skiller mediedekningen seg markant fra blant annet tilsynsrapportene. Selv om organisatoriske årsaker er de som nevnes hyppigst i forbindelse med sikkerhetstilstanden så er det eksempler på *menneskelige* årsaker som slås opp i nyhetene. I særdeleshet så er det «den naive og lettlurte Ola og Kari Nordmann» som får mye oppmerksomhet.



Figur 3.2 Illustrasjon av den norske mediedebatten om forebyggende sikkerhet

Media bruker ofte evokative og ekspressive formuleringer og kallenavn. For eksempel blir ofte etterretnings-, overvåkings- og sikkerhetstjenestene omtalt som «hysj-tjenestene». En positiv trend er at media ikke bare rapporterer om sikkerhetstruende hendelser men at det også tidvis kommer innslag av typen «slik kan du beskytte PC-en» og lignende. Dette vitner om en økende bevissthet rundt viktigheten av forebyggende sikkerhet i hverdagen, en bevissthet som på sikt kan komme det formelle forebyggende sikkerhetsarbeidet til gode.

3.2.2 Leders ansvar å avsette ressurser

Virksomhetens leder har det overordnede ansvaret for den forebyggende sikkerhetstjenesten i sin virksomhet, samt i underlagte virksomheter.[154] Lederen skal minst én gang i året evaluere den generelle sikkerhetstilstanden i virksomheten,[155] samt påse at det settes av nødvendige ressurser for å ivareta den forebyggende sikkerhetstjenesten.[156] Støtte fra lederen i form av ressurser og oppfølging er avgjørende for at virksomheten skal kunne oppdage og reagere på sårbarheter og sikkerhetstruende hendelser. God sikkerhet i virksomheten starter hos ledelsen.

Feil og mangler:

- Lederen avsetter ikke nødvendige ressurser for å ivareta den forebyggende sikkerhetstjenesten.
- Lederen gjennomfører ikke årlig evaluering av sikkerhetstilstanden i virksomheten.
- Sikkerhetsorganisasjonen er underdimensjonert og ressurssvak i forhold til sikkerhetsbehovet.
- Mangelfull gjennomføring av sikkerhetsfaglige tiltak innen forebyggende sikkerhet.

[154] Forskrift om sikkerhetsadministrasjon § 2-1.
[155] Forskrift om sikkerhetsadministrasjon § 4-4.
[156] Forskrift om sikkerhetsadministrasjon § 2-1.

- Utøvende og kontrollerende oppgaver innen sikkerhet fordeles ikke på forskjellige medarbeidere.

Bakenforliggende årsaker:
Analysen av tilsynsrapportene viser at enkelte ledere *ikke* avsetter nødvendige ressurser til å ivareta den forebyggende sikkerhetstjenesten. En effekt av dette er underdimensjonerte og ressurssvake sikkerhetsorganisasjoner som ikke er i stand til å ivareta virksomhetens forebyggende sikkerhet. Når tilsynsrapportene i tillegg maler et bilde av ledere som sjelden evaluerer sikkerhetstilstanden i virksomheten, er det grunn til å anta at ressursfordelingen ikke i tilstrekkelig grad tar høyde for det aktuelle risikobildet.[157]

Ledere måles sjelden på hvor godt de ivaretar den forebyggende sikkerheten. En administrerende direktør blir gjerne målt på virksomhetens kjerneproduksjon, herunder måloppnåelse hva gjelder økonomi og effektivitet, men ikke på sikkerhetstilstanden. Måleparametere knyttet til forebyggende sikkerhet og kompetansebygging innen sikkerhet på ledelsesnivå er viktige faktorer i arbeidet med å bedre sikkerhetstilstanden.[158] Virksomhetens leder har dessuten et overordnet ansvar for den forebyggende sikkerhetstjenesten i underlagte virksomheter.[159] Likevel observerer NSM at de færreste overordnede virksomheter bevisst etterspør rapportering om sikkerhetsarbeidet i underliggende etater.[160] Sentrale styringsinstrumenter fra departementer til underliggende virksomheter (eksempelvis tildelingsbrev/oppdragsbrev) inneholder gjerne krav til rapportering om sikkerhetstilstanden, men forebyggende sikkerhet er på mange måter et nytt fokusområde som krever tettere oppfølging fra overordnet hold, for å påse at forebyggende sikkerhet settes på dagsorden uten at det stjeler tid fra det som ofte anses som *mer viktige* gjøremål.

«Dette er en veldig utakknemlig jobb fordi det genererer ressursbruk og tungvinte rutiner».

Intervjuobjekt

Økt sikkerhetsinteresse på ledelsesnivå kan dessuten føre til en mer *bevisst* styring av det forebyggende sikkerhetsarbeidet. Sikringstiltakene skal være et resultat av bevisste avgjørelser og gjennomarbeidede risikoanalyser, som påser at de mest kritiske verdiene sikres først. Alle fagområdene må tillegges tilstrekkelig vekt i sikringsøyemed.[161] Risikoanalyser kan med fordel innbefatte potensielle konsekvenser og/eller kostnader ved håndtering av krisehendelser. Kostnadsberegninger tenderer å komme i etterkant av alvorlige hendelser, men dersom beregningene integreres i kombinasjon med drøfting av forebyggende sikringstiltak vil det gi et bedre beslutningsgrunnlag. Det er helt avgjørende å ha en god risikoforståelse for å kunne

[157] Leders årlige evaluering av sikkerhetstilstanden kan eksempelvis ta utgangspunkt i interne sikkerhetsrevisjoner, tilbakemeldinger fra tilsyn, risikovurderinger, resultater fra øvelser, innrapporterte sikkerhetstruende hendelser, osv.
[158] Måleparametere for sikkerhet diskuteres også i del 3.2.4 om dokumentasjon av det forebyggende sikkerhetsarbeidet.
[159] Forskrift om sikkerhetsadministrasjon § 2-1.
[160] Dette påpekes av NSM i Rapport om sikkerhetstilstanden 2011, s.11.
[161] Sikkerhetsloven presenterer fagområdene som skal inngå i den forebyggende sikkerhetstjenesten: informasjonssikkerhet, objektsikkerhet, personellsikkerhet og sikkerhetsgraderte anskaffelser.

gjennomføre målrettede sikringstiltak.[162] Selv i de virksomheter med tilstrekkelig ressurstilgang påpeker intervjuobjekter at det oppstår diskusjoner om ressurser, fordi virksomhetens ansatte har ulike oppfatninger av hvordan ressursene bør brukes. Gjennomføring av risikovurderinger vil gi ledere og medarbeidere en felles forståelse av risikobildet, og derved gi sikringstiltakene en bredere oppslutning internt.[163]

«Det er ikke en bevisst styring av beredskap og forebyggende sikkerhet i vår virksomhet. Den er mer ubevisst».

Intervjuobjekt

Virksomhetens leder skal påse at sikkerhetsoppgaver og -ansvar fordeles mellom medarbeidere i virksomheten slik at enkeltpersoner ikke kan undergrave sikkerheten.[164] I praksis innebærer dette blant annet at utøvende og kontrollerende oppgaver innen sikkerhet skal fordeles på forskjellige medarbeidere.[165] Eksempelvis bør ikke virksomhetens IKT-ansvarlig også fungere som datasikkerhetsleder (DSL). Flere av tilsynsrapportene viser imidlertid at en og samme person ofte blir satt til å kontrollere eget sikkerhetsarbeid. Flere virksomheter sliter med underdimensjonerte sikkerhetsorganisasjoner hvor et fåtall ansatte sitter med mye ansvar. Ansettelser er kostbart, og en del virksomheter velger å benytte midlertidige ansettelser i sin sikkerhetsorganisasjon. Alle virksomheter må selv vurdere størrelsen på sin sikkerhetsorganisasjon etter behov. Samtidig må ledere påse at virksomheten har tilstrekkelig med personellressurser til å fordele ansvaret på et tilstrekkelig antall ansatte.

«Beredskap er så viktig at det bør være flere faste ansettelser».

Intervjuobjekt

Dersom arbeidsbelastningen og ansvarsbyrden blir i overkant stor for enkeltpersoner, kan dette medføre at sikkerhetsansatte slutter i sine stillinger. Det er et utbredt problem at virksomheter opplever gjennomtrekk i sikkerhetsorganisasjonen (diskuteres også i del 3.2.3).

3.2.3 Opplæring og kompetansebygging

Virksomheter som er underlagt Sikkerhetsloven skal påse at ansatte får tilstrekkelig opplæring i sikkerhetsspørsmål, og at den sikkerhetsfaglige kompetansen utvikles og vedlikeholdes.[166] Virksomhetens leder skal motivere og bevisstgjøre behovet for sikkerhetstjeneste i virksomheten, og påse at personell jevnlig får sikkerhetsveiledning.[167] I tillegg skal virksomheten til enhver tid

[162] NSM 2011. Rapport om sikkerhetstilstanden 2011, s.6.
[163] Virksomhetene skal gjennomføre risikovurderinger, blant annet for å avdekke behovet for sikkerhetstiltak utover minimumskravene i Sikkerhetsloven med forskrifter. Flere av tilsynsrapportene viser imidlertid at risikovurderinger ikke alltid gjennomføres. Det registreres at NSM har mandat til å pålegge en virksomhet å utarbeide skriftlig risikovurdering, men kun «når særlige grunner foreligger», jf. Forskrift i sikkerhetsadministrasjon § 4-2.
[164] Forskrift om sikkerhetsadministrasjon § 2-4.
[165] Forskrift om sikkerhetsadministrasjon § 2-4.
[166] Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) § 5, og Forskrift om sikkerhetsadministrasjon § 3-2.
[167] Forskrift om sikkerhetsadministrasjon § 3-1.

ha oversikt over den sikkerhetsfaglige kompetansen i virksomheten.[168] Disse og andre krav om sikkerhetsfaglig opplæring og kompetansebygging finnes i sikkerhetsloven og forskrift om sikkerhetsadministrasjon.

Feil og mangler:

- Mangler oversikt over den sikkerhetsfaglige kompetansen i virksomheten.
- Mangelfull veiledning av personell som har ansvar for autorisasjon av ansatte.
- Mangler rutiner som sikrer at den sikkerhetsfaglige kompetansen utvikles og vedlikeholdes.
- Mangelfull kompetanse blant de ansatte i sikkerhetsorganisasjonen.
- Mangler krav til kompetanse i stillingsinstrukser for ansatte innen sikkerhetsorganisasjonen.
- Mangelfull autorisering av ansatte som kan få tilgang til skjermingsverdig informasjon.

Bakenforliggende årsaker:

NSM bemerker at kompetansen hos sikkerhetspersonell de senere årene har vært nedadgående.[169] Sikkerhetsmedarbeidere mangler tilstrekkelig relevant kompetanse innen forebyggende sikkerhetstjeneste, spesielt knyttet til risikovurdering og risikohåndtering.[170] Mangelfull kompetanse medfører at ledere og medarbeidere begår ubevisste, alvorlige sikkerhetsbrudd som kan gjøre virksomheten mer sårbar for uønskede hendelser.[171] Ledere og sikkerhetsansatte skal være foregangseksempler som påser at virksomhetens ansatte opptrer i tråd med bestemmelsene i sikkerhetsloven med forskrifter, samt motiverer de ansatte til å være sikkerhetsbevisste. Dette lar seg vanskelig gjennomføre i praksis dersom foregangseksemplene selv mangler tilstrekkelig sikkerhetsforståelse og -kompetanse.

Høy sikkerhetsfaglig kompetanse i sikkerhetsorganisasjonen avhenger av et bredt rekrutteringsgrunnlag der kvalifiserte personer søker seg til virksomheters sikkerhetsorganisasjoner. Konkurransen om de best kvalifiserte er hard, da sikkerhetskompetanse er etterspurt, også i privat sektor. Det kan være utfordrende for sikkerhetsorganisasjoner å konkurrere om å rekruttere og beholde spesialister innen eksempelvis IKT-sikkerhet.[172] Flere av de sikkerhetsansatte vi intervjuet mente de hadde stående jobbtilbud fra andre arbeidsgivere.

NSM har også erfart at sikkerhetspersonell som ikke oppfyller kompetansekravene, men som ønsker kompetansebygging, ikke får tilstrekkelig støtte for dette i virksomheten.[173] Våre intervjuer understøtter en slik tendens. Flere intervjuobjekter uttrykte et ønske om å delta på flere sikkerhetsrelaterte kurs, men formidlet at dette hadde blitt nedprioritert grunnet en voksende arbeidsmengde og tidsfrister. For å hindre at dette skjer, kan det være lurt at virksomhetene

[168] Forskrift om sikkerhetsadministrasjon § 3-2.
[169] NSM 2011. Rapport om sikkerhetstilstanden 2011, s.11.
[170] NSM 2009. Rapport om sikkerhetstilstanden 2009, s.5.
[171] NSM 2011. Rapport om sikkerhetstilstanden 2011, s.11. NSM 2010. Rapport om sikkerhetstilstanden 2010, s.10.
[172] Etterspørselen etter IKT-sikkerhetskompetanse er også diskutert av NSM i Rapport om sikkerhetstilstanden fra 2007, s.7.
[173] NSM 2010. Rapport om sikkerhetstilstanden 2010, s.10.

etablerer kortsiktige og langsiktige planer og rutiner for opplæring og videreutvikling av sikkerhetskompetansen i virksomheten.[174]

«Jeg har vært påmeldt til kurs, men har ikke hatt tid til å prioritere det».

Intervjuobjekt

Enkelte intervjuobjekter etterspurte flere spesialiserte sikkerhetsforum, der konkrete bestemmelser og krav i sikkerhetsloven med tilhørende forskrifter gjennomgås. Det arrangeres stadig flere sikkerhetskonferanser, inkludert NSMs årlige sikkerhetskonferanse og Samfunnssikkerhetskonferansen i Stavanger, men enkelte mente disse har blitt veldig populariserte og derved ikke bidro til kompetanseheving for sikkerhetsansatte som allerede arbeider med forebyggende sikkerhet. Et mer spesialisert kurs er eksempelvis NSMs kurs i objektsikkerhet, hvor målgruppen er nettopp sikkerhetsansatte i de virksomheter som eier eller forvalter skjermingsverdige objekter.

I enkelte virksomheter oppstår det uenighet mellom sikkerhetsansatte som vil jobbe kontinuerlig med å bedre sikkerheten, og sikkerhetsansatte som foretrekker videreføring av eksisterende praksis som de mener er «god nok». I et slikt miljø blir det fort gjennomtrekk i sikkerhetsorganisasjonen. Flere av våre intervjuobjekter hadde nylig tiltrådt sine stillinger.

Høy utskiftningsgrad og gjennomtrekk i sikkerhetsorganisasjonen er en stor utfordring i norske virksomheter. NSM erfarer at virksomheter ofte bruker «nyansettelser» som begrunnelse for hvorfor sikkerhetsansatte mangler tilstrekkelig sikkerhetsfaglig kompetanse.[175] Dette ble bekreftet gjennom våre intervjuer. Flere intervjuobjekter mente de var i en opplæringsprosess, og at sikkerhetsorganisasjonen ennå var litt umoden grunnet flere nyansettelser. Flere mente at sikkerhetstilstanden ville bedres i virksomheten når rollene hadde satt seg. Virksomheter må bli flinkere til å påse at ingen sikkerhetsansatte slutter i sine stillinger før etterfølger har fått nødvendig sikkerhetsopplæring. Enkelte virksomheter har også en del midlertidig ansatte i sin sikkerhetsorganisasjon, og selv om sikkerhetsloven[176] krever at midlertidig ansatte skal få tilstrekkelig sikkerhetsopplæring, vil virksomheter i praksis sjelden investere store summer i kompetanseheving for personell som kan forsvinne i løpet av kort tid. Faste ansettelser i sikkerhetsorganisasjonen skaper forutsigbarhet og kontinuitet i sikkerhetsarbeidet.

«Sikkerhetskompetansen i virksomheten burde vært bedre».

Intervjuobjekt

Mange sikkerhetsansatte har utilstrekkelig kompetanse hva gjelder gjennomføring av *sikkerhetsklareringer*[177] og *autorisasjoner*.[178] Selv om flere virksomheter har mandat til å

[174] I følge Forskrift om sikkerhetsadministrasjon § 3-2 skal virksomheter ha rutiner for dette.
[175] NSM 2011. Rapport om sikkerhetstilstanden, s.11.
[176] Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) § 5.
[177] Sikkerhetslovens § 3 definerer sikkerhetsklarering som «avgjørelse, foretatt av klareringsmyndighet og bygget på personkontroll, om en persons antatte sikkerhetsmessige skikkethet for angitt sikkerhetsgrad.»

sikkerhetsklarere sine ansatte, er det er en utfordring at klareringsmyndigheter ikke alltid besitter tilstrekkelig kompetanse om hvordan sikkerhetsklareringer skal foretas.[179] Dette kan medføre at personer med uønskede hensikter innvilges sikkerhetsklarering og får tilgang til skjermingsverdig informasjon, eller adgang til områder hvor slik informasjon håndteres. NSM avdekker også stadig ikke-autorisert personell som har fått tilgang til sikkerhetsgradert informasjon, og at virksomheter mangler oppdaterte autorisasjonslister.[180] Enkelte intervjuobjekter fremhevet at arbeidsoppgavene tilsa at personer ikke hadde behov for autorisasjon, noe som ofte kan være tilfellet. Den mer vanlige begrunnelsen var at virksomheter ikke hadde rukket å autorisere personell grunnet nye tilsatte, oppbemanning eller ferieavvikling. En annen årsak ser ut til å være at enkelte autorisasjonsansvarlige mangler forståelse for viktigheten av autorisasjon. Autorisasjon av et stort antall medarbeidere er tidkrevende, både for autorisasjonsansvarlige og medarbeiderne, og for å lykkes med gjennomføringen må ledere på forhånd få tilstrekkelig opplæring. Delegering av autorisasjonsansvaret kan bidra positivt ved å øke sikkerhetsbevisstheten nedover i organisasjonen, men det forutsetter at de autorisasjonsansvarlige forstår viktigheten av det. Kompetanseheving er avgjørende for at virksomheter skal overholde kravene om sikkerhetsklarering og autorisasjon.[181]

3.2.4 Dokumentasjon av det forebyggende sikkerhetsarbeidet

Virksomheter som er underlagt sikkerhetsloven plikter å oppfylle en rekke krav om dokumentasjon av det forebyggende sikkerhetsarbeidet. Det mest sentrale dokumentet innen en virksomhets forebyggende sikkerhetsarbeid er *grunnlagsdokumentet for sikkerhet.* Grunnlagsdokumentet skal identifisere de grunnleggende forutsetningene for virksomhetens håndtering av skjermingsverdig informasjon. Dokumentet skal være ajourført og det skal blant annet inneholde en beskrivelse av virksomhetens sikkerhetsorganisasjon og dens myndighet samt referanser til annen sikkerhetsdokumentasjon (planer, instrukser etc.).[182] Virksomhetene plikter også å ha oversikt over den sikkerhetsfaglige kompetansen til de ansatte, spesielt personell i sikkerhetsorganisasjonen.[183] Disse og andre krav til dokumentasjon av det forebyggende sikkerhetsarbeidet foreligger i Forskrift om sikkerhetsadministrasjon.

Feil og mangler:

- Manglende register over sikkerhetstruende hendelser.
- Manglende, mangelfulle eller utdaterte planverk og instrukser.
- Manglende stillingsinstrukser innen fagområdene.
- Utdaterte autorisasjons- og klareringslister.

---

[178] Sikkerhetslovens § 3 definerer autorisasjon som «avgjørelse, foretatt av autorisasjonsansvarlig, om at en person etter forutgående sikkerhetsklarering (med unntak for tilgang til informasjon sikkerhetsgradert BEGRENSET), bedømmelse av kunnskap om sikkerhetsbestemmelser, tjenstlig behov samt avlagt skriftlig taushetsløfte, gis tilgang til informasjon med angitt sikkerhetsgrad».

[179] NSM 2012. Rapport om sikkerhetstilstanden 2012, s.15 og s.18.

[180] Kravene til autorisasjon står blant annet beskrevet i sikkerhetslovens § 19, § 23, § 24, og Forskrift om personellsikkerhet § 5-1 og § 5-8. Ytterligere informasjon om autorisasjon er tilgjengelig i "Håndbok i autorisasjon og autorisasjonssamtale" utgitt av Nasjonal sikkerhetsmyndighet (april 2011).

[181] Kravene omtales blant annet i sikkerhetsloven og Forskrift om personellsikkerhet.

[182] Forskrift om sikkerhetsadministrasjon § 3-3.

[183] Ibid. § 3-2.

- Manglende dokumentasjon av leders årlige evaluering av den generelle sikkerhetstilstanden i virksomheten.
- Manglende dokumentasjon om tiltak som skal iverksettes dersom en hendelse inntreffer (f. eks. nødmakulering).
- Manglende dokumentasjon om kontroll av sikkerhetsgraderte dokumenter.
- Manglende oversikt over sikkerhetsfaglig kompetanse.
- Resultatet av interne sikkerhetsrevisjoner var ikke dokumentert.

Det er noe variasjon med hensyn til virksomhetenes størrelse og sektor når det gjelder manglende eller mangelfull dokumentasjon av sikkerhetsarbeidet i virksomhetene. NSM rapporterer at store virksomheter «synes å gjøre en bedre jobb enn små, men disse er også gjerne eksponert for større risiko» og at private virksomheter «synes å ha en bedre intern kultur for å følge opp sikkerhetsproblemer enn offentlige virksomheter».[184] Manglende dokumentasjon av det forebyggende sikkerhetsarbeidet er til tross for disse variasjonene et utbredt problem. De bakenforliggende årsakene for hvorfor mange virksomheter mangler eller har mangelfull sikkerhetsdokumentasjon er mange og i noen grad sammenfallende årsaker som diskuteres andre steder i dette kapittelet (se for eksempel del 3.2.2 om leders ansvar og ressurser, del 3.2.3 om opplæring og kompetansebygging, og del 3.2.8 om mangler i regelverket).

Bakenforliggende årsaker:
Ufullstendig eller manglende dokumentasjon av det foregående sikkerhetsarbeidet er et problem NSM har meldt om i en årrekke. En viktig årsak som NSM påpeker og som også gjentas blant de ansatte i virksomhetene selv er mangel på måleparametere knyttet til forebyggende sikkerhet.[185] Det har tidligere blitt påpekt at ledere sjelden måles på hvor godt de ivaretar den forebyggende sikkerheten (se del 3.2.2), men dette gjelder også for ansatte i sikkerhetsorganisasjonen og virksomheten for øvrig. I mange tilfeller er sikkerhetstiltak et «forstyrrende» moment som stjeler tid fra arbeidsoppgaver som man blir målt på og som man av den grunn kan ha bedre motivasjon til å bruke arbeidstiden på.

«Dokumentasjon er ekstremt viktig når det er stor turnover».

Intervjuobjekt

Manglende dokumentasjon av det forebyggende sikkerhetsarbeid kan være et symptom på manglende forståelse for hvor viktig dette er. Våre analyser peker imidlertid heller i retning av at mange medarbeidere skjønner hvor viktig det er å dokumentere også det forebyggende sikkerhetsarbeidet, men at blant annet tidspress fører til at dette arbeidet blir mangelfullt. I mange tilfeller søkes dette løst ved å bruke konsulenttjenester for å utvikle virksomhetens sikkerhetsdokumentasjon. Selv om dette kan synes en god løsning er dette heller ikke uproblematisk. For det første, en virksomhets sikkerhetsdokumentasjon skal lokaltilpasses noe som krever inngående kjennskap til virksomheten og dens skjermingsverdige informasjon og objekter. Det er noe uklart hvor godt dette hensynet kan ivaretas av eksterne konsulenter.

[184] NSM, 2010, Rapport om sikkerhetstilstanden 2010, s. 9.
[185] NSM, 2012, Rapport om sikkerhetstilstanden 2012, s. 10.

«Det handler om kompetanse og kapasitet. Man må ha interesse for å utvikle instrukser og tid til å gjøre det».

Intervjuobjekt

Et annet og særlig viktig moment er *reelt eierskap* til innholdet i dokumentasjonen. Selv om virksomhetens sikkerhetsdokumentasjon formelt eies av virksomheten skjer det ofte at virksomhetens medarbeidere ikke føler seg fortrolige med dokumentasjonen, hverken med tanke på hvor godt den passer virksomhetens behov eller med tanke på hvordan den enkelte medarbeider kan sørge for å etterleve de planer og instrukser som er blitt utviklet. Manglende fortrolighet med sikkerhetsdokumentasjonen gjør seg også mer gjeldende når der er stor gjennomtrekk i sikkerhetsorganisasjonen, noe våre delanalyser tilsier at ofte er tilfelle.

«Nye ansatte har tilkommet og de har ikke samme eierskap til sikkerhetsdokumentene».

Intervjuobjekt

Manglende følelse av reelt eierskap til virksomhetens sikkerhetsdokumentasjon fører også til «følgefeil» ved at dokumentasjonen ikke blir oppdatert fordi de lokale medarbeiderne ikke føler seg fortrolige med dokumentene. I slike tilfeller er det lett å falle tilbake til gamle vaner, mens sikkerhetsdokumentasjonen blir en slags «spøkelsesdokumentasjon» som ikke reflekterer de faktiske tiltakene og rutinene som gjennomføres, og som da heller ikke bidrar til at disse forbedres. Virksomhetene kan med fordel også tilrettelegge bedre for enklere håndtering og formidling av sikkerhetsgradert informasjon slik at de ansatte kan etterleve planverket uten for tungvinte rutiner.

«Sikkerhetsdokumentene er nok bedre enn forståelsen av dokumentene».

Intervjuobjekt

I sin årsmelding av 2008 skrev NSM at de «avdekker stadig at systemsikkerhetstiltakene som er påkrevd for å følge sikkerhetsloven ikke er på plass. Dette skjer til tross for at virksomhetene selv beskriver slike tiltak i sin sikkerhetsdokumentasjon.»[186] I sin rapport om sikkerhetstilstanden av 2011 listet NSM en rekke områder som de mener blir skadelidende som følge av feil og mangler i dokumentasjonen av det forbyggende sikkerhetsarbeidet inkludert: kontroll av det forebyggende sikkerhetsarbeidet, oversikt over utviklingen over tid, samt oppfølging og forbedring av det forebyggende sikkerhetsarbeidet som isteden blir tilfeldig og ad hoc.[187] Den samme rapporten oppgir også at «dokumentasjon bærer gjerne preg av å ha blitt opprettet rett før tilsyn og ofte gjentas kun krav i lov og forskrift. Kravene er gjerne ikke operasjonalisert og heller ikke gitt en løsning forankret i lokale forhold. Dette tyder på at dokumentasjonen ikke er knyttet til det daglige virket.»[188] At virksomheter ikke i tilstrekkelig grad har etablert planverk og instrukser innen forebyggende sikkerhet vanskeliggjør også gjennomføringen av internrevisjoner, siden revisjonen gjerne består i å kontrollere sikkerhetsarbeidet opp mot planverket.[189]

[186] NSM, 2008, Årsmelding 2008, s. 8.
[187] NSM, 2011, Rapport om sikkerhetstilstanden 2011, s. 12.
[188] Ibid.
[189] NSM 2010. Rapport om sikkerhetstilstanden 2010, s.9.

«Man prioriterer utøvelse fremfor kontroll, grunnet kapasitetsutfordringer».

Intervjuobjekt

Mangel på måleparametere innen forebyggende sikkerhet for både ledere og medarbeidere, og mangel på reelt eierskap til sikkerhetsdokumentene, er to underliggende årsaker som trolig kan, hvis de utbedres, styrke det forebyggende sikkerhetsarbeidet i virksomhetene på en effektiv og hensiktsmessig måte. Med måleparametere på forebyggende sikkerhet vil dette arbeidet ikke lenger være, som det dessverre ofte anses for å være, et «forstyrrelsesmoment» som stjeler tid fra den man «egentlig» burde drive med. Hvis dette kombineres med lokalt tilpasset sikkerhetsdokumentasjon som medarbeidere og ledere føler reelt eierskap til så er grunnlaget lagt for å styrke dokumentasjonen av det forebyggende sikkerhetsarbeidet med de følgeresultater dette også måtte ha for forbedring av det forebyggende sikkerhetsarbeidet også mer generelt.

3.2.5 Håndtering av sikkerhetstruende hendelser

Når en sikkerhetstruende hendelse oppstår skal ansatte omgående rapportere om hendelsen til sin nærmeste overordnede, virksomhetens leder eller den lederen bemyndiger.[190] Virksomhetens leder skal alltid informeres, og NSM skal også underrettes om slike hendelser.[191] Dessuten må alle virksomheter underlagt sikkerhetsloven føre et register over sikkerhetstruende hendelser.[192] Personell som har tilgang til kryptomateriell skal rapportere om sikkerhetstruende hendelser til kryptosikkerhetsleder, som skal rapportere videre til virksomhetens leder.[193]
Sikkerhetsorganisasjonen skal være oversiktlig, og det skal fremkomme i virksomhetens grunnlagsdokument for sikkerhet hvilke stillinger som inngår i sikkerhetsorganisasjonen, deres oppgaver og ansvarsområde.[194]

Feil og mangler:

- Mangler register over sikkerhetstruende hendelser.
- Uklare rapporteringslinjer internt ved sikkerhetstruende hendelser.
- Mangelfull rapportering til NSM ved sikkerhetstruende hendelser.
- Uoversiktlig sikkerhetsorganisasjon.
- Manglende ivaretakelse av sikkerheten når personell fratrer.

[190] Forskrift om sikkerhetsadministrasjon § 2-3.
[191] Ibid. § 5-4 og § 5-6.
[192] Ibid. § 5-4.
[193] Forskrift om informasjonssikkerhet § 7-42.
[194] Forskrift om sikkerhetsadministrasjon § 3-3.

Bakenforliggende årsaker:

NSMs tilsyn viser en underrapportering av sikkerhetstruende hendelser, både innad i virksomheter og til NSM.[195] *Sikkerhetstruende hendelser* er å regne som:[196]

- *sikkerhetstruende virksomhet*, det vil si, «forberedelse til, forsøk på og gjennomføring av spionasje, sabotasje eller terrorhandlinger, samt medvirkning til slik virksomhet».[197]
- kompromittering av skjermingsverdig informasjon [og/eller objekt[198]]
- *grove sikkerhetsbrudd*, det vil si, brudd på lov eller forskrift «som har medvirket, eller det er uvisst om har medvirket til sikkerhetstruende virksomhet eller kompromittering», eksempelvis «en ulåst kontor-, hvelv- eller safedør til/i sperret område».[199]

I 2012 ble det innrapportert 109 sikkerhetstruende hendelser til NSM, mens tallet var 77 sikkerhetstruende hendelser i 2011, og 35 sikkerhetstruende hendelser i 2010.[200] Her fryktes store mørketall. En årsak til mangelfull innrapportering av slike hendelser er i følge NSM at enkeltstående hendelser ikke fremstår viktige nok for virksomheten.[201] Delanalysene viser dessuten at mange sikkerhetsansatte ikke forstår forskjellen på sikkerhetsbrudd og sikkerhetstruende hendelser, og er usikre på hvilke typer hendelser som skal registreres og rapporteres til NSM. Dette medfører at virksomhetene unnlater innrapportering, med begrunnelse om at de *ikke* har vært utsatt for sikkerhetstruende hendelser. NSMs «Rundskriv 1/11» om rapportering av sikkerhetstruende hendelser til NSM kan med fordel gjøres bedre kjent.

«Instruks og praksis avviker noe når det gjelder rapporteringsrutiner».

Intervjuobjekt

En annen viktig årsak er uklare rapporteringslinjer. Flere ansatte mangler oversikt over hvem de skal rapportere til ved sikkerhetstruende hendelser, som kan medføre at alvorlige hendelser ikke registreres eller følges opp av rette vedkommende. NSM observerer stadig ledere som sjelden varsles om sikkerhetstruende hendelser.[202] Flere virksomheter unnlater også å føre register over sikkerhetstruende hendelser, og mangler retningslinjer for hvordan alvorlige hendelser skal følges opp. I realiteten forsømmes en rekke sikkerhetsaktiviteter som følge av en uklar rollefordeling, der sikkerhetsansatte går ut fra at kollegaer har kontroll, der de selv mangler oversikt. Dette kan bidra til en illusjon om at sikkerhetstilstanden i virksomheten er bedre enn den i realiteten er.

«Vi har en uklar ansvarsfordeling i sikkerhetsorganisasjonen».

---

[195] NSM 2009. Rapport om sikkerhetstilstanden 2009, i/d.
[196] Forskrift om sikkerhetsadministrasjon, § 1-2.
[197] Sikkerhetsloven, § 3.2.
[198] Trolig skal også skjermingsverdige objekter regnes med her, men dette fagområdet synes å ha falt utenfor i mange dokumenter utformet før FOR-2010-10-221362 Forskrift om objektsikkerhet trådte i kraft i 2011.
[199] NSM, 2011, Rundskriv 1/11.
[200] NSM 2012. Rapport om sikkerhetstilstanden 2012, s.11.
[201] NSM 2012. Rapport om sikkerhetstilstanden 2012, s.11.
[202] Se for eksempel NSMs rapport om sikkerhetstilstanden 2011, s.11, og NSMs rapport om sikkerhetstilstanden 2010, s.8.

Mange sikkerhetsansatte, spesielt i store virksomheter, har ulike oppfatninger av hvem som inngår i virksomhetens sikkerhetsorganisasjon. De fleste virksomheter har utpekt stedfortredende Sikkerhetsleder (SL), og mange virksomheter har også utpekt stedfortredende Datasikkerhetsleder (DSL).[203] De færreste har imidlertid klargjort på forhånd når stedfortredende skal gå inn i rollen som henholdsvis SL og DSL ved deres fravær. NSM bemerker også at enkelte virksomheter i perioder har vært helt uten SL eller DSL. En sikkerhetsorganisasjon med uklar rollefordeling og periodevis fravær av sikkerhetsledelse er neppe i stand til å følge opp alle sikkerhetstruende hendelser med relevante tiltak.

Generelt sett kan sikkerhetsorganisasjoner med fordel bli mer synlige i virksomhetene, slik at ansatte har lav terskel for å ta kontakt med fagekspertene. Sikkerhetsorganisasjonene bør også ha en sentral plass i virksomheters organisasjonskart og -struktur.

3.2.6 Øvelser innen forebyggende sikkerhet

Alle virksomheter underlagt sikkerhetsloven er forpliktet til å ha oppdaterte lister over sikkerhetstiltak som kan iverksettes dersom risikoen øker ved for eksempel beredskap, krise eller krig.[204] Virksomheter skal ha en beredskapsplan som inneholder informasjon om beredskapsorganisasjonen og sikkerhetstiltakene, og denne planen skal øves jevnlig og minst én gang i året. Virksomheter skal også ha en plan for gjennomføring av evakuering og tilintetgjøring av dokumenter ved nødsituasjoner.[205] Det er viktig at virksomhetene har vurdert og dokumentert sikkerhetstiltakene i forkant, slik at virksomhetene har oversikt over hvem som er ansvarlig og hvordan disse bør opptre dersom en hendelse inntreffer.

Feil og mangler:

- Mangler oppdaterte lister over sikkerhetstiltak som kan iverksettes dersom risikoen øker ved for eksempel beredskap, krise eller krig.
- Beredskapsplanen øves ikke årlig.
- Mangelfull plan for gjennomføring av evakuering og tilintetgjøring av dokumentering ved nødsituasjoner.

Bakenforliggende årsaker:

Gjennomføring av øvelser innen forebyggende sikkerhet er viktig for å påse at eksisterende beredskapsplaner faktisk vil fungere i en reell krisesituasjon. Øvelser kan bidra til å avdekke utfordringer knyttet til personell og kompetanse, og sikre informasjonsflyt innad i virksomheten og ut til eksterne aktører.[206] NSM registrerer at norske virksomheter ikke i tilstrekkelig grad

[203] Virksomhetens leder skal utpeke en Sikkerhetsleder med stedfortreder, samt annet personell som bør inngå som en del av virksomhetens sikkerhetsorganisasjon, herunder en Datasikkerhetsleder med stedfortreder dersom virksomheten har informasjonssystemer som behandler sikkerhetsgradert informasjon. Se Forskrift om sikkerhetsadministrasjon § 2-5, og Forskrift om informasjonssikkerhet § 5-14. Se for øvrig Forskrift om informasjonssikkerhet § 7-6 og 7-8 angående kryptosikkerhetsorganisasjon.
[204] Forskrift om sikkerhetsadministrasjon § 3-4.
[205] Forskrift om informasjonssikkerhet §4-35.
[206] NSM 2007. Rapport om sikkerhetstilstanden 2007, s.19.

avholder øvelser innen forebyggende sikkerhet.[207] Et stort flertall av virksomhetene i vårt utvalg hadde ikke øvet de sikkerhetstiltak som skal kunne iverksettes dersom risikoen øker ved for eksempel beredskap, krise eller krig. Eksempelvis gjaldt dette manglende øvelser innen evakuering og tilintetgjøring av sikkerhetsgraderte dokumenter og kryptomateriell ved nødsituasjoner. Mer alvorlig er det at virksomheter, i følge NSM, muligens *bevisst* ikke etterlever disse kravene i sikkerhetsloven og forskriftene som omhandler gjennomføring av øvelser.[208]

Norske virksomheter kan ha vanskeligheter med å forholde seg til scenarioer i øvre del av krisespekteret. I en hektisk hverdag må det vurderes hvilke forebyggende sikkerhetstiltak som skal prioriteres, hvorav øvelser innen evakuering og tilintetgjøring av sikkerhetsgraderte dokumenter tilsynelatende anses som mindre akutt. I følge Gjørv-kommisjonen var det redusert oppmerksomhet omkring behovet for beskyttelse av skjermingsverdig informasjon i forbindelse med terrorangrepene 22. juli 2011, til tross for økt etterretningsrisiko mot Norge.[209] Av naturlige årsaker var liv og helse første prioritet, men da situasjonsbildet ble mer oversiktlig var det nødvendig å beskytte sikkerhetsgraderte dokumenter.

«Angrepene 22/7 var ikke rettet direkte mot skjermingsverdig informasjon, og kommisjonen har derfor ikke hatt særskilt søkelys på dette, annet enn der det er en naturlig den av angrepene 22/7»

22. juli kommisjonen[210]

I kjølvannet av terrorangrepet var NSMs ledelse i kontakt med Statsministerens kontor (SMK) og Justisdepartementet (JD)[211] med tilbud om støtte for å sikre skjermingsverdig informasjon og utstyr. Gjørv-kommisjonen bemerker at NSMs ekspertise i liten grad ble benyttet.[212] Likeledes, da enkelte departementer flyttet inn i midlertidige lokaler etter terrorangrepet, ga NSM råd om sikring av de evakuerte lokalene. Likevel avdekket NSMs egne befaringer flere eksempler på usikret oppbevaring av skjermingsverdig utstyr. Dette til tross for at terrorangrepet medførte økt risiko for spionasje og kompromittering av sensitiv informasjon.[213]

NSM bemerker at arkivpersonale ofte har gode forutsetninger for å ivareta dokumentsikkerheten, og til å spre sikkerhetskompetanse innad i virksomheten.[214] En viktig utfordring er at arkivmedarbeidere ikke alltid er en integrert del av sikkerhetsorganisasjonen i virksomhetene. Arkivpersonell er en viktig ressurs som med fordel kan inkluderes mer i sikkerhetsarbeidet i de fleste virksomheter. Når det er avstand mellom arkivansatte og sikkerhetsseksjonen for øvrig blir det vanskelig å fange opp arkivets behov, eksempelvis hva gjelder øvelser innen forebyggende sikkerhet. NSM har tidligere diskutert nytteverdien av å sentralisere sikkerhetskompetansen på ett sted i virksomheten.[215] En viktig fordel ved dette er et sterkere sikkerhetsfaglig miljø, der

[207] NSM 2012. Rapport om sikkerhetstilstanden 2012, s.10.
[208] NSM 2011. Rapport om sikkerhetstilstanden 2011, s.11.
[209] Rapport fra 22. juli kommisjonen, NOU 2012: 14, s.228
[210] Rapport fra 22. juli kommisjonen, NOU 2012: 14, s.71, i fotnote.
[211] Nåværende Justis- og beredskapsdepartementet.
[212] Rapport fra 22. juli kommisjonen, NOU 2012: 14, s.228.
[213] Ibid.
[214] NSM 2010. Rapport om sikkerhetstilstanden 2010, s.10.
[215] NSM 2004. Risikovurdering 2004, s.8.

sikkerhetsansatte samarbeider tett og drar nytte av hverandres kompetanse. Ulempen er at sikkerhetskompetansen blir sittende ett sted i virksomheten, som kan innebære desto lavere sikkerhetskompetanse andre steder i virksomheten.[216]

«Vi blir ikke så involvert og prioritert i virksomhetens sikkerhetsarbeid som vi skulle ønske».

Intervjuobjekt

Virksomheter bør i større grad gjennomføre øvelser innen forebyggende sikkerhet for å sikre god beredskap ved en alvorlig hendelse.[217] Forståelsen omkring viktigheten av beskyttelse av skjermingsverdig informasjon i krisesituasjoner er tilsynelatende utilstrekkelig. Mange virksomheter forstår ikke hvilke verdier de besitter i form av skjermingsverdig informasjon og skjermingsverdige objekter, og at trusselaktører potensielt kan være interessert i disse verdiene.

3.2.7 Oppfølging fra NSM etter tilsyn

NSM har en viktig rolle som nasjonal rådgiver og veileder innen forebyggende sikkerhetstjeneste. NSM skal imidlertid også fungere som tilsynsmyndighet, og eventuelt gi pålegg om forbedringer. Begge disse områdene må tillegges tilstrekkelig vekt. Flere intervjuobjekter etterspør mer oppfølging og veiledning fra NSM etter endt tilsyn.

3.2.7.1 Håndhevelsesmekanismer ved mangelfull etterlevelse

NSMs tilsynsarbeid innebærer å sjekke om norske virksomheter opptrer i tråd med forpliktelsene i sikkerhetsloven og dens forskrifter. Etter endt tilsyn kan NSM bidra med råd og veiledning til virksomheter, eventuelt gi pålegg om forbedringer.[218] Selv om NSM rapporterer om alvorlige sikkerhetsbrudd i norske virksomheter hvert år, er det lite som tyder på at sikkerhetsbruddene får konsekvenser utover påleggene. Dette kan medføre at virksomheter ikke føler seg like bundet av forpliktelsene.

Feil og mangler:

- Mangelfull etterlevelse av sikkerhetsloven og dens forskrifter.
- Mangelfull korrigering av avvik og oppfølging av observasjoner.
- Manglende konsekvenser når det begås sikkerhetsbrudd.

Bakenforliggende årsaker:

NSM er oppmerksomme på at sikkerhetsbrudd bør få konsekvenser. I rapport om sikkerhetstilstanden[219] påpekes det at sikkerhetskulturen i virksomheter «svekkes der sikkerhetsbrudd begås uten at dette får konsekvenser». Likevel, lite tyder på at virksomheter forfølger sikkerhetsbrudd og påser at det får konsekvenser for de ansatte. På tilsvarende vis er det få overordnede virksomheter som bevisst etterspør rapportering om sikkerhetsarbeid i

[216] Ibid.
[217] NSM 2007. Risikovurdering 2007, s.10.
[218] Sikkerhetsloven § 9.
[219] NSM 2010. Rapport om sikkerhetstilstanden 2010, s.11.

underliggende etater (se også del 3.2.2).[220] Manglende eller sovende straffemekanismer har ført til en uformell «aksept» av mangelfull etterlevelse av krav til forebyggende sikkerhet blant virksomheter som behandler lovpålagte krav som om de skulle vært oppfordringer.

I sikkerhetslovens § 31 om straffemekanismer sies det at «den som forsettlig eller uaktsomt overtrer bestemmelser… straffes med bøter eller fengsel».[221] NSM er gitt myndighet gjennom sikkerhetsloven til å politianmelde den som overtrer bestemmelsene. Dette kan føre til bøtelegging eller straff med fengsel i inntil seks måneder eller ett år, avhengig av lovbruddet. Det trekkes frem at enkelte lovbrudd også kan falle inn under strengere straffebestemmelser.

I Stortingsmelding nr.17[222] om statlige tilsyn listes det opp følgende reaksjonsmuligheter som NSM har til rådighet:

- Påpeking av plikter overfor tilsynsobjekt
- Avtaler mellom tilsynsetat og tilsynsobjekt om korrigerende tiltak som skal gjennomføres, eksempelvis innen gitt frist.
- Enkeltvedtak om korrigerende tiltak (pålegg)
- Enkeltvedtak om tvangsmulkt/gebyr
- Enkeltvedtak om forelegg/tvangsgjennomføring, eksempelvis dersom tilsynsobjekt ikke har fulgt opp tidligere vedtak
- Enkeltvedtak om stansing, tilbakekalling av tillatelse/produkt
- Politianmeldelse

NSM forholder seg først og fremst til kravene i sikkerhetsloven og dens forskrifter. Likevel, enkelte av reaksjonsmulighetene i Stortingsmelding nr.17 benyttes regelmessig av NSM. Dette gjelder spesielt påpeking av virksomhetens plikter, samt anbefalinger og pålegg om korrigering av avvik innen en gitt frist. NSM etterspør også dokumentert tilbakemelding fra virksomheter når korrigeringen er foretatt. I praksis hender det, dog ytterst sjelden, at NSM kaller inn til en alvorlig samtale mellom NSM og virksomhetens leder for å påse at avvikene rettes opp og sikkerhetstilstanden bedres. NSM kan også true med tilbaketrekking av godkjenning, eller faktisk trekke tilbake godkjenning. En slik sanksjonsmulighet benyttes imidlertid sjelden fordi det kan få alvorlige konsekvenser for det daglige arbeidet i virksomheten. Det finnes imidlertid eksempler på at dette har vært nødvendig. Våre samtaler med mange ansatte i NSM gir lite informasjon om

[220] Dette påpekes av NSM i Rapport om sikkerhetstilstanden 2011, s.11. Forskrift om sikkerhetsadministrasjon § 2-1 sier at: "Virksomhetens leder har overordnet ansvar for den forebyggende sikkerhetstjeneste innen sitt ansvars- og myndighetsområde, herunder underlagte virksomheter".

[221] Helt konkret gjelder det følgende bestemmelser i følge sikkerhetslovens § 31: "Den som forsettlig eller uaktsomt overtrer bestemmelser gitt i eller i medhold av §§ 5, 10, 12 annet ledd, 13 første og fjerde ledd, 14 første, tredje og fjerde ledd og 17 i loven her, eller overtrer pålegg gitt av Nasjonal sikkerhetsmyndighet i medhold av § 9 første ledd bokstav c i loven her, straffes med bøter eller fengsel inntil seks måneder, hvis ikke forholdet går inn under en strengere straffebestemmelse. Medvirkning straffes tilsvarende. Den som forsettlig eller grovt uaktsomt overtrer § 11 annet ledd første punktum i loven her, straffes med bøter eller fengsel inntil seks måneder, hvis ikke forholdet går inn under en strengere straffebestemmelse. Den som forsettlig eller grovt uaktsomt krenker taushetsplikt etter § 12 første ledd, straffes med bøter eller fengsel inntil ett år, hvis ikke forholdet går inn under en strengere straffebestemmelse."

[222] Stortingsmelding nr.17 2002-2003, s.101.

politianmeldelse og påfølgende bøtelegging. Terskelen for dette er forståelig nok svært høy. Kun et fåtall kjenner til hendelser hvor mekanismene ble benyttet.

Enhver kan forestille seg hvilke konsekvenser det kan ha dersom NSM politianmelder kjente virksomheter for brudd på sikkerhetsloven, spesielt hvis virksomhetene besitter informasjon eller objekter av nasjonal verdi og har høy tillit i offentligheten.

Hvert år avdekker NSM svært alvorlige avvik hos norske virksomheter. Dette kommer tydelig frem i tilsynsrapportene vi har fått tilgang til, observasjonene vi har gjort under tilsyn, og NSMs årlige rapportering om sikkerhetstilstanden. NSM har selv registrert at enkelte virksomheter tilsynelatende *bevisst* velger å ikke etterleve sikkerhetsloven og dens forskrifter, blant annet knyttet til sikkerhetsgradering av informasjon.[223] Det kan få alvorlige skadefølger dersom virksomheter ikke lukker alvorlige avvik som omhandler beskyttelse av skjermingsverdig informasjon eller objekter med betydning for rikets sikkerhet. I slike tilfeller er det ikke urimelig hvis NSM velger å presse virksomhetene til å korrigere avvikene.

Et troverdig håndhevelsessystem sender et signal til virksomhetene om at mangelfull etterlevelse vil sanksjoneres. Vissheten om at sikkerhetsbrudd ikke får konsekvenser vil trolig påvirke virksomheters handlingsmønstre. Det kan også tenkes at enkelte virksomheter trenger et ekstra press for å sette sikkerhet øverst på agendaen. Dette kan også føre til at overordnede virksomheter legger økt press på sine underliggende etater. NSM bør på nytt vurdere hvilke reaksjonsmuligheter som bør benyttes utover skriftlige pålegg, samt muligens foreta en ny vurdering av lovbrudd som bør forfølges i tråd med § 31 i sikkerhetsloven, og få prøvd saker for domstolene som kunne skapt presedens for senere avgjørelser.[224]

3.2.7.2 Råd og veiledning etter tilsyn

Norske virksomheter har et behov for råd og veiledning om forebyggende sikkerhetstjeneste. Virksomheter forstår ikke alltid hvilke verdier de besitter i form av skjermingsverdig informasjon og skjermingsverdige objekter, og hvor avhengig andre kan være av deres funksjon. Samtidig har virksomheter en tendens til å feiltolke kravene i sikkerhetsloven og dets forskrifter. NSM er den viktigste nasjonale rådgiver innen forebyggende sikkerhetstjeneste i Norge og har en betydningsfull oppgave i å veilede norske virksomheter til å bedre sikkerheten. Virksomheter etterspør mer oppfølging og veiledning fra NSM etter endt tilsyn. Når det er sagt har virksomhetene selv hovedansvaret for å bedre sikkerhetstilstanden i sin virksomhet. Sikkerhetsansatte må aktivt søke informasjon og tilegne seg kunnskap gjennom NSMs veiledere, rundskriv, og andre relevante utgivelser.

Feil og mangler:

- Mangelfull oversikt over NSMs veiledere, rundskriv og andre utgivelser.
- Mangelfull korrigering av avvik i virksomhetene etter tilsyn.
- Mangelfull kartlegging av de underliggende årsakene bak avvikene.

[223] NSM 2010. Rapport om sikkerhetstilstanden 2010, s.9.
[224] Dersom domsavgjørelser blir gradert kan de vanskelig brukes som bevis siden.

Bakenforliggende årsaker:

NSM benytter ulike metoder for å bistå virksomhetene i arbeidet med å forbedre sikkerhetstilstanden. En viktig del av arbeidet består av å utgi tilsynsrapporter etter endt tilsyn, årlig rapport om sikkerhetstilstanden, samt bidrag til felles trusselvurdering med PST og E-tjenesten. NSM har også en rekke andre publikasjoner inkludert brosjyrer, årsmeldinger, sikkerhetsvarsler, temahefter, skjemaer og håndbøker om ulike sikkerhetsrelaterte temaer. Særdeles viktig er også NSMs skriftlige veiledere som utdyper og forklarer kravene og regelverket i den forebyggende sikkerhetstjenesten. NSM bistår også med veiledning under og etter tilsyn ved behov. I tillegg holder NSM foredrag, kurs og annen møtevirksomhet som setter forebyggende sikkerhet på dagsorden. Arbeidet som gjøres av NSM er viktig og nyttig for å bistå virksomheter med å bedre sikkerhetstilstanden. Arbeidet bidrar også til å synliggjøre NSMs rolle som nasjonal sikkerhetsrådgiver og tilsynsmyndighet.

NSMs årlige, ugraderte rapporter om sikkerhetstilstanden kunne med fordel vært mer detaljerte med gode eksempler som konkretiserer utfordringer. NSM besitter verdifull informasjon og detaljer vedrørende sikkerhetstilstanden i norske virksomheter som skildres på en utmerket måte i tilsynsrapportene og de graderte rapportene om sikkerhetstilstanden. Detaljer bidrar til å øke kunnskapen og skape interesse for sikkerhetsspørsmål. De graderte versjonene av NSMs rapport om sikkerhetstilstanden inneholder mange viktige poenger og opplysninger i paragrafer merket (U) som ikke er gjengitt i de ugraderte versjonene. Det hadde vært formålstjenlig å inkludere flere/alle av de ugraderte detaljene i de ugraderte versjonene av rapportene. Ved å formidle erfaringer fra eksempelvis NSMs tilsyn, og mulige konsekvenser av avvik, vil virksomheter enklere forstå viktigheten av å implementere sikkerhetstiltak. NSMs ugraderte rapporter om sikkerhetstilstanden har blitt gradvis mer detaljerte og bedre de siste årene. Den siste i rekken av graderte rapporter om sikkerhetstilstanden er på vei i motsatt retning, der viktige detaljer utelates.

Etter tilsyn skal virksomhetene lukke avvikene som påpekes av NSM i tilsynsrapportene.[225] Dette innebærer å korrigere avviket, men også å påse at tilsvarende avvik ikke gjenoppstår; som i praksis betyr at virksomheten må finne den underliggende årsaken til at avviket oppstod. Altså, avviket er neppe lukket før årsaken er funnet. Intervjuobjekter har uttrykt vanskeligheter med å sette av tilstrekkelig tid til å finne årsakene. Dessuten observerer vi at virksomhetene har en tendens til å lete på feil sted etter årsaken. Eksempelvis hjelper det lite å utvikle et nytt planverk som følge av tilsyn, hvis kommunikasjonen er dårlig og planverket uansett ikke følges av de ansatte i organisasjonen. Årsakene bak et avvik er ofte flere, og virksomhetene må bli flinkere til å ta tak i hovedutfordringene. Mange virksomheter har behov for assistanse fra utenforstående for å bli oppmerksomme på årsakene. NSM kan med fordel påpeke slike utfordringer under sluttmøtene etter tilsyn eller som såkalte «observasjoner» i tilsynsrapportene.[226] Motargumentet er opplagt. NSM har ansvaret for å kontrollere sikkerhetstilstanden og må påse at de ikke rapporterer om forhold som observeres utover dette. Samtidig blir det umulig for NSM å bedre

[225] Avvik angir manglende samsvar med bestemmelsene i eller i medhold av sikkerhetsloven. Avvik skal korrigeres av virksomheten.

[226] Observasjoner angir forhold som ikke er avvik, men som NSM mener virksomheten bør vurdere i arbeidet med å forbedre sikkerhetstilstanden og den forebyggende sikkerheten.

sikkerhetstilstanden dersom det gjøres avgjørende observasjoner som svekker sikkerhetsarbeidet i virksomheten og som ikke følges opp.

NSM kunne med fordel stilt et rådgiverteam til disposisjon for virksomheter etter endt tilsyn. NSMs revisjonslag har begrenset tid til å bedrive veiledning under tilsynet, og etter tilsynet er revisorene som regel opptatt med å planlegge nye tilsyn. Dessuten eksisterer det gjerne et mulighetsrom for implementering av tiltak etter tilsyn fordi NSM har satt sikkerhet på agendaen hos virksomheten – i en periode. En visshet om at NSM returnerer med et rådgiverteam etter tilsyn kan i seg selv ha en positiv effekt på virksomhetens sikkerhetsarbeid. Dette er selvsagt et ressursspørsmål. Som et minimum burde NSM oppgi kontaktinformasjon til relevante fagpersoner i NSM som kan besvare henvendelser og oppfølgingsspørsmål fra virksomhetene etter endt tilsyn. Flere intervjuobjekter har uttrykt et ønske om mer veiledning fra NSM etter tilsyn.

«Det er vanskelig å vite hvem i NSM man kan ringe for å be om råd».

Intervjuobjekt

Flere intervjuobjekter fremhevet at det er overveldende for en virksomhet å få påpekt flere titalls avvik av NSM gjennom tilsynsrapportene. I tillegg kan det fremstå uklart for virksomhetene hvilke avvik som er mest alvorlige og bør korrigeres umiddelbart, og hvilke avvik som er mindre viktige. Dersom NSM hadde rangert avvikene etter alvorlighetsgrad i tilsynsrapportene hadde det forenklet virksomhetens arbeid med å finne årsakene til de mest alvorlige avvikene. Dessuten er ofte mindre avvik direkte følgefeil av større, mer alvorlige avvik.

«Rangering av avvik vil gjøre det lettere for oss å se hvilke ressurser som trengs for å lukke avviket».

Intervjuobjekt

Motargumentet er selvfølgelig at avvik vanskelig lar seg rangere, da det vil innebære å sette fagområdene opp mot hverandre. Samtidig er det tydelig at enkelte avvik er svært alvorlige og bør fremheves, eksempelvis dersom en virksomhet ikke kan gjøre rede for høyt graderte dokumenter. Ved å fokusere på de mest alvorlige avvikene kan NSM bidra med kompetanseheving på dette området, og virksomhetene blir sittende igjen med et tydeligere bilde av hvor de må ta grep. Det kunne i det minste vært nyttig for NSM å utrede hvilken effekt det kan ha dersom de viktigste avvikene fremheves under sluttmøtene og tydelig markeres i tilsynsrapportene.

«Intervjuobjektene kan gjerne få beskjed om de små avvikene, men presenter kun de viktigste avvikene under sluttmøtet».

Intervjuobjekt

NSM har utviklet en rekke veiledninger som ligger tilgjengelig på NSMs nettsider. Det oppfordres til at NSM annonserer eventuelle endringer som gjøres i disse. Eksempelvis registreres

det at NSM har gjort «Veiledning i risiko- og sårbarhetsanalyse» datert 2006 utilgjengelig, mens DSB/NUSB i oktober 2013 arrangerte metodekurs for personer som jobber med skjermingsverdige objekter og informasjonssystemer hvor den overnevnte veilederen inngikk som en sentral del av kurslitteraturen. Det registreres også at en rekke virksomheter ikke kjenner til «Rundskriv 1/11» om rapportering av sikkerhetstruende hendelser til NSM. Det er beklagelig at rundskrivet ikke har nådd de riktige personene selv om dette ble sendt fra NSM. Det anbefales at rundskrivet legges lett tilgjengelig under «Publikasjoner» på NSMs nettsider.

NSM skal balansere rollen som veileder innen forebyggende sikkerhet på den ene siden, og tilsynsrollen på den andre. Flere virksomheter forbinder NSM mest med tilsynsrollen, og det er gjennom denne aktiviteten NSM og virksomhetene har tettest kontakt. Flere intervjuobjekter etterspør mer oppfølging og veiledning fra NSM etter endt tilsyn, og det er viktig at NSM tillegger veilederrollen tilstrekkelig vekt i tiden fremover.

3.2.8 Mangler i sentrale og sektorvise regelverk

I kapittel 2 presenterte vi kort de mest sentrale bestemmelsene i det sektorovergripende lovverket om den forebyggende sikkerhetstjenesten, sikkerhetsloven med forskrifter (2.1.1), og de mest relevante bestemmelsene angående sektorspesifikt forebyggende sikkerhetsarbeid, representert ved olje- og energisektoren (2.1.2). Basert på vår gjennomgang av disse lovtekstene samt våre erfaringer og observasjoner fra de andre delanalysene har vi funnet en rekke uklarheter som sammen med årsaker vi allerede har presentert vanskeliggjør arbeidet med forebyggende sikkerhet.

Å sette riktig sikkerhetsgrad på skjermingsverdig informasjon er en av de oppgavene som blir vanskeligere enn hva som synes nødvendig som følge av uklare formuleringer og manglende definisjoner. Selv om de fire kategoriene som sådan (STRENGT HEMMELIG, HEMMELIG, KONFIDENSIELT og BEGRENSET) er enkle å forholde seg til så er det ikke umiddelbart opplagt hva som menes med «helt avgjørende skadefølger» osv. Det er iøynefallende at slike helt sentrale kriterier i sikkerhetsloven med forskrifter, som jo er avgjørende for hvordan en virksomhet skal forholde seg til de fleste andre bestemmelser i lovverket, ikke er definert. De kunne i det minste vært illustrert ved bruk av hypotetiske eksempler som kan hjelpe virksomhetene til å relatere sin informasjon opp mot «Norges og dets allierte sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser», en øvelse som ikke nødvendigvis inngår i virksomhetenes daglige tenkesett og kompetanse. På lik linje med vanskeligheter forbundet med gradering av informasjon så er det også vanskeligheter forbundet med utvelgelse og klassifisering av skjermingsverdige objekter.

«Det var veldig uklart hvilket nivå man skulle legge seg på». (Utvelgelse av skjermingsverdige objekter.)

Intervjuobjekt.

Per i dag er dette nok i hovedsak forbundet med at objektsikkerhet først fikk sin forskrift i kraft fra 1. januar 2011. Denne forsinkelsen har også fått ringvirkninger for arbeidet med sikkerhetsadministrasjon, som nødvendigvis har vært ufullstendig da et av fagområdene i praksis

har manglet. Objektsikkerhetens «fravær» har også ført til usikkerhet vedrørende ellers klare krav i sikkerhetsloven med forskrifter. For eksempel, Forskrift om sikkerhetsadministrasjon § 3-3 fastsetter at:

> «Virksomhet med skjermingsverdig informasjon skal ha et ajourført grunnlagsdokument for sikkerhet. Grunnlagsdokumentet skal identifisere grunnleggende forutsetninger for virksomhetens håndtering av skjermingsverdig informasjon, herunder
> 1. sikkerhetsorganisasjonen og dens myndighet,
> 2. sikkerhetsmessig inndeling i fysiske områder ved virksomheten, og hvor sikkerhetsgradert informasjon tillates behandlet og oppbevart med angivelse av høyeste sikkerhetsgrad.
> [...]»[227]

Denne paragrafen inngår i forskriftens kapittel om veiledning, kompetanse og instrukser (kapittel 3) og det synes ikke logisk at det ikke her nevnes skjermingsverdige objekter på lik linje med skjermingsverdig informasjon. Det er usikkert om denne og andre bestemmelser gjelder nettopp for skjermingsverdig informasjon alene eller om objektsikkerheten er unnlatt inkludert av gammel vane. Forskriften om sikkerhetsadministrasjon er forøvrig blitt endret etter at forskriften om objektsikkerhet trådte i kraft (senest i juni 2012) og burde derfor være oppdatert på dette punktet.

Energiloven og Beredskapsforskriften, som i det store og hele gjør en god jobb hva gjelder eksemplifisering av de kategoriene de opererer med, refererer derimot til «ekstraordinære forhold» og «ekstraordinære situasjoner» uten å definere hva disse begrepene omfatter. Noe klarere blir det når Beredskapsforskriften refererer til «store ulykker, vesentlig skade, trusselsituasjoner, rasjonering og andre ekstraordinære situasjoner som kan påvirke energiforsyningens drift og sikkerhet».[228] De siste «andre ekstraordinære situasjonene» forblir udefinerte. Det gis heller ingen forklaring på hvilke kriterier som skal legges til grunn ved vurdering av hva som «kan påvirke energiforsyningens drift og sikkerhet». Beredskapsforskriften fastslår også at skader og funksjonstap ved klasse 1 anlegg skal oppdages «innen rimelig tid», uten å oppgi hva som er å regne som «rimelig tid».[229] Både sikkerhetsloven og forskrift om informasjonssikkerhet bruker «åpenbart» som beskrivelse av beslutningsgrunnlag for hhv. gjennomførelse av sikkerhetssamtale[230] og avgradering av dokumenter gradert HEMMELIG.[231] Slike uklare formuleringer uten definisjoner gir stort rom for fortolkning og usikkerhet vedrørende hva som faktisk kreves.

---

[227] Flere punkter listes opp i Forskrift om sikkerhetsadministrasjon, § 3-3.
[228] FOR 2012-12-07-1157, § 2-5.
[229] Beredskapsforskriften, § 5-4.
[230] «Sikkerhetssamtale skal gjennomføres der dette ikke anses som åpenbart unødvendig». Sikkerhetsloven § 21.
[231] «I tillegg kan Riksarkivaren beslutte avgradering av dokument gradert HEMMELIG eller lavere som er avlevert til Arkivverket, når det må anses åpenbart at det ikke lenger er grunnlag for å gradere dokumentet i samsvar med sikkerhetsloven § 11 første ledd». Forskrift om informasjonssikkerhet, § 2-11.

Et annet eksempel på uklarhet som muligens er ennå mer kritisk vedrører ansvar for sikring: «eier eller driver plikter å sikre anlegg, system eller annet som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller oppretting i ekstraordinære situasjoner mot uønskede hendelser og handlinger, herunder adgang for uvedkommende».[232] Det gis ingen ytterligere informasjon om ansvar eller ansvarsdeling dersom anlegget eies og drives av forskjellige virksomheter. Vi har gjennom arbeid med denne studiens delanalyser observert hvordan lignende uklarheter kan føre til ansvarsfraskrivelse fra begge sider. Et klarere lovverk som angir, i det minste, en hovedansvarshaver i de tilfeller hvor eierskap og drift ikke sammenfaller ville være å foretrekke. På dette punktet synes forøvrig Energiloven å ha den bedre formulering av de tre hovedlovene som er behandlet her: «den som helt eller delvis eier eller driver anlegg eller system... plikter...». Selv om det ikke nødvendigvis er helt klart hvordan ansvarsdelingen er mellom de som «delvis» eier eller driver anlegget eller systemet så gir formuleringen heller ingen av de involverte anledning til å mene de ikke har noe ansvar.

Også i forlengelsen av det ovennevnte sitatet gis det forøvrig noen eksempler på hva som er å regne som «ekstraordinært» da Beredskapsforskriften oppfordrer til at det tas særlig hensyn til «uvær og annen naturgitt skade; brann og eksplosjoner; alvorlig teknisk svikt; innbrudd, hærverk, sabotasje og andre kriminelle handlinger».[233] Det sistnevnte inkluderer sabotasje blant sektorens potensielle «ekstraordinære situasjoner». Hverken Energiloven eller Beredskapsforskriften nevner terrorangrep eller etterretning/spionasje som potensielle trusler. I lys av dagens trusselbilde er dette noe som med fordel kunne inkluderes i en eksplisitt og operasjonalisert oversikt over potensielle «ekstraordinære situasjoner».

Som det ble nevnt avslutningsvis i 2.1.2 i forrige kapittelet så er det klart at det finnes betydelig variasjon i sektorregelverket. Selv vårt lille utvalg av olje- og energisektorens regelverk illustrerer dette godt. På den ene siden finner vi regelverket for petroleumsvirksomheten på norsk sokkel som i veldig liten grad adresserer problematikken rundt forebyggende sikkerhet mot spionasje, sabotasje og terror. På den andre siden, finner vi regelverket for kraftforsyningen som i høy grad tar for seg forebyggende sikkerhetstiltak og som også legger klare føringer for beredskapsorganisasjonene som skal implementere og opprettholde disse tiltakene. Energiloven og Beredskapsforskriften synes å være foregangseksempler hva gjelder klare og operasjonaliserte retningslinjer for klassifisering av objekter (anlegg m.m.) gjennom konkrete eksempler (jf. klasse 1-3 som presentert i 2.1.2).

Selv om vi ved å inkludere argumentasjonen som ble fremsatt i proposisjon nr. 46 om forslag til ny § 9-3 i Petroleumsloven (se del 2.1.2 om Sektorlovverk) illustrerte at nettopp denne typen spionasje, sabotasje og terror var medregnet i diskusjonen som ledet opp mot at beredskap mot såkalte «bevisste anslag» ble inkludert i loven, så må vi bemerke at disse momentene ikke ble inkludert i selve lovteksten. Faktisk så er «bevisste anslag» brukt uten noen form for definisjon eller eksempler. Vi kan heller ikke se at sikringstiltakene som rettighetshaverne er pålagt å opprette og opprettholde er definert eller at det finnes noen kriterier for utforming av beredskapsplanene som de plikter å ha til enhver tid.

[232] Beredskapsforskriften, § 5-1.
[233] Ibid.

I den forbindelse kan vi også rette oppmerksomheten mot en debatt som utspilte seg i media etter at det i mars 2013 ble kjent at OED hadde konkludert med at sektoren ikke hadde noen skjermingsverdige objekter i henhold til kriteriene i sikkerhetsloven. Sikkerhetssjef i Secode, Lars Thoresen, uttalte til Teknisk ukeblad at oljeindustrien sitter på verdier i form av store mengder ny teknologi samt økonomiske verdier.[234] Blant potensielle trusselaktører ramser Thoresen opp: konkurrenter fra mindre kontrollerte stater, økoterrorister og ideologiske terrorister.[235] Dette er etter alt å dømme aktører som kunne tenkes å ty til både spionasje og terrorhandlinger for å fremme sine respektive mål.

Selve kompleksiteten og mengden av krav som virksomheter som er underlagt sikkerhetsloven må etterleve gjør at arbeidet med å sette seg inn i, implementere og oppdatere det forebyggende sikkerhetsarbeidet også blir en komplisert oppgave. Dette er ingen ny observasjon, i sin årsmelding for 2008 skrev NSM at:

> «Funn fra våre tilsyn viser at sikkerhetsregelverket ikke etterleves godt nok. Sikkerhetsloven med forskrifter inneholder over tusen individuelle pålegg og krav. Forskrift om informasjonssikkerhet er den mest omfattende regelsamlingen. Den består av 12 kapitler med i alt 92 paragrafer. Flere virksomheter har vansker med å forholde seg til denne regelmengden. Det kan stilles spørsmål ved om regelverket er unødig komplisert, og for lite dynamisk i forhold til den teknologiske utviklingen».[236]

Det dreier seg dessuten om en uanskuelig mengde krav fordelt på en rekke forskrifter samt oppdateringer til disse. Og i tillegg kommer også krav som fremsettes i sektorregelverket for de forskjellige sektorene.

I 2011 ble det opprettet en arbeidsgruppe med representanter fra FD, JD, NSM og Forsvaret som fikk i oppdrag å evaluere sikkerhetsloven. Blant de spørsmål arbeidsgruppen skulle evaluere var: nye utfordringer knyttet til informasjonssikkerhet, organisatoriske endringer etter at NSM ble opprettet som et eget direktorat samt en mulig styrking av NorCERT. Arbeidsgruppen avgav sin rapport i november 2012 og det ble besluttet at sikkerhetsloven skal revideres.[237] FDs pressemelding med tittelen Styrking av det forebyggende sikkerhetsarbeidet oppgir «samfunnets enorme endringer det siste tiår, ikke minst innenfor det teknologiske området og hvordan informasjon i dag blir spredd» som bakgrunnen for at loven nå revideres.[238] Revisjonsarbeidet ledes av FD og med deltagelse fra JD og NSM.[239] Det er ikke sikkert når en ny versjon av sikkerhetsloven eventuelt legges frem men det oppgis at arbeidet gis høy prioritet i inneværende år (2013).[240]

[234] Teknisk Ukeblad, 2013, Terror Mot Oljebransjen, 20 august.
[235] Ibid.
[236] NSM, 2008, Årsmelding 2008, s. 8.
[237] Meld. St. 21, 2012–2013, Terrorberedskap.
[238] FD, Pressemelding nr. 14/2013, Styrking av det forebyggende sikkerhetsarbeidet.
[239] Ibid.
[240] Meld. St. 21, 2012–2013, Terrorberedskap.

NSM har i en årrekke argumentert at en av årsakene for at det forebyggende sikkerhetsarbeidet ikke ivaretas i tilstrekkelig grad er at virksomheter som besitter skjermingsverdig informasjon og objekter faller utenfor lovens virkeområde.[241] I 2012 skriver direktoratet at «Sikkerhetsloven slik den fremstår i dag er ikke dekkende for samfunnets sikkerhetsbehov. Det er en ambisjon å utvikle et sikkerhetsregelverk som tar utgangspunkt i hele samfunnets sikkerhetsbehov, uavhengig av den organisatoriske tilhørigheten og skillet mellom gradert og ugradert informasjon».[242] Denne søken etter å utvikle et regelverk som dekker hele samfunnets behov synes å motstride det prinsippet som ble nedfelt i Objeksikkerhetsforskriften da den kom for bare et par år siden. I § 1-3 i Objektsikkerhetsforskriften heter det at: «Der det finnes relevante og tilstrekkelige bestemmelser innenfor sektorlovgivningen, og det er etablert tilsynsorgan, går disse foran bestemmelsene i denne forskriften». Denne siste av sikkerhetslovens forskrifter er den eneste som eksplisitt adresserer forholdet til sektorlovgivningen. Det er allerede blitt nevnt at de virksomhetene som forholder seg til både sikkerhetsloven og sektorlovgivningen har en stor mengde krav de skal etterleve. Et annet kompliserende moment de må forholde seg til er det fortsatt uavklarte forholdet mellom sikkerhetsloven med forskrifter og sektorlovgivningen. Slik situasjonen er i dag så frafaller de nylig innførte bestemmelsene om objektsikkerhet dersom det finnes «relevante og tilstrekkelige» bestemmelser i sektorlovgivningen, mens bestemmelsene om informasjonssikkerhet osv. ikke kommer med noen tilsvarende kriterier for anvendelse. Dersom det ubalanserte forholdet som er oppstått mellom de «opprinnelige» fagområdene og objektsikkerhet ikke balanseres ut så synes målet om en helhetlig styrking av det forebyggende sikkerhetsarbeidet fjernt. Dersom det forebyggende sikkerhetsarbeidet skal styrkes på en helhetlig måte trengs det et helhetlig lovverk med klare grensesnitt til annet eksisterende lovverk. Dette sammen med en innføring av klare definisjoner og kriterier som beslutningsgrunnlag for riktig etterlevelse av lovverkets bestemmelser er de to mest sentrale forbedringspunktene i lovverket slik det foreligger i dag.

[241] Eksempelvis: NSM, 2007, Risikovurdering 2007, s. 6. og NSM, 2005, Risikovurdering 2005, s. 6.
[242] NSM, 2012, Rapport om Sikkerhetstilstanden 2012, 2. 16.

4 Konklusjoner og anbefalinger

4.1 Oppsummering og overordnede vurderinger

Våre verdier øker i volum og betydning, og trusselbildet blir stadig mer komplisert. Sårbarhetene våre øker i takt med denne endringen, særlig i forhold til IKT. Norske virksomheter begår gjentatte brudd med kravene i sikkerhetsloven og dens forskrifter, og virksomhetene lukker ikke alvorlige avvik som følge av tilsyn fra Nasjonal sikkerhetsmyndighet (NSM). Norske virksomheter må imøtekomme sårbarhetene gjennom forebyggende sikkerhetstiltak, og kontinuerlig styrke evnen til å reagere på sårbarheter og sikkerhetstruende hendelser.

Denne rapporten identifiserer årsakene til at Norge står overfor en mangelfull sikkerhetstilstand. Gjennom fem delanalyser har det blitt samlet inn materiale fra forskjellige kilder. Studien fokuserer på allmenngyldige og konkrete årsaker. Dette er viktig med tanke på forbedringspotensialet på kort sikt og som et supplement til det pågående arbeidet med å fremme bevissthet om og å forbedre «sikkerhetskulturen». «Sikkerhetskultur» er et veldig komplekst og abstrakt konsept som krever klare definisjoner for flere omfattende begreper. Det samme gjelder et annet begrep som har gjort sitt inntog i debatten om det forebyggende arbeidet, nemlig «risikoerkjennelse og -forståelse», det vil si, mangelen på risikoerkjennelse og -forståelse. Denne studien legger seg på et lavere og mer konkret nivå for å supplere disse vide begrepene. Studien retter fokus mot konkrete årsaker som ikke krever konseptuell avgrensning og som på sikt kan påvirke vår risikoerkjennelse og-forståelse og vår sikkerhetskultur til det bedre.

Det skilles mellom eksterne og interne årsaker. *Eksterne årsaker* er faktorer som ligger utenfor vår innflytelse og som ikke enkelt kan utbedres, men som vi like fullt må være bevisst. Dette gjelder eksempelvis endringer i trusselbildet. *Interne årsaker* er faktorer vi har muligheten til å utbedre, eksempelvis ved å styrke det forebyggende sikkerhetsarbeidet i norske virksomheter. At vi i denne studien fokuserer på interne årsaker har sin naturlige forklaring i at det er her vi har mulighet til å forbedre sikkerhetstilstanden.

Analysen avslører at *organisatoriske årsaker* oftest forklarer sikkerhetsbrudd i virksomhetene. Selv om menneskelige og teknologiske årsaker også er relevante, synes det som at slike sikkerhetsbrudd ofte er et resultat av manglende organisatoriske sikringstiltak. Medieanalysen vår understøtter funnet om at organisatoriske årsaker er sentrale, selv om det er eksempler på *menneskelige årsaker* som slås opp i nyhetene. I særdeleshet så er det «den naive og lettlurte nordmannen» som får mye oppmerksomhet.

Analysen har identifisert en rekke svakheter i forholdet mellom den sektorovergripende lovgivningen for forebyggende sikkerhet (sikkerhetsloven) og sektorspesifikt lovverk på samme tema, med fokus på olje- og energisektoren. De virksomhetene som forholder seg til både sikkerhetsloven og sektorlovgivningen har en stor mengde krav de skal etterleve. Et kompliserende moment er et fortsatt uavklart forhold mellom sikkerhetsloven med forskrifter og sektorlovgivningen. Det trengs et helhetlig lovverk med klare grensesnitt til annet eksisterende lovverk. Dessuten eksisterer det uklarheter omkring definisjoner og kriterier som

beslutningsgrunnlag for riktig etterlevelse av lovverkets bestemmelser. Uklarhetene kan medføre ansvarsfraskrivelse fra virksomhetene.

Ledere i norske virksomheter avsetter ikke i tilstrekkelig grad ressurser til ivaretakelse av den forebyggende sikkerhetstjenesten, som resulterer i underdimensjonerte og ressurssvake sikkerhetsorganisasjoner som ikke er i stand til å ivareta virksomhetens forebyggende sikkerhet. Magre ressurser henger sammen med at ledere sjelden har oversikt over sikkerhetstilstanden i virksomheten. Ledere måles sjelden på hvor godt de ivaretar den forebyggende sikkerheten, og i mange tilfeller er sikkerhetstiltak et «forstyrrende» moment som stjeler tid fra arbeidsoppgaver som man blir målt på og som man av den grunn kan ha bedre motivasjon til å bruke arbeidstiden på. Måleparametere knyttet til forebyggende sikkerhet og kompetansebygging innen sikkerhet på ledelsesnivå er viktige faktorer i arbeidet med å bedre sikkerhetstilstanden.

I enkelte virksomheter oppstår det uenighet mellom sikkerhetsansatte som vil jobbe kontinuerlig med å bedre sikkerheten, og sikkerhetsansatte som foretrekker videreføring av eksisterende praksis som de mener er god nok. I et slikt miljø blir det fort gjennomtrekk i sikkerhetsorganisasjonen. Virksomheter bør påse at ingen sikkerhetsansatte slutter i sine stillinger før etterfølger har tilegnet seg tilstrekkelig kompetanse og fått nødvendig sikkerhetsopplæring. Virksomheter bør også tilrettelegge for kompetansebygging og kursing av de sikkerhetsansatte slik at de forblir i sine stillinger.

Gjennomtrekk av ansatte i sikkerhetsorganisasjonen medfører et økt behov for oppdatert sikkerhetsdokumentasjon. Manglende dokumentasjon av det forebyggende sikkerhetsarbeidet er imidlertid et utbredt problem. En del virksomheter har benyttet innleide konsulenter eller tidligere ansatte til å utvikle sikkerhetsdokumentasjonen. I slike tilfeller har ikke medarbeidere et reelt eierskap til dokumentasjonen, som medfører lite oppdatering av dokumentene. Da faller ofte de ansatte tilbake på gamle vaner og praksis som ikke reflekteres i sikkerhetsdokumentasjonen. Manglende planverk vanskeliggjør også gjennomføringen av internrevisjoner.

Enkelte virksomheter har dårlig oversikt over hvem som inngår i sikkerhetsorganisasjonen og hvem som skal informeres ved sikkerhetstruende hendelser. Uklare rapporteringslinjer kan medføre at sikkerhetstruende hendelser ikke registreres eller følges opp av rette vedkommende. Virksomhetene bør påse at ansvarsforholdet er avklart, og at sikkerhetspersonell på alle nivåer i virksomheten samarbeider. Virksomhetene bør også etablere planer og rutiner for opplæring og videreutvikling av sikkerhetskompetansen i virksomheten.

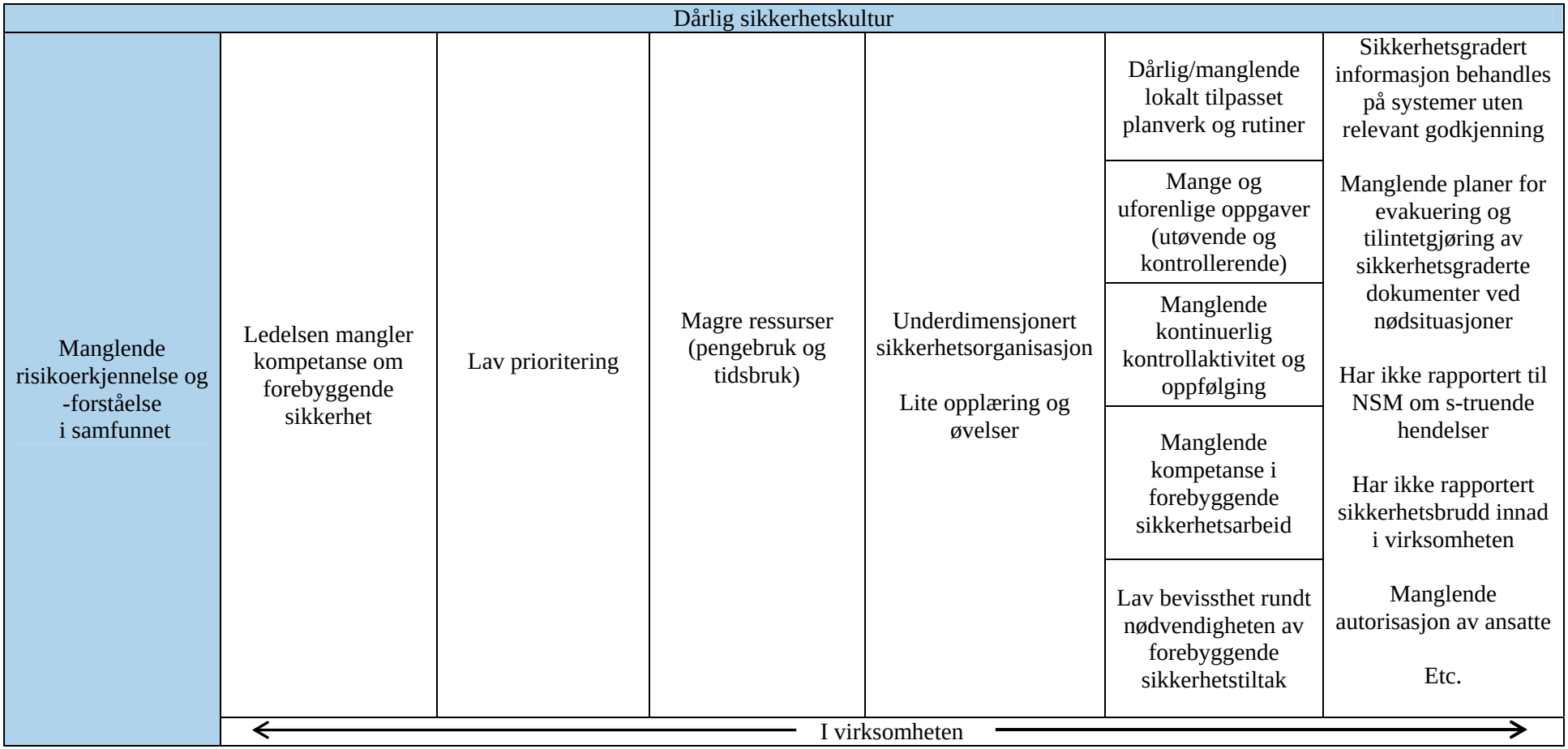
NSM har registrert at enkelte virksomheter tilsynelatende *bevisst* velger å ikke etterleve sikkerhetsloven og dens forskrifter, blant annet hva gjelder sikkerhetsgradering av informasjon. Virksomhetene bør iverksette organisatoriske tiltak som sikrer at ansatte etterlever regelverket, uten for tungvinte rutiner. Det bør tilrettelegges for enklere håndtering og formidling av sikkerhetsgradert informasjon slik at de ansatte velger riktig handlemåte.

Selv om norske virksomheter begår sikkerhetsbrudd er det lite som tyder på at sikkerhetsbruddene får konsekvenser, utover påleggene fra NSM. Manglende eller sovende straffemekanismer kan

medføre at virksomheter ikke føler seg like bundet av forpliktelsene. Virksomheter bør i større grad kartlegge og følge opp sikkerhetsbrudd som begås internt, og overordnede virksomheter bør tilegne seg en bedre oversikt over sikkerhetstilstanden i underliggende etater. I tillegg kan NSM med fordel på nytt vurdere hvilke reaksjonsmuligheter som bør benyttes utover skriftlige pålegg. Et troverdig håndhevelsessystem sender et signal til virksomhetene om at mangelfull etterlevelse vil straffes. NSM skal balansere rollen som veileder innen forebyggende sikkerhet på den ene siden, og tilsynsrollen på den andre. Flere virksomheter forbinder NSM mest med tilsynsrollen, og det er gjennom denne aktiviteten NSM og virksomhetene har tettest kontakt. Flere intervjuobjekter etterspør mer oppfølging og veiledning fra NSM etter endt tilsyn, og det er viktig at direktoratet tillegger veilederrollen tilstrekkelig vekt i tiden fremover.

Som vi har sett, er årsakene sammensatte og komplekse. En og samme svakhet kan ha mange årsaker og disse kan i seg selv være «følgefeil» som skyldes andre og mer underliggende årsaker. Det synes hensiktsmessig å tilnærme seg det overordnede årsaksbildet som et *kontinuum* hvor abstrakte og konkrete årsaker plasseres langs en akse som illustrert i Figur 4.1 (fra det abstrakte på venstresiden og til det konkrete på høyresiden). De eksemplene vi har ført inn i figuren er på ingen måte uttømmende. Dette er kun en illustrasjon av hvordan årsakene vi er interessert i henger sammen.

Ytterst til venstre finner vi «manglende risikoerkjennelse og -forståelse i samfunnet». Dette gir seg utslag i at forebyggende sikkerhet ikke nødvendigvis prioriteres eller inngår i lederporteføljen. Manglende kompetanse om forebyggende sikkerhet blant virksomhetens ledere kan manifestere seg ved lav prioritering og lite ressurser avsatt til det forebyggende sikkerhetsarbeidet. Dette fører igjen til at sikkerhetsorganisasjonene blir underdimensjonerte og at de ikke får tilstrekkelig opplæring. Dette gir seg utslag på mange forskjellige områder, for eksempel i form av dårlige sikkerhetsinstrukser som ikke er tilpasset virksomheten. Dårlige instrukser har selvfølgelig også sine konsekvenser… Alt dette og mer til gir «dårlig sikkerhetskultur» som vi har plassert øverst og langs hele aksen.



Figur 4.1 «Årsakskontinuum»

Det lengre til venstre på aksen en årsak ligger desto mer omfattende følgefeil produserer den bortover *kontinuum*-et. Det vil si at hvis vi «fikser» en slik fundamental årsak så vil det sannsynligvis føre til store forbedringer i sikkerhetskulturen vår og følgelig i det forebyggende sikkerhetsarbeidet. Samtidig så er det lettere sagt enn gjort å fikse risikoerkjennelse og -forståelse og lederforankring. Desto enklere er det å fikse, for eksempel et grunnlagsdokument for sikkerhet i en virksomhet. Sistnevnte kan føre til betydelig forbedring i det forebyggende sikkerhetsarbeidet men gir kun minimal uttelling på det forebyggende sikkerhetsarbeidet som helhet og på sikkerhetstilstanden i Norge.

For å bedre det forebyggende sikkerhetsarbeidet på en helhetlig og hensiktsmessig måte er det viktig å være bevisst kompleksiteten i årsakene som ligger til grunn for vår utførelse og etterlevelse innen forebyggende sikkerhet. Vi må også fokusere på det området i årsakskontinuumet hvor vi faktisk kan utgjøre en forskjell på kort sikt, for å, gjennom å påvirke årsakskjeden også i motsatt retning (fra høyre til venstre), på lengre sikt kunne oppnå en bedre risikoerkjennelse og -forståelse. På lang sikt kan vi få en bedre sikkerhetskultur, men det ligger i selve begrepet kultur at dette ikke er noe vi kan oppnå i løpet av kort tid. Årsakskontinuumet må ses som en helhet og alle områdene må tillegges tilstrekkelig vekt.

4.2 Anbefalinger

For å bedre det forebyggende sikkerhetsarbeidet på en helhetlig og hensiktsmessig måte må virksomhetene arbeide både kortsiktig og langsiktig med å bedre sikkerheten. På den ene siden bør det fokuseres på det området hvor vi faktisk kan utgjøre en forskjell på *kort sikt*. Eksempelvis bør det fokuseres mer på dokumentasjon av det forebyggende sikkerhetsarbeidet, for å sikre etterprøvbarhet og bevare kontinuiteten i sikkerhetsarbeidet når kritisk sikkerhetspersonell skiftes ut. Det bør også innarbeides bedre rutiner for rapportering og håndtering av sikkerhetstruende hendelser, gjennomføres øvelser innen forebyggende sikkerhet, arbeides for å øke ansattes forståelse om viktigheten av sikkerhetsklarering og autorisasjonssamtaler, og utvikle rutiner for å sikre kontinuerlig kontrollaktivitet i virksomheten. Slike tiltak kan på kort sikt styrke sikkerhetstilstanden i de fleste virksomheter underlagt sikkerhetsloven.

Samtidig må det arbeides *langsiktig* med å rette opp i fundamentale årsaker, som for eksempel å bedre «sikkerhetskulturen» i virksomheten. Men det ligger i selve begrepet «kultur» at dette ikke er noe som kan endres raskt på. Ledere må engasjere seg mer i sikkerhetsarbeidet og ha tettere dialog med ansatte i sikkerhetsorganisasjonen. Dette er helt avgjørende for å sikre at det bevilges ressurser som tar høyde for det aktuelle risikobilde, og derav sikre en bevisst styring av beredskap og forebyggende sikkerhet. Økt fokus på sikkerhet på ledelsesnivå kan dessuten bidra positivt ved å øke sikkerhetsbevisstheten i virksomheten totalt sett. På lang sikt kan vi få en bedre sikkerhetskultur, men det krever at det arbeides både kortsiktig og langsiktig med å bedre sikkerheten. Det sentrale fremover blir å se årsakskompleksiteten som en helhet og tillegge alle områdene tilstrekkelig vekt.

Forkortelser og enheter

AIM Norway	Aerospace Industrial Maintenance Norway
Beredskapsforskriften	Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen
BFF	Beredskapssystem for forsvarssektoren
CERT	Computer Emergency Response Team
DSL	Datasikkerhetsleder
Energiloven	Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m
EOS-loven	Lov om kontroll med EOS-tjenestene
EOS-utvalget	Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjenestene
E-tjenesten	Etterretningstjenesten
FD	Forsvarsdepartementet
FFI	Forsvarets forskningsinstitutt
FO/S	Forsvartes overkommando/Sikkerhetsstaben
FSA	Forsvarets sikkerhetsavdeling
HMS	Helse, miljø og sikkerhet
IKT	Informasjons- og kommunikasjonsteknologi
JD	Justis- og beredskapsdepartementet
KBO	Kraftforsyningens beredskapsorganisasjon
KDS	Kraftforsyningens distriktssjefer
KSL	Kraftforsyningens sentrale ledelse
NBS	Nasjonalt beredskapssystem
NCRS	NATO Crisis Response System
NorSIS	Norsk senter for informasjonssikring
NOU-er	Norges offentlige utredninger
NSM	Nasjonal sikkerhetsmyndighet
NSR	Næringslivets sikkerhetsråd
NUSB	Nasjonalt kompetansesenter for samfunnssikkerhet og beredskap
OED	Olje- og energidepartementet
PST	Politiets sikkerhetstjeneste
ROS	Risiko- og sårbarhetsanalyse
SBS	Sivilt Beredskapssystem
Sikkerhetsloven	Lov om forebyggende sikkerhetstjeneste
Sivilbeskyttelsesloven	Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret
SL	Sikkerhetsleder
SMK	Statsministerens kontor
SÅKOV	Sikkerhetstilstanden – årsaker, konsekvenser og virkemidler (forskningsprosjekt)
ÅMS	Årsaker til mangelfull sikkerhetstilstand (forskningsprosjekt)

Figurer

Referanser

Aftenposten 2013, Statsråder bryter sikkerhetsloven, 19. mars.

Beredskapsloven, se LOV-1950-12-15-7 .

Beredskapsforskriften, se FOR-2012-12-07-1157.

Beskyttelsesinstruksen, se FOR-1972-03-17-3352.

Bowen, Glenn A. 2009, Document Analysis as a Qualitative Research Method, Qualitative Research Journal, vol. 9, no. 2.

DoS - Denial of Service (compnetworking.about.com)

Domstolloven, se LOV-1915-08-13-5.

Energiloven, se LOV-1990-06-29-50.

Etterretningstjenesteloven, se LOV-1998-03-20-11.

FOR-1972-03-17-3352 Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen)

FOR-2001-06-29-721 Delegering av myndighet til Forsvarsdepartementet etter sikkerhetsloven § 12 andre ledd, § 15 fjerde ledd, § 16 andre ledd og § 29.

FOR-2001-06-29-722 Forskrift om personellsikkerhet.

FOR-2001-06-29-723 Forskrift om sikkerhetsadministrasjon.

FOR-2001-07-01-744 Forskrift om informasjonssikkerhet.

FOR 2001-07-01-753 Forskrift om sikkerhetsgraderte anskaffelser.

FOR-2003-06-27-802 Delegering av myndighet til Forsvarsdepartementet etter sikkerhetslovens § 2 tredje ledd.

FOR-2003-07-04-900 Fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet.

FOR-2004-02-12-1221 Delegering av myndighet til Petroleumstilsynet etter sikkerhetsloven.

FOR-2010-04-29-695 Instruks om sikkerhetstjeneste i Forsvaret.

FOR-2010-10-22-1362 Forskrift om objektsikkerhet.

FOR 2012-12-07-1157: Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften).

FD, Nyhet 29.04.2010: Ny instruks for sikkerhetsarbeidet i Forsvaret, www.regjeringen.no (lest: 25.04.2013)

FD, 2013, Sikkerhetsloven foreslås utvidet til Svalbard og Jan Mayen, 8 Mars. www.regjeringen.no (lest: 15.05.2013)

FD, Pressemelding Nr. 14/2013, Styrking av det forebyggende sikkerhetsarbeidet.

FD, Høringsbrev 15.11.2012, Forslag til ny forskrift om forsvars – og sikkerhetsanskaffelser.

Johansen, Iver, 2006, Scenarioklasser i Forsvarsstudie 2007: En morfologisk analyse av sikkerhetspolitiske utfordringer mot Norge, FFI-rapport 2006/02664.

Kleiven, R. et. al. 1995, I samfunnet. Samfunnslære for videregående skole.

Krippendorf, Klaus, 2013 (3rd ed.), Content Analysis: An Introduction to its Methodology, SAGE Publications.

LOV 1914-08-18-03 Lov om forsvarshemmeligheter.

LOV-1915-08-13-5 Lov om domstolene (domstolloven).

LOV-1950-12-15-7 Lov om særlige rådgjerder under krig, krigsfare og liknende forhold (beredskapsloven).

LOV 1953-06-26-8 Lov om oppfinnelser av betydning for rikets forsvar (lov om forsvarsviktige oppfinnelser).

LOV-1967-02-10 Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven).

LOV-1981-05-22-25 Lov om rettergangsmåten i straffesaker (straffeprosessloven).

LOV-1990-06-29-50. Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven).

LOV-1995-02-02-7 Lov om kontroll med etterretnings-, overvåknings- og sikkerhetstjeneste (EOS-loven).

LOV-1995-08-04-53 Lov om politiet (politiloven).

LOV-1996-11-29-72. Lov om petroleumsvirksomhet (petroleumsloven).

LOV 1998-03-20-10 Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven).

LOV-1998-03-20-11 Lov om Etterretningstjenesten (etterretningstjenesteloven).

LOV 2000-04-14-31 Lov om behandling av personopplysninger (personopplysningsloven).

LOV 2006-05-19-16 Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova).

LOV 2008-04-11-9 Lov om endringer i lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) (endringslov til sikkerhetsloven).

LOV-2010-06-25-45 Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven).

Meld. St. 21, 2012–2013, Terrorberedskap.

Meld. St. 17, 2002-2003, Om statlige tilsyn.

Phishing. (merriam-webster.com/dictionary/phishing)

What is a botnet? (microft.com/security)

NSM, 2012, Rapport om sikkerhetstilstanden 2012

NSM, 2011, Veileder i objektsikkerhet, Versjon 1, 2011-01-30

NSM, 2011, Rapport om sikkerhetstilstanden 2011

NSM, 2010, Sikkerhetsadministrasjon (veiledning), 2010-07-01

NSM, 2010, Rapport om sikkerhetstilstanden 2010

NSM, 2009, Veiledning i verdivurdering, 2009-04-14

NSM, 2009, Rapport om sikkerhetstilstanden 2009

NSM, 2008, Årsmelding 2008 (med 'Rapport om sikkerhetstilstanden – Status for 2008')

NSM, 2007, Hovedpunkter fra NSMs årlige Rapport om sikkerhetstilstanden 2007/2008

NSM, 2007, NSMs Risikovurdering 2007

NSM, 2006, Veiledning i risiko- og sårbarhetsanalyse, 2006-12-05

NSM, 2006, NSMs Risikovurdering 2006

NSM, 2005, NSMs Risikovurdering 2005

NSM, 2004, NSMs Risikovurdering 2004

NSM, 2003, Risikovurdering 2003

NSM, i. d. Historikk https://www.nsm.stat.no/Om-NSM/Historikk/ (10.05.2013)

NOU 2012:14 Rapport fra 22. juli-kommisjonen.

NOU 2006:6, Når sikkerheten er viktigst.

NOU 1994:4, Kontrollen med de hemmelige tjenestene. Innstilling fra EOS-kommisjonen oppnevnt ved Kgl. Resolusjon 24.september 1993. Avgitt 7. februar 1994.

OED, i. d. "Ansvarsområder". www.regjeringen.no

Petroleumsloven, se LOV-1996-11-29-72.

Sikkerhetsloven, se LOV 1998-03-20-10.

Sivilbeskyttelsesloven, se LOV-2010-06-25-45.

Standard Norge, 2012, Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi (NS 5830:2012)

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjenestene se EOS-utvalget.

Strøm-Erichsen, Anne-Grete, 2012, Forsvarsministerens foredrag på NSMs sikkerhetskonferanse 19. mars. www.regjeringen.no (26.06.2013)

Teknisk Ukeblad, 2013, Terror Mot Oljebransjen, 20 august.

Appendix A

Kodebok (operasjonalisert)

Søkeord:

År (mnd):
Tittel:

Nøkkelord:

Anledning for nyhetssaken:

Ikke kjent ☐

Negativ hendelse (e.g. sikkerhetsbrudd) ☐

Positiv hendelse (konferanse etc.) ☐

Sikkerhetstilstanden:

Eksplisitt nevnt		Implisitt omtalt		Ingen omtale
positiv omtale	☐	i positivt ordelag	☐	☐
negativ omtale	☐	i negativt ordelag	☐	
nøytral omtale	☐	i nøytralt ordelag	☐	

Trusler ☐ Sårbarheter ☐ Verdier ☐

Årsaker (eksplisitte/implisitte) til at sikkerhetstilstanden er som den er:

Menneskelige ☐ Organisatoriske ☐ Teknologiske ☐ Ingen omtale ☐

NSM: Omtales positivt ☐

" negativt ☐

" nøytralt ☐

Ingen omtale ☐

Kostnader forbundet med sikkerhet

Kostnader forbundet med sikkerhetsbrudd ☐

Kostnader forbundet med forebyggende tiltak ☐

Ingen omtale ☐

Kommentarer: