FFI-RAPPORT

16/00702

Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart

sluttrapport til Sikkerhetsutvalget

–
Jan Ivar Botnan
Rune Lausund

Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart

sluttrapport til Sikkerhetsutvalget

Jan Ivar Botnan
Rune Lausund

Forsvarets forskningsinstitutt (FFI) 24 oktober 2016

Emneord

Sikkerhetsloven
Kraftsektoren
Petroleumssektoren
Luftfartssektoren

FFI-rapport
FFI-RAPPORT 16/00702

Prosjektnummer
5148

ISBN
P: ISBN 978-82-464-2824-6
E: ISBN 978-82-464-2825-3

Godkjent av
Kjersti brattekås, *forskningsleder*
Janet Martha Blatny, a*vdelingssjef*

Sammendrag

På oppdrag fra Sikkerhetsutvalget, oppnevnt 27. mars 2015, har FFI gjennomgått håndtering av forebyggende sikkerhet i sektorene kraft, petroleum og luftfart. Det er identifisert svakheter og anbefalt tiltak i forbindelse med revisjon av sikkerhetsloven med forskrifter.

Studien viser at sektorene er godt organisert, men at regulering og håndtering av forebyggende sikkerhet av naturlige årsaker er svært forskjellig. God sikkerhet innen luftfart krever utstrakt internasjonalt samarbeid under felles regelverk. Luftfartsloven med tilhørende forskrifter er av den grunn sterkt preget av EU-rettsakter som detaljert regulerer sikkerheten og anviser løsninger. Sikkerhet i kraftsektoren er knyttet til forebyggende arbeid overfor naturgitte hendelser, og er i tillegg preget av etterkrigstidens krigs- og sabotasjeforebyggende tenkning. Sektorens beredskapsorganisasjon er godt regulert med tydelig fordeling av ansvar og myndighet. Forebyggende beredskap håndteres med god regulering, systemtilnærming og redundans. Utviklingen av petroleumsressursene på sokkelen har med stor suksess foregått i nært samarbeid med bransjen, noe som har brakt mye teknologi til landet. I petroleumssektoren drives også sikkerhetsarbeid, men med svak styring fra myndighetene.

Rapportens anbefalinger er basert på gjennomgang av lover, forskrifter og regelverk, samt relevante og tilgjengelige utredninger, hendelses- og øvelsesrapporter. I tillegg er det gjennomført samtaler og diskusjoner med relevante aktører i sektorene. De viktigste anbefalingene er:

- Det er behov for å styrke Forsvarets og justis- og beredskapssektorens formidling av trusselbildet til øvrige sektorer. Det langsiktige trusselbildet bør danne grunnlag for etablering av tverrsektorielle scenarioer og scenarioklasser som vedtas av regjeringen og gjøres gjeldende for beredskapsarbeidet i alle sektorer.

- «Økonomisk og finansiell handlefrihet» bør inkluderes som kriterium ved valg av skjermingsverdige objekter. Et «skjermingsverdig objekt» bør knyttes til kritiske samfunnsfunksjoner og relateres til et nytt begrep; «skjermingsverdig system». Et skjermingsverdig system er et system innen kritiske samfunnsfunksjoner som må beskyttes ved overvåkning, grunnsikring av objekter eller redundans.

- Det anbefales sikkerhetsklarering av i) personell med tilgang til sikkerhetsgradert eller sensitiv informasjon (sikkerhetsklarering), og ii) personell med adgang til kritiske anlegg, men uten behov for tilgang til sensitiv informasjon (adgangsklarering). Kriteriene for klarering bør være de samme for alle sektorer.

- Det anbefales at sektordepartementene kan pålegge virksomheter å delta i NorCERTs nasjonale varslingssystem for digital infrastruktur (VDI). Det bør også etableres bransjespesifikke CERT-er for alle sektorer hvor driftskontrollsystemer er avgjørende for sektorens virksomhet.

Summary

On contract by the Norwegian Commission for Protective National Security, FFI has studied the regulation and handling of security in three sectors; electric power, petroleum and aviation. Weaknesses are identified, and measures related to the revision of the Security act and its regulations are recommended. This study shows that the sectors are well organized, but with significant differences regarding regulation and management of security. Within the aviation sector, the security system requires extensive international cooperation under common rules. The Aviation Act and associated regulations are therefore strongly influenced by EU legislation, which in detail regulates Security and advices on solutions. Security in the electric power sector is linked to preventive security against natural disasters, and seems to be influenced by the post-war security culture. This sector's emergency response organization is well regulated with clear allocation of responsibility and authority. Security management is characterized by well-defined regulations, system approach and redundancy. The petroleum sector has been successfully developed in close cooperation between the government and the industry, which has brought a lot of technology to the country. Management and regulation of security is well-developed in this sector, however, but with weak governmental management.

The recommendations provided in this study are based on a review of laws, regulations and rules, as well as relevant and available reports. In addition, meetings and discussions with several relevant stakeholders in the sectors have contributed to the study. The main recommendations are:

- The Ministry of Defense and the Ministry of Justice should strengthen their communication to other sectors on the relevant threats. The long-term threat definition should form the basis for developing inter-sectoral scenarios and scenario classes used as the basis for measures and management of national security.

- "Economy and financial flexibility" should be included as a criterion when selecting “Sensitive object”. A "Sensitive object" should be linked to critical infrastructure and related to a new term; "Sensitive system."

- Security clearance should be performed for i) personnel with access to classified or sensitive information (security clearance), and ii) personnel with access to critical facilities, but with no need for access to sensitive information (entry clearance). The clearance criteria should be common for all sectors.

- The sector ministries should have the authority to require that companies and enterprises shall participate in NorCERT’s national warning system for digital infrastructure (VDI). All sectors where SCADA **(**Supervisory Control And Data Acquisition) systems are essential should establish specific CERT functions.

Innhold

1 Innledning

FFI har på vegne av Sikkerhetsutvalget oppnevnt 27. mars 2015, gjennomført en vurdering av det forebyggende sikkerhetsarbeid i kraft-, petroleums-, og luftfartssektoren. Det er gjennomført en kartlegging av dagens regulering og praksis i sektorene, og denne er vurdert opp mot sikkerhetsloven.

De tre sektorene er svært forskjellige, noe som også reflekteres i rapportens struktur. Luftfartssektoren er, når det gjelder sikring av lufthavner og fly, sterkt regulert gjennom et internasjonalt regelverk som er tatt inn i norsk lov og forskrifter. Petroleumssektoren er preget av en bransje med til dels store internasjonale konsern, en historie der man i Norge har utviklet en særdeles sterk håndtering innenfor «Safety», og der internasjonale konsern har operert i noen av verdens mest konfliktfylte områder og derigjennom utviklet systemer for operasjoner under terror- og krigstrussel. Kraftsektoren har en sterk og operativ beredskapsorganisasjon, og løser årlig flere tusen mindre og større naturgitte hendelser, teknisk svikt og ulykker. Sektoren har i tillegg en lang historie knyttet til forebyggende sikkerhet hvor sabotasje og krigstrusler er håndtert.

I rapporten er hver av sektorene gjennomgått og noen konklusjoner trukket. Dernest er de viktigste funnene relatert til oppdragsteksten oppsummert før rapporten avsluttes med hovedkonklusjoner og anbefalinger i kapittel 7. Det antydes også hvordan anbefalingene bør reflekteres i lover og forskrifter.

1.1 Oppdraget

Formålet med oppdraget, slik dette er formulert i oppdragsteksten, er å foreta en sikkerhetsfaglig vurdering av:

- hvorvidt sektorregelverket er tilstrekkelig for god sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner,
- om en overordnet lovregulering kan bidra til bedre forebyggende sikkerhet for ivaretakelse av kritiske samfunnsfunksjoner,
- hvilke forhold som eventuelt bør reguleres i et overordnet regelverk (lov og/eller forskrift).

FFIs vurderinger skal baseres på (Høyskolen i Akershus) HiOAs kartlegging av regelverk. Det skal velges ut regelverk for grundigere analyse i samråd med Sikkerhetsutvalget representert ved sekretariatet. HiOAs oppdrag inkluderer en kartlegging av myndighets- og ansvarsforhold innen forebyggende sikkerhet i utvalgte samfunnssektorer.

FFIs oppdrag skal lede ut i en sikkerhetsfaglig vurdering av styrker og svakheter ved gjeldende sektorovergripende regelverk og regelverk innen utvalgte samfunnssektorer. Forebyggende

sikkerhet for kritiske samfunnsfunksjoner skal vektlegges. I den sammenheng er det blant annet relevant å vurdere:

- Harmonisering og koordinering av risikovurdering og forebyggende sikkerhetstiltak på tvers av sektorer (ansvars og myndighetsstrukturer)
- Intern organisering i den enkelte sektor, herunder tilsynsregime og sanksjonsmuligheter ved manglende etterlevelse av regelverk
- Eventuell manglende tydeliggjøring av ansvar for sentrale funksjoner
- Overlappende/dupliserte ansvars-, myndighets-, og tilsynsoppgaver mellom virksomheter og/eller sektorer

Vurderingene vil metodisk ta utgangpunkt i etablerte standarder og anerkjente prinsipper for sikkerhetsarbeid og risikostyring. Det vil bli foretatt en vurdering av i hvilken grad organiseringen og ansvarsfordelingen innen de utvalgte sektorene er i tråd med de aktuelle standarder eller prinsipper.

Videre vil det bli foretatt en vurdering av samordningen mellom sektorene. Dette innbefatter:

- Trusselforståelse og risikovurdering:
    - I hvilken grad er det sammenfallende oppfatning av trusler mellom sentrale myndigheter, relevante etater og private virksomheter?
    - I hvilken utstrekning har relevante myndigheter og virksomheter tilgang til nødvendig informasjon for få etablert en riktig trusselforståelse?
    - I hvilken grad er det sammenfallende oppfatninger av sårbarhet for ulike samfunnsfunksjoner mellom sentrale myndigheter og relevante etater?
    - I hvilken grad benyttes en risikobasert tilnærming, og i hvilken grad er denne enhetlig i sektorene og mellom sektorene?
- Kritiske samfunnsfunksjoner:
    - avhengigheter mellom infrastrukturer og ressurser på tvers av sektorer
    - vurderinger av verdier og sårbarheter utover egen virksomhet
- Samordning/koordinering:
    - I hvilken grad forekommer det formalisert samordning mellom sektorene?

- Er ansvarsforholdene avklart?

- I hvilken grad samordnes tilsyn i og mellom sektorene, og i hvilken grad benyttes sårbarhets- og risikoforståelse ved tilsyn.

Der det fremkommer avvik mellom sektorer eller avdekkes mangelfull ansvarsfordeling vil det bli gjort en vurdering av om avvikene/funnene skyldes mangelfullt regelverk, uklart regelverk, manglende etterlevelse av regelverket, mangelfull tilretteleggelse for særskilte behov og/eller mangelfull sikkerhetskultur.

Relevant sektorregelverk vil også bli sammenholdt med reguleringen i sikkerhetsloven med forskrifter. I denne sammenheng vil det bli gjort en vurdering av om sikkerhetslovens regulering er en hensiktsmessig tilnærming til sikring av kritiske samfunnsfunksjoner og kritisk infrastruktur.

Gjennomføringen av oppdraget vil baseres på gjennomgang av relevante dokumenter, intervjuer med sentrale personer og skriftlig korrespondanse med relevante virksomheter.

Når det gjelder oversikt over relevant regelverk, samt ansvarsforholdene i dette, vil arbeidet hovedsakelig baseres på leveransen HiOAs leveranser.

2 Metode

Tidlig i arbeidet ble det i samarbeid med Senter for risikostyring og samfunnssikkerhet (SEROS) ved Universitetet i Stavanger (UiS) vurdert gjennomføring av en kvantitativ spørreundersøkelse i de utvalgte sektorene. SEROS-senteret leverte et tilbud til FFI, men hverken tid eller økonomiske ressurser muliggjorde en kvantitativ studie med tilstrekkelig kvalitetsnivå. UiS valgte derfor å avstå fra gjennomføring av studien. Med de rammer som har vært tilgjengelige, har vi, i forståelse med utvalgets sekretariat og SEROS-senteret, valgt en kvalitativ studie. De innledende samtalene med SEROS-senteret var av stor nytte for det videre arbeid.

Dette er en utredning som skal tjene Sikkerhetsutvalget arbeid basert på ordlyden i oppdragsteksten, og er ikke en rapport for vitenskapelig publisering. Arbeidet har hovedsakelig bestått i gjennomgang av lover, forskrifter og regelverk i de studerte sektorene, samt relevante og tilgjengelige utredninger, hendelses- og øvelsesrapporter. Dette utgjør til sammen et stort materiale og det kan ikke utelukkes at relevant informasjon har unnsluppet vår oppmerksomhet, spesielt sikkerhetsgraderte rapporter eller rapporter unntatt offentlighet. For å få tilgang til slikt materiale har vi vært avhengige av hjelp fra sektorrepresentantene. Gradert informasjonen, som vi har fått tilgang til, ville på enkelte punkter ha styrket argumentasjonen i rapporten, men det

ville ikke fått noen betydning for de endelige konklusjoner. Vi har derfor, med tanke på videre bruk, valgt å gjøre rapporten ugradert.

Det legges frem en oversikt over de møter som er avholdt, men vi identifiserer ikke hvem som har gitt hvilke uttalelser. Denne formen har vært hensiktsmessig i den forstand at vi har oppnådd stor grad av åpenhet under møtene.

De deskriptive avsnittene om kraft, petroleum og luftfart er gjennomgått av henholdsvis NVE, Petroleumstilsynet og Luftfartstilsynet for kontroll av fakta.

Gjennomførte intervjuer er oppsummert i tabell 2.1.

Tabell 2.1 Oversikt over avholdte møter

Kraftsektoren			
Myndighet/selskap	**Møtedato**	**Hovedkontakt**	**Kommentar**
NVE	21.12.2015	Sjefsingeniør Helge Ulsberg	Innledende møte med Beredskapsmyndigheten
NVE	30.3.2016	Vassdrags- og energidirektør Per Sanderud	Avsluttende møte for blant annet å sjekke faktaopplysninger
Statnett	12.2.2016	Konserndirektør Drift Øyvind Rue	Bredt sammensatt møte
Statkraft Energi A/S	8.2.2016	Senior Advicer Lars Holten	Bredt sammensatt møte inkludert SVP Operations and Maintenance management Ivar Arne Børset, og Head of Security and risk Eirin Kjølstad
Hafslund Nett A/S	3.3.2016	Beredskapsleder Even Ungersness	Bredt sammensatt møte inkludert administrerende direktør Kristin Lian
Petroleumssektoren			
Petroleumstilsynet	4.2.2016 og 11.2.2016	Fagdirektør Finn Carlsen	Gjennomført to møter med detaljert gjennomgang av

			strukturene i sektoren
Gassco	15.2.2016	Advicor Are Jacobsen	Gjennomført et møte, herunder gjennomgang av Gasscos ansvar og myndighet.
Norske Shell		Beredskapssjef Frode Auset	
Norsk Olje og gass	24.5.2016	Fagsjef HMS Aud Nistov	
ASD	31.5.2016	Seniorrådgiver Anders Østre	Bredt sammensatt møte med blant annet ekspedisjonssjef Ragnhild Nordaas.
Luftfartssektoren			
Luftfartstilsynet		Seniorrådgiver Bjørnar Davidsen	Gjennomført et møte i Bodø, samt flere telefonsamtaler og utveksling av epost
SD	4.3.2016	Fagdirektør Espen Aamodt	
Avinor	4.3.2016	Seniorrådgiver Asgeir Hagen	
Avinor - Luftkontroll	7.3.2016	Leder Drift og vedlikehold Asbjørn Gaustad	
Sektoruavhengige			
NSM	16.2.2016	Seniorrådgiver Klaus Søreide	NSM stilte med et bredt utvalg av representanter, inkludert avdelingssjefene Carsten Rapp og Vigdis Grønhaug

NorCERT	9.3.2016	Avd sjef Hans Christian Pretorius	
FSK	10.2.2016	Torgeir Mørkved	
FD	1.4.2016	Avdelingsdirektør Tore Jacobsen	

3 Trusselvurderinger

Terrorisme, sabotasje eller spionasje krever at noen har både intensjon og kapasitet. De må ville oss vondt og være i stand til å påføre oss skade. Motivene kan være svært forskjellige, basert på alt fra psykiske lidelser til gjennomarbeidede politiske strategier. De mentalt syke vil alltid representere en trussel, mens de politisk motiverte vil la seg inspirere av den politiske situasjonen og maktforholdene, slik de utvikler seg, nasjonalt og internasjonalt. Intensjon har derfor alltid vært vanskelig å forutsi fordi grunnlaget for den kan endre seg raskt. Terroristene må ha tilgang på effektive virkemidler for å lykkes.

Dette kapittelet har fokus på terroristhandlinger og trusler tilknyttet terrorisme.

3.1 Generell trussel mot Europa

Terrortrusselen mot Europa har endret seg fra perioden med intern trussel fra IRA (Irish Republican Army), ETA (Euskadi Ta Askatasuna), Røde brigader og Baader-Meinhof til en situasjon der Europa primært trues av terrororganisasjoner med utspring i konfliktområder utenfor Europa. Fra århundreskiftet har al-Qaida gjennomført flere vellykkede anslag mot Vesten og vestlige interesser, i samsvar med lederens uttalte mål. Etter fremveksten av ISIL (Den islamske staten i Irak og Levanten) var det lenge usikkert om de ville konsentrere sine ressurser i kampområdene i Syria og Irak, eller om de også ville rette angrep mot Europa. De har valgt det siste, trolig for å skremme Europa fra å engasjere seg militært. Slik strategi har virket tidligere; terrorbombene i Madrid i mars 2004, bidrog trolig til et annet valgresultat enn meningsmålingene før anslaget tydet på, og den nye regjeringen valgte å trekke spanske styrker ut av Irak. Det er liten tvil om at eksempelvis et vellykket angrep mot norsk petroleumsvirksomhet vil ha stor symbolverdi og kan få store konsekvenser, spesielt for gassforsyningen til Europa.

Vi har sett hvor omskiftelig trusselbildet er. Derfor er det krevende å gjennomføre risiko- og sårbarhetsanalyser som grunnlag for konstruksjon av infrastrukturelementer med forventet

levetid på flere tiår. Dette understreker behovet for at bransjen ikke bare har et tett samarbeid med de tjenester som tegner dagens trusselbilde, men også har inngrep med de forskningsmiljøer som studerer mer langsiktige trender.

Terroranslagene gir verdifull informasjon om hva man kan bli utsatt for. Statoil har høstet mye lærdom av hendelsen i In Amenas[1]. Terrorisme lykkes imidlertid ofte fordi den kommer uventet og nye virkemidler blir tatt i bruk. Improviserte bomber ble et av Talibans mest effektive våpen mot den internasjonale koalisjonen i Afghanistan. Teknologien ble utviklet og raffinert etter hvert som den overlegne motpart innførte motmidler, som deteksjonsutstyr og jammere. Teknologien er nå spredt til store deler av verden og har blitt benyttet ved flere av de store terroraksjonene i Europa. Mange av dem som kan ha ambisjon om å utføre terroraksjoner, vil trolig ha tilgang til komponenter som er nødvendige for å bygge bomber.

Trusselvurderingene fra PST[2] har påpekt at bruk av enklere virkemidler som håndvåpen og kniver, har blitt mer vanlig. Dette henger sammen med vestlig etterretnings forbedrede evne til å fange opp personer som reiser til Afghanistan for opplæring i terrorisme. Fremveksten av ISIL og det store antall fremmedkrigere fra Europa som har fått våpenopplæring, har igjen økt sannsynligheten for mer avanserte anslag. Bomber med spiker ble detonert på flyplassen og T-banen i Brussel i 2016. Nervegassen sarin [3]har blitt brukt under borgerkrigen i Syria. Under trusler om omfattende represalier, undertegnet Syria kjemivåpenkonvensjonen og aksepterte avrustning under oppsyn av FN. Dette har skjedd, men man har ingen garanti for at alt er destruert. Det er senere rapportert at ISIL[4] har benyttet giftige kjemikalier og det er godt dokumentert at dette inkluderer sennepsgass. Fremmedkrigerne får tilgang til ulike typer våpen som også kan benyttes i terrorisme.

Bombekastere og ustyrte raketter produseres rutinemessig av ulike terrorgrupper. Dette kan være hensiktsmessige virkemidler når man ønsker å påføre begrenset og uspesifikk skade fra avstander som gjør det mulig å unnslippe politiets reaksjon. Luftfarten har skjerpet beredskapen etter angrepene med passasjerfly 11. september 2001, men fortsatt kan det utrettes stor skade ved å styrte fly med mye drivstoff inn mot kritisk infrastruktur.

3.2 Trusselvurderinger IKT

Lysneutvalget[5] har kartlagt samfunnets digitale sårbarhet og foreslått konkrete tiltak for å styrke beredskapen og redusere sårbarheten. Utvalgets mandat var samfunnets sårbarhet overfor naturhendelser, ulykker og tilsiktede hendelser. Sikkerhetslovens virkeområde er imidlertid avgrenset til sabotasje, spionasje og terrorisme. Disse truslene representeres i hovedsak av sofistikerte angripere med høy kapasitet. Aktørene kan være statlige eller statsfinansierte grupper som bryter seg inn i IKT-systemer for å påføre skade eller hente informasjon som kan

[1] http://www.statoil.com/no/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf
[2] http://www.pst.no/media/74351/PSTs_tv2015-2.pdf
[3] https://en.wikipedia.org/wiki/Ghouta_chemical_attack
[4] http://www.reuters.com/article/us-mideast-crisis-iraq-chemicalweapons-idUSKCN0VO1IC
[5] https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

benyttes for å nå økonomiske, politiske eller militære mål. Motivene kan i ytterste konsekvens være forberedelser til fremtidige sabotasjeoperasjoner, terrorisme eller krig. Utsatte grupper er leverandører, utviklere og operatører knyttet til kritisk infrastruktur, for eksempel i forbindelse med plassering av digitale bakdører og utro tjenere.

Felles trusselforståelse er nødvendig for effektiv ressursutnyttelse i arbeidet for å forhindre bevisste anslag mot f eks prosesskontrollsystemer. Norske sikkerhetsmyndigheter har registrert en skjerping av den digitale trusselen mot norsk industri, ikke minst mot petroleumsindustrien[6]. Tidligere var digitale sårbarheter først og fremst et tema for tradisjonell informasjons- og kommunikasjonsteknologi. De seneste år har man imidlertid blitt oppmerksom på mulighetene for bevisste anslag.

Fremmede makter kan gjennom nettverksbaserte etterretningsoperasjoner i fredstid erverve inngående kjennskap til kritisk infrastruktur. Kunnskapen kan senere benyttes til å gjennomføre terroraksjoner. Flere land utvikler skadevare som vil kunne brukes til å sabotere infrastruktur eller forstyrre kritiske samfunnsfunksjoner. På den annen side arbeides det aktivt for å utbedre feil og tette smutthull. Utviklingen minner mer og mer om et våpenkappløp. Skadevare kan ramme alle systemer som er koblet til et nettverk. Brannmurer og antivirusprogramvare er ingen garanti mot kompromittering, selv om slike tiltak reduserer risikoen.

3.3 Hendelser

For å illustrere hva trusselen består i, har vi valgt å beskrive noen «vellykkede» hendelser.

I 2007 ble Estland [7]utsatt for et tjenesteangrep som i stor skala blokkerte informasjon fra myndighetene og isolerte viktige samfunnsfunksjoner. Samtidig ble websider kompromittert og brukt til å spre propaganda. Det er lett å forstå at slike angrep kan skape kaos og svekke forsvarsevnen. Trolig var det også hensikten.

I 2010 lyktes man med dataormen Stuxnet[8] å trenge inn i kontrollsystemet til sentrifugene som ble benyttet til å separere uranisotoper i Iran. Dette viser til fulle potensialet i utnyttelse av digitale sårbarheter, men angrep av denne typen er svært krevende. Derfor ble mistanken rettet mot teknologisk avanserte land som USA og Israel, men det er grunn til å frykte at også andre land kan være i stand til å gjennomføre så avanserte anslag.

Et annet bemerkelsesverdig anslag fant sted i 2008 mot rørledningen som frakter olje fra Det kaspiske hav til Middelhavet[9]. Rørledningen ble rammet av en eksplosjon med påfølgende brann ved byen Refaihye i provinsen Erzincan i det østlige Tyrkia. Den tyrkiske regjeringen hevdet det hele skyldtes en mekanisk feil, mens PKK raskt påsto at de hadde sprengt rørledningen, men senere etterforskning tyder på at eksplosjonen ble utløst av et avansert cyberangrep på ledningens kontroll- og sikkerhetssystem. Alarmer var slått av og

[6] https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2015-web.pdf
[7] https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
[8] https://en.wikipedia.org/wiki/Stuxnet
[9] http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

kommunikasjonen brutt slik at ingen alarm gikk av da trykket ble satt opp så rørledningen eksploderte. Det er interessant at eksplosjonen fant sted to dager før Russland gikk til angrep på Georgia. Oljeledningen opereres av British Petroleum (BP). Statoil har en eierandel på 8,7 %.

I 2013 ble et tysk stålverk[10] rammet av innbrudd i kontrollsystemene som ble manipulert slik at en masovn ikke lot seg stenge ned, noe som resulterte i massiv skade. Rapporter fra tyske myndigheter tyder på at angriperne fikk tilgang til prosesskontrollsystemet gjennom bedriftens administrative nettverk. Det ble infiltrert ved å sende eposter som tilsynelatende kom fra en trygg kilde og lurte mottageren til å åpne skadelige vedlegg eller besøke infiserte nettsteder. Angriperne hadde åpenbart hatt inngående kunnskap om kontrollsystemet og en utro tjener har trolig forbundet det administrative systemet med prosesskontrollsystemet. Dette viser at selv et frittstående nett kan bli kompromittert hvis man ikke har kontroll på sikkerhetsrutinene, herunder personellsikkerhet.

Et av de mest omfattende dataangrepene[11] mot Norge fant sted i 2014 og var rettet mot olje- og energisektoren. I slutten av august ble en rekke virksomheter varslet av NSM som da hadde avdekket over 50 forsøk på dataangrep i form av eposter med infiserte vedlegg. Årlig registreres et stort antall dataangrep. NSM/NorCERT registrerte[12] 20886 og håndterte 4327 saker i 2015, hvorav 22 anses som spesielt alvorlige.

Terroranslag med konvensjonelle midler blir hyppig utført mot petroleumsindustrien. Anslaget mot In Amenas i 2013 regnes imidlertid som et av de alvorligste. Onsdag 16. januar ble anlegget okkupert av den radikale islamistiske gruppen Den maskerte brigade og flere hundre arbeidere fra Algerie og åtte andre nasjoner ble tatt som gisler. Algeriske styrker stormet anlegget 19. januar. Minst 685 arbeidere fra Algerie og 107 utlendinger ble satt fri, mens 40 gisler og 32 gisseltakere ble drept, ifølge regjeringskilder. Statoil hadde 17 ansatte på anlegget, av disse omkom fem. Statoil oppnevnte i februar 2013 et utvalg under ledelse av generalløytnant (R) Torgeir Hagen for å kartlegge terroraksjonen 26. februar og «enable Statoil to further improve within the areas of security, risk assessment, and emergancy preparedness».

Gassanlegget Kreschba[13] nord i Algerie som driftes av Statoil og BP, ble 18. mars 2016 angrepet med raketter, men skadene ble små.

[10] https://www.wired.com/2015/01/german-steel-mill-hack-destruction/
[11] https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2015-web.pdf
[12] https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2016.pdf
[13] http://www.reuters.com/article/us-algeria-security-idUSKCN0WM0IN

4 Kraftsektoren

4.1 Innledning

I denne studien vil begrepet «Kraftsektoren» kun omfatte produksjon, overføring, regulering, transformering og distribusjon av elektrisk kraft fra vannkraftanlegg. Vi inkluderer ikke vindkraft og varmekraft i studien.. Norges totalproduksjon av elektrisk kraft var i perioden februar 2015 – januar 2016, 146 629 GWh. Av dette utgjorde vannkraft 140 674 GWh, vindkraft 3 507 GWh og varmekraft 2 447 GwH. Norge er normalt nettoeksportør av elektrisk kraft, og eksporterte i den nevnte perioden 21 844 GWh. Totalt produseres elektrisk kraft pr 1.1 2016 fra 26 vindkraftanlegg, 1543 vannkraftverk og 247 fjernvarmeanlegg. Tabellene[14] nedenfor viser fordelingen i installert ytelse og produksjonskapasitet.

Tabell 1.1: *Antall kraftanlegg i Norge*

Antall	**< 1 MW**	**> 1 MW**	**> 10 MW**	**> 100 MW**	**> 1000 MW**	**Sum**
Vindkraft	2	7	14	3	0	26
Vannkraft	570	637	256	80	0	1543
Fjernvarme	9	109	121	8	0	247

Tabell 1.2: *Installert produksjonskapasitet i norske kraftanlegg*

Ytelse [MW]	**< 1 MW**	**> 1 MW**	**> 10 MW**	**> 100 MW**	**> 1000 MW**	**Sum installert MW**
Vindkraft	0,8	17,75	594,35	434,70	0	1 047
Vannkraft	180	2160	9578	19305	0	31 223
Fjernvarme	5,97	543,4	3166,95	1291,00	0	5007,32

[14] Epost fra senioringeniør Amir Messiha, NVE datert 17.03.2016

Beredskapsarbeidet i elektrisitetsforsyningen skal inkludere sikring av;

- dammer,
- produksjonsanlegg,
- overføringsnett, delt i tre hoveddeler, sentralnettet, regionalnettet og distribusjonsnettet, samt transformatorstasjoner i alle de tre nevnte nettene
- reguleringssystem,

I det videre beskrives organisering i kraftbransjens beredskapsarbeid, samt de lover og forskrifter som regulerer arbeidet. Dernest vurderes styrker og svakheter med dagens organisering.

4.2 Organisering

Olje- og Energidepartementet gav i 2013 ut «Fakta – 2013 – Energi- og vannressurser i Norge»[15]. For mer informasjon om organiseringen i kraftsektoren vises det til kapittel 1 «Rammeverk, organisering og aktører» i kraftsektoren i denne publikasjonen.

Energiloven[16] § 9-1 definerer Kraftsektorens beredskapsorganisasjon (KBO). KBO omfatter alle enheter som eier og driver konsesjonspliktige energianlegg. Beredskapsmyndigheten (NVE) kan, når dette er hensiktsmessig, ved enkeltvedtak bestemme at også andre enheter enn de som automatisk er medlem av KBO, skal være en del av KBO. NVE skal utpeke den samlede ledelsen i KBO. Spesielt gjelder dette Kraftforsyningens sentrale ledelse (KSL) og Kraftforsyningens distriktssjefer. Alle KBO-enheter skal ha en beredskapsleder, beredskapskoordinator og en IKT-sikkerhetskoordinator. Koordinatorene er faglig kontaktpunkt til beredskapsmyndigheten.

For vassdragsanlegg gir damsikkerhetsforskriften[17] i §2 tydelige krav til organisering av beredskapsarbeidet (kap 4.3). NVE har tilsynsmyndighet for KBO-enheter og vassdragsanlegg.

Lover, forskrifter og veiledere innen kraftsektoren er meget tydelige når det gjelder plassering av ansvar og myndighet for kraftsektorens beredskapsarbeid. Sektorens operative beredskapsorganisasjon, samt dens beredskapssystemer, testes jevnlig ved naturgitte hendelser, tekniske feil og øvelser.

[15] Fakta 2013 – Energi- og vannressurser i Norge, Olje og energidepartementet (2013). ISSN 0809-9464
[16] Lov om produksjon, omforming, omsetning, fordeling og bruk av energi m.m. ISBN 82-504-1505-1
[17] Forskrift om sikkerhet i vassdragsanlegg (damsikkerhetsforskriften). FOR-2009-12-18-1600

4.3 Lover og forskrifter – sikring av dammer

Forskrift om sikkerhet ved vassdragsanlegg (damsikkerhetsforskriften) er hjemlet i lov om vassdrag og grunnvann[18] (vannressursloven) og regulerer sikkerhetsarbeidet i vassdragsanlegg. Damsikkerhetsforskriftens formål slik den er formulert i § 1- 1 er:

> Forskriften skal fremme sikkerhet ved vassdragsanlegg og forebygge skade på mennesker, miljø og eiendom

Forskriften forvaltes av NVE, og NVE gis myndighet til å pålegge krav, godkjenne planer, godkjenne organisasjon, godkjenne faglig kvalifikasjon for nøkkelpersonell, godkjenne beregningsgrunnlag, godkjenne tiltak og pålegge endringer. Konkret gir forskriften NVE hjemmel til i særskilte tilfeller å utpeke ansvarlig for et anlegg, samt endre organiseringen av sikkerhetsarbeidet.

Sikkerhetsarbeid ved vassdragsanlegg har i nasjonalt perspektiv to hovedpunkt i prioritert rekkefølge;

1. forebygge skade på mennesker, miljø og eiendom,
2. forsyningssikkerhet for elektrisk kraft.

For selskapene kommer i tillegg at vassdragsanleggene representerer store verdier og fremtidige inntekter.

Damsikkerhetsforskriften gir i §2 tydelige krav til organisering av det forebyggende sikkerhetsarbeidet. Eieren av anlegget er ansvarlig og skal i henhold til forskriften etablere en organisasjon som omfatter;

- Leder av vassdragsanlegget,
- Vassdragsteknisk ansvarlig (VTA) med stedfortreder,
- Tilsynspersonell.

En person kan, dersom krav til kvalifikasjon er oppfylt, ha flere roller.

NVE kan i særskilte tilfeller kreve at antallet i organisasjonen økes, samt godkjenne en annen ansvarlig enn eieren.

Det stilles tydelige kvalifikasjonskrav til utdanning og erfaring for vassdragsanleggenes

- Leder
- VTA
- Stedfortredende VTA
- Fagansvarlig
- Utførende foretak og anleggsleder

[18] Lov om vassdrag og grunnvann (vannressursloven). LOV-2000-11-24-82

- Kontrollør

NVE skal som nevnt godkjenne at krav til kvalifikasjon er oppfylt.

Alle vassdragsanlegg skal klassifiseres i en av fem (klasse 0 – 4) konsekvensklasser. Den ansvarlige skal foreta en vurdering av anlegg og omgivelser og sende søknad om klassifisering. NVE treffer vedtak om konsekvensklasse. Forskriften setter tydelige kriterier for de fem klassene, og knytter disse til antall boliger, infrastruktur og miljø som vil påvirkes av vannføring fra et ødelagt anlegg. Forskriften er i §5-3 eksplisitt om at anlegg i konsekvensklasse 3 og 4 skal dimensjoneres og kontrolleres mot tilsiktede hendelser i fred, under beredskap og i krig. Forskriften gir krav til den dokumentasjon som kreves ved en søknad, og gir NVE myndighet til å pålegge ansvarlig å fremme tilleggsdokumentasjon ved behov.

Det overordnede krav til sikkerhetsnivå er «-et tilstrekkelig høyt sikkerhetsnivå, slik at det ikke inntrer brudd, svikt eller feilfunksjon». Dette er i utgangspunktet uspesifisert, men § 5 «Tekniske krav» i forskriften gir meget tydelige og spesifiserte krav til vassdragsanlegget. I tillegg er forskriftens §5-1 klar når det gjelder kompenserende tiltak, godkjenning av slike tiltak, samt NVEs myndighet til å spesifisere innholdet i de tekniske kravene gitt i §5.

Forskriftens §5-3 beskriver de laster som skal vurderes. De mest sentrale er permanente, variable og miljømessige laster. I §5-3 punkt c gjennomgås andre relevante ulykkeslaster i tillegg til flom. Blant disse er «eksplosjon, last som følge av tilfeldig ulykkeshendelse eller sabotasje/terror i fred og under beredskap og krig»

Som nevnt gir § 5 et godt teknisk og faglig fundert kravsett med kriterier. Forskriften beskriver kontrollregimet, og gir totalt sett inntrykk av meget god regulering for å redusere konsekvensen ved hendelser, enten disse er tilsiktet eller har naturgitte årsaker.

I § 7 beskriver forskriften krav til drift av vassdragsanlegget. Det stilles i § 7-2 krav til overvåkning, herunder kontinuerlig overvåkning av tilgang til anlegget der dette kreves. Tilstandsparametere skal måles og tilsyn skal utføres etter spesifiserte krav for de ulike konsekvensklasser.

I § 7-4 gjennomgås krav til beredskapsplaner. Disse skal baseres på analyse av risiko og sårbarhet, samt på beregning av dambruddsbølger. Kriterier er gitt i §7-3.

Informasjonssikkerhet er omhandlet i § 7-8. Det gis krav om at informasjon skal sikres. Det kreves effektiv avskjerming og tilgangskontroll. Utover dette er ikke krav til informasjonssikkerhet spesifisert. Forskriften sier at «NVE kan treffe vedtak om at informasjon om vassdragsanlegg skal behandles i henhold til bestemmelsene i lov 20. mars nr 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven)[19]». Dette er forskriftens eneste referanse til sikkerhetsloven.

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

NVE har utarbeidet en rekke veiledere til damsikkerhetsforskriften. Disse omfatter blant annet veiledning til;

- Klassifisering av anlegg
- Planlegging og bygging
- Veiledning for fyllingsdammer
- Sikring ved vassdragsanlegg

NVE har tilsyns- og veilederansvar, og veilederne er, som det uttrykkes i forordet til veileder 3/2014[20], «ment som et hjelpemiddel for personell hos ansvarlige for vassdragsanlegg og for rådgivere». Utover sin rådgivende funksjon er veilederne også i enkelte sammenhenger kravdokumenter. Der krav listes, angir veilederne absolutte krav, minimumskrav og anbefalinger. Dette blir markert i aktuell veilederes bruk av «må», «må minst» og «bør».

Pålegg om sikring mot krigshandlinger og sabotasje av kraftverksdammer har eksistert siden lov om forsvarsmessig sikring av kraftforsyningen ble vedtatt i 1948. I beredskapsforskriften[21] (forebyggende sikkerhet og beredskap i energiforsyningen) er krigslaster omtalt under §5-3. Konsekvensreduserende tiltak vil være lik enten bakgrunnen for hendelsen er naturgitt, teknisk feil eller en tilsiktet handling. Det veiledes dermed ikke spesifikt i anbefalte beskyttelsestiltak knyttet til tilsiktede hendelser.

4.4 Lover og forskrifter – energiloven med forskrifter

Kraftsektoren reguleres gjennom «Lov om produksjon, omforming, overføring, omsetning og bruk av energi» (energiloven), datert 29. juni 1990. Kapittel 9 «Beredskap» regulerer håndtering av beredskap og forebyggende sikkerhetstiltak. Kraftforsyningens beredskapsorganisasjon (KBO) er den sentrale enheten i beredskapsorganiseringen, og defineres i energilovens §9-1.

> Kraftforsyningens beredskapsorganisasjon (KBO) består 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, omsetting eller fordeling av elektrisk energi eller fjernvarme. Beredskapsmyndigheten kan ved forskrift eller enkeltvedtak fastsette hvilke enheter som skal inngå i KBO

I motsetning til i damsikkerhetsforskriften omtales ikke NVE i energiloven eller i beredskapsforskriften. Dette er begrunnet i Ot.prp. nr. 56 (2000-2001)[22] der begrepet «beredskapsmyndigheten» ble innført i stedet for «NVE» i energilovens § 9-7. Enkelte høringsinstanser til Prop.112 L (2010–2011) «Endringer i energiloven og i enkelte andre lover», påpekte at begrepet «beredskapsmyndigheten» er uklart. Energiloven ble derfor endret slik at begrepet «beredskapsmyndigheten» ble innarbeidet konsekvent i hele lovens kapittel 9 om

[20] Veileder til damsikkerhetsforskriften 3/2014. NVE (www.nve.no)
[21] Forskrift om forebyggende sikkerhet i energiforsyningen (beredskapsforskriften). FOR-2012-12-07-1157

[22] Ot Prop 56 (2000-2001)

beredskap. Departementets myndighet er delegert til NVE, som har oppgaven som beredskapsmyndighet med den myndighet som fremgår av lovbestemmelsene, jf. delegeringsvedtak av 14. september 2009 nr. 1191. Det ble understreket at endringen ikke innebærer noen endring i ansvarsfordelingen mellom NVE og departementet.

Det er beredskapsmyndigheten, altså NVE, som skal samordne beredskapsarbeidet og utpeke den samlede ledelsen i KBO. Videre sier §9-1 i energiloven at «Beredskapsmyndigheten kan under beredskap og krig underlegge kraftforsyningen KBO. Kraftforsyningen plikter å følge de pålegg som gis og gjennomføre de tiltak som kreves.»

De overordnede krav knyttet til beredskap er omhandlet i energiloven §9-2. Hovedpunktene er:

- Eier av anlegg plikter å sørge for effektiv sikring og beredskap og iverksette forebyggende tiltak,
- Beredskapsmyndigheten kan gi forskrift eller treffe enkeltvedtak om beredskapstiltak for å forebygge, håndtere eller begrense virkning av ekstraordinære situasjoner,
- Beredskapstiltak kan gjelde for eksisterende og planlagte anlegg eller systemer,
- Vedtak om beredskapstiltak kan omfatte blant annet organisering, planlegging, forebygging, sikkerhets- eller sikringstiltak, utførelse, gjennomføring, gjennomrettingsevne, ledelse og drift,
- Beredskapsmyndigheten kan treffe vedtak om at drift i ekstraordinære situasjoner skal kunne skje fra norsk territorium,
- Den som pålegges beredskapstiltak plikter å gjennomføre tiltakene for egen regning og risiko,
- Beredskapsmyndigheten kan, uten hensyn til tidligere pålegg, treffe vedtak om at nye eller endrede beredskapstiltak skal settes i verk.

Beredskapsforskriften stiller tydelige krav og gir sammen med veilederen[23] detaljerte krav til forebyggende tiltak. I §2 beskrives generelle krav til ansvar, organisasjon og funksjon, samt beredskapsplikt.

Beredskapsorganisasjonen skal som nevnt ha en leder, beredskapskoordinator og en IKT-sikkerhetskoordinator. Koordinatorene er faglig kontaktpunkt til beredskapsmyndigheten. Det stilles i §2-4 krav om at «alle KBO enheter skal gjennomføre risiko- og sårbarhetsanalyser knyttet til ekstraordinære forhold». Omfanget defineres og minimum en årlig gjennomgang kreves.

[23] Veiledning til forskrift om forebyggende sikkerhet i energiforsyningen. 1/2013 (www.nve.no)

Begrepet ekstraordinære situasjoner er sentralt i forskriften. Forskriften gir ikke en entydig definisjon av hvilke situasjoner dette omfatter, men NVEs veileder beskriver ekstraordinære situasjoner i kapittel 1.2.2 som «alle former for ekstraordinære situasjoner som kan skade eller hindre energiforsyningen, slik som naturgitte skader, omfattende teknisk svikt og påført skade». Påført skade inkluderer tilsiktede handlinger. Veilederen nevner eksempler på slike handlinger, herunder sabotasje, terror og krigsliknende handlinger.

Til tross for at tilsiktede handlinger omfattes i lov, forskrift og veileder, er hverken energiloven, beredskapsforskriften eller veilederen tydelig når det gjelder krav til tiltak. Det er understreket i flere samtaler at konsekvensreduserende tiltak er uavhengig av årsaken til en hendelse. Kravet, slik det er formulert i veilederen, er dermed først og fremst knyttet til sannsynligheten for at en tilsiktet hendelse skal inntreffe. Veilederen sier at man må se nærmere på hvor stor sannsynlighet det er for å utføre tilsiktede handlinger, og at stor grad av sannsynlighet og store konsekvenser vil fortelle mye om sårbarhetsbildet. Veilederen viser ikke til hvilke scenarioer som skal legges til grunn for ROS-analyser. Derimot henviser veilederen til at ROS analyser er til stor hjelp for å avdekke aktuelle scenarioer for øvelser.

§3-5 i beredskapsforskriften regulerer ansvar og oppgaver for KBO-enheter eller KBO under beredskap og krig. Paragrafen er hjemlet i energiloven § 9-1. Forskriften slår tydelig fast at Departementet under beredskap og krig kan underlegge energiforsyningen KBO og at Beredskapsmyndigheten kan instruerer kraftforsyningens distriktssjefer og KBO. Kraftforsyningens sentralledelse (KSL) overtar ledelsen av KBO, og Statnett skal i slike situasjoner være KSLs utøvende organ for regulering av produksjon, omforming, overføring og fordeling av elektrisk energi. Det kreves at Statnett innretter sin organisasjon slik at myndighet kan utføres regionalt i tett dialog med kraftforsyningens distriktssjefer.

4.5 Oppsummering/Konklusjon

4.5.1 Generelt om sikkerhetsarbeidet i kraftsektoren

Kraftsektoren har en lang historie knyttet til sikring mot skader forårsaket av sabotasje, terror og krigshandlinger. Lov om forsvarsmessig sikring av kraftanlegg ble vedtatt i 1948. Her er forebygging og beredskap mot krigs- og sabotasjehandlinger sentralt. Gjeldende energilov, samt sikkerhetskulturen i NVE og de intervjuede selskapene, bærer preg av denne historien. Det legges meget stor vekt på redundans og fleksibilitet, og det presiseres fra intervjuede selskaper at beredskapsplaner, -organisasjon og –utstyr testes jevnlig både gjennom øvelser og reelle større og mindre naturgitte hendelser. Figur 4.1 er hentet fra veileder 1/2013 til beredskapsforskriften, og viser det helhetlige beredskapskonseptet i sektoren slik dette er presisert fra beredskapsmyndigheten (NVE).

Figur 4.1 Kraftsektorens helhetlige beredskapskonsept hentet fra veileder 1/2013 til beredskapsforskriften

Krav til kunnskapsnivå hos aktørene er høyt, og sikres gjennom etablerte pålegg gitt av forskrifter og beredskapsmyndigheten (NVE), samt godkjennings- og tilsynsrutiner. Inntrykket er at dette er sterkest regulert innen fysisk sikring og mindre regulert fra beredskapsmyndighetens side innen IKT-sikkerhet. NVE har gitt krav/føringer innen IKT-sikkerhet i veilederen:

Krav om reparasjonsberedskap (veilederens 4.3.4) i driftskontrollsystemer (=IKT-systemer), inkl. krav om tilstrekkelig personell med spesialkompetanse (veilederens 4.2.3).

Krav om utstyr og prosedyrer for effektiv deteksjon og håndtering av uønskede hendelser i driftskontrollsystememe (=IKT-systemer), veilederens kap. 5.II.2 og 5.II.3 og kap. 4.3.5.7 (responstider).

NVE har nylig gjennomført skriftlige revisjoner med konkrete spørsmål angående IKT sikkerhet i prosesstyringen for å følge opp at selskapene har nødvendig utstyr og prosedyrer for å håndtere IKT-hendelser. KraftCERT har assistert NVE med å lage spørsmålene i revisjonen.

Denne studien vurderer ikke kvaliteten på sikkerhetsarbeidet, men kun de rutiner og ordninger som er etablert, og ser dette opp mot Sikkerhetsutvalgets arbeid. Det må likevel påpekes at inntrykket er et meget høyt og kompetent sikkerhetsarbeid, særlig knyttet til naturgitte hendelser, ulykker, tekniske feil og sikring av anlegg mot uvedkommende. Når det gjelder forebyggende sikkerhet mot tilsiktede hendelser, er dette en integrert del av sikkerhetsarbeidet. Vi har ikke funnet tydelig veiledning knyttet til;

- hvilke scenarioer som legges til grunn,
- hvilke kriterier som skal vektlegges, og

- hvordan forebyggende tiltak overfor tilsiktede handlinger kan avvike fra tilsvarende tiltak overfor naturgitte hendelser.

4.5.2 Informasjonssikkerhet

Informasjonssikkerhet i kraftsektoren er regulert av energilovens §9-3, hvor det understrekes at KBO-enheter,

- skal kartlegge sensitiv informasjon,
- vite hvor informasjonen befinner seg, samt
- påse at skjermings- og beskyttelsestiltak er etablert.

Kravet er (§9-3) utvetydig; «enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen».

Beredskapsforskriften definerer i §6-2 hva som omfattes av begrepet sensitiv informasjon. Definisjonen er omfattende og spesifikk. Overordnet sier forskriften at «med sensitiv informasjon menes spesifikk og inngående opplysninger om anlegg energiforsyningen som kan brukes til å skade eller påvirke funksjoner som har betydning for energiforsyningen». Deretter spesifiseres dette i ti punkter.

Det stilles krav til at det skal finnes systemer for merking, oppbevaring, bruk, distribusjon og tilintetgjørelse av informasjon, og det stilles krav om at det skal etableres tiltak for intern og ekstern rapportering av sikkerhetshendelser. Det vises i forskriften ikke til hvordan merking skal gjennomføres, og det stilles ikke krav til sikring av informasjon for de områder sikkerhetsloven omfatter, dvs skadefølger for Norges, og våre alliertes sikkerhet, samt forholdet til fremmede makter. Det er ingen referanser til merkesystemer brukt i sikkerhetsloven, men veilederen (1/2013) har et eget punkt (6.2.15) om merking av dokumenter. Her vises det til at KBO-enheten har plikt til å vurdere hva som er sensitiv informasjon. Sensitiv informasjon skal merkes slik:

Bokmål	Nynorsk
Underlagt taushetsplikt etter energiloven § 9-3 jf bfe § 6-2. Unntatt fra innsyn etter offentleglova § 13.	Underlagd teieplikt etter energiloven § 9-3 jf bfe § 6-2. Unntatt frå innsyn etter offentleglova § 13.

Det stilles ikke krav til sikkerhetsklarering av det personell som har tilgang til og håndterer sensitiv informasjon, men beredskapsforskriften stiller krav om taushetsplikt, inngåelse av sikkerhetsavtaler med underleverandører, etablering av tilgangskontroll, avskjerming og beskyttelse, samt til etablering av sikkerhetsinstrukser. I tillegg klarerer NVE personell i sektoren for håndtering av sensitiv og sikkerhetsgradert informasjon. NSM fører tilsyn med NVEs klareringsrutiner.

Forskriften stiller som tidligere nevnt krav til at det skal være en IKT-sikkerhetskoordinator i alle enheter som omfattes av forskriften, og det stilles krav til gjennomføring av ROS-analyser.

Alle intervjuede selskaper tar informasjonssikkerhet og IKT-sikkerhet meget alvorlig. Det samarbeides med NorCERT, hvor alle intervjuede selskaper kjøper tjenesten som knytter selskapene til det nasjonale varslingssystem for digital infrastruktur (VDI). Det er uttalt at NorCERT ikke har inngående kunnskap om kraftsektorens prosesskontrollsystemer.

NVE har derfor tatt initiativ til, men ikke pålagt, etableringen av en «kraftCERT». Statkraft, Hafslund Nett og Statnett har etablert KraftCERT A/S for å bedre sikkerheten i sektorens prosesskontrollsystemer. KraftCERT bistår kraftbransjen i trusselforståelse, kunnskap om sårbare punkter, samt deteksjon og motvirkning av digitale angrep. KraftCERT samarbeider med NorCERT. Det understrekes at KraftCERT leverer tjenester til hele bransjen uavhengig av eierstrukturen, samt at KraftCERT skal bidra til informasjonsdeling mellom selskapene i sektoren.

4.5.3 Objektsikkerhet

Objektsikring i kraftsektoren er forankret i energiloven § 9 Beredskap. Ingen objekter i sektoren er innmeldt som skjermingsverdige objekter i henhold til sikkehetsloven og objektsikringsforskriften[24]. Objektsikkerhetsforskriften § 1-3 sier at «der det finnes relevante og tilstrekkelige bestemmelser innenfor sektorlovgivningen, og det er etablert tilsynsorgan, går disse foran bestemmelsene i denne forskriften». Det avgjørende spørsmålet er dermed om kraftsektorens lover og forskrifter også dekker sikkerhetslovens krav.

Beredskapsforskriften stiller generelle krav til beredskap, definerer og stiller krav til organisering av sektorens beredskap, klassifiserer anlegg, stiller krav til sikringstiltak innen hver klasse, og har krav til informasjonssikkerhet og IKT sikkerhet. Lov og forskrift er, som nevnt, tydelig når det gjelder ansvar og myndighet i beredskapsorganisasjonen.

Klassifisering av anlegg, leveransesikkerhet, sikring av befolkning og miljø, samt sikring av kritiske funksjoner for det sivile samfunnet er sentralt i alle lover og forskrifter knyttet til sikring av vassdragsanlegg og produksjon, overføring, distribusjon og bruk av elektrisk energi. Klassifisering gjennomføres ikke i henhold til sikkerhetslovens § 17 som omfatter:

- Betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket,
- Betydning for kritiske funksjoner for det sivile samfunn,
- Symbolverdi, og
- Mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse

[24] Forskrift om objektsikkerhet. FOR-2010-10-22-1362

Valgt klassifisering er derimot basert på anleggenes tekniske ytelse, men også for om de har spesielt stor betydning på kraftforsyningen lokalt i området. Den overordnete vurdering er basert på sektorens leveransesikkerhet.

Fra lov om forsvarsmessig sikring av kraftanlegg (1948), og til dagens lovverk er anlegg klassifisert. I damsikkerhetsforskriften er dette knyttet til konsekvensklasser. I beredskapsforskriften defineres tre klasser (§ 5-2) basert på anleggets «betydning for drift eller gjenoppretting av eller sikkerhet i produksjon, omforming, overføring eller fordeling av elektrisk energi eller fjernvarme».

Beredskapsforskriften stiller i egne vedlegg konkrete og detaljerte krav til hvordan sikring skal gjennomføres i de definerte klassene. Det henvises til normer og standarder. Det sies i vedleggene at «dersom et minst like godt sikringsnivå kan dokumenteres, kan beredskapsmyndigheten akseptere andre sikringstiltak enn de som er beskrevet». Det åpnes dermed for at selskapene kan etablere nye og bedre sikkerhetsløsninger, samtidig som det angis krav til en grunnsikring som alle skal oppfylle.

De tiltak som kreves dekker i stor grad objektsikkerhetsforskriftens (§ 3-1) krav til grunnsikring bestående av en kombinasjon av barrierer, deteksjon, verifikasjon og reaksjon. På noen områder går beredskapsforskriften lenger enn objektsikkerhetsforskriften. Veileder 1/2013 er meget detaljert, og etter vår vurdering på noen områder for detaljert.

Beredskapsforskriften har en betydelig fysisk tilnærming til grunnsikringen, og presiserer ikke slik objektsikringsforskriften sier at «barrierer kan være av fysisk, elektronisk eller administrativ art». Når det gjelder trusselnivå som det skal sikres mot, henviser beredskapsforskriften (§5-1) til ekstraordinære situasjoner. Her er sabotasje og kriminelle handlinger spesifikt omtalt. Hensyn til sikkerhetspolitisk krisehåndtering eller forsvar av riket (krig) omtales ikke.

4.5.4 Personellsikkerhet

Sikkerhetsklarering og autorisering av personell, slik dette defineres i sikkerhetslovens § 19, er ikke tatt inn i energiloven eller beredskapsforskriften. Det stilles i lovverket ikke krav til bakgrunnssjekk av personell som skal ha tilgang til sensitiv informasjon i kraftsektoren, eller til personell som skal ha tilgang til et anlegg.

Det stilles strenge krav til taushetsplikt med hjemmel i energiloven § 9-3 hvor det står at «enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen». Og at «departementet kan gi nærmere forskrifter om informasjonssikkerhet i kraftforsyningen og om taushetsplikten». Det stilles i beredskapsforskriften § 6-7 krav til at personell «som vil kunne få tilgang til informasjon som er sikkerhetsgradert etter lov 20. mars 1998 nr 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven), skal være sikkerhetsklarert og autorisert. Autorisasjon for BEGRENSET kan skje uten forutgående sikkerhetsklarering». Det tas dermed i forskriften høyde for klarering av personell for å få tilgang til graderte trusselvurderinger, samt tilgang til informasjon knyttet til Forsvarets eventuelle vurdering av et anleggs betydning i en nasjonal sikkerhetspolitisk krise.

NVE gjennomfører sikkerhetsklarering av personell i sektoren, og gjennomfører bakgrunnssjekk av personell som har behov for tilgang til sensitiv og sikkerhetsgradert informasjon. NSM fører tilsyn med NVEs klareringsrutiner.

Det legges stor vekt på at ingen uvedkommende skal ha tilgang til anleggene. Dette gjelder for vassdragsanlegg og alle anlegg som faller inn under energiloven. Beredskapsforskriften krever at alle anlegg i klasse 1 – 3 skal ha adgangskontroll. Videre stiller forskriften i § 5-11 krav til besøksrestriksjoner for alle driftssentraler i klassifiserte driftskontrollsystemer, og alle energianlegg klassifisert i klasse 3 (høyeste klasse). Besøkskontroll betyr at besøkende skal følge en fast avgrenset rute, være ledsaget av en erfaren og ansvarlig representant for anlegget, at opplysninger om sensitiv informasjon ikke skal gis, og at fotografering normalt er forbudt. Beredskapsmyndigheten kan pålegge anlegg i lavere klasse besøksrestriksjon.

Beredskapsforskriften stiller i § 7 krav til beskyttelse av driftskontrollsystemer. I § 7-4 stilles det krav til brukertilgang. Det skal være kontrollordninger for tilgang, virksomheten skal til enhver tid kunne kontrollere hvilke personer som er eller har vært pålogget, også når ekstern tilkobling benyttes, og kontrollordningene skal gjennomgås minst en gang hvert år.

4.5.5 Sikkerhetsgraderte anskaffelser

Beredskapsforskriften stiller i § 6-5 krav ved anskaffelse av tjenester fra underleverandører. KBO-enheten skal påse at underleverandører etterlever bestemmelsene om informasjonssikkerhet og taushetsplikt for sensitiv informasjon. KBO-enheten skal i avtalen med en underleverandør opplyse om at beredskapsmyndigheten kan føre tilsyn med etterlevelse av bestemmelsene nevnt i §6-5. Dersom en leverandør velger å benytte egne underleverandører, gjelder fortsatt denne opplysningsplikten.

Anbudsinnbydelser kan med hjemmel i beredskapsforskriftens § 6-6 begrenses for å hindre at sikkerhetsgradert eller sensitiv informasjon om energiforsyningen blir offentlig tilgjengelig gjennom anbudsdokumentene. Her henvises det til anskaffelsesregelverket uten at dette er nærmere presisert i selve forskriften. I veileder 1/2013 til beredskapsforskriften er dette nærmere presisert, og det vises til lov om offentlig anskaffelse med forskrifter, samt til sikkerhetsloven med forskrifter. Det presiseres at «dersom anbudsdokumentene eller oppdraget inneholder sensitiv informasjon, kan anbudet begrenses ved at kun leverandører som har inngått sikkerhetsavtale med KBO-enheten, får tilsendt anbudsdokumenter».

Det i stilles i veilederen «må-krav» til etablering av sikkerhetsavtale. Det understrekes i veilederen at det er KBO-enhetens ansvar å sikre korrekt håndtering av sensitiv informasjon. Fram til 01.01.2014 fantes en ordning med landsdekkende sikkerhetsavtaler, men etter 01.01.2014 inngår NVE sikkerhetsavtaler kun med egne leverandører. KBO-enhetene har som nevnt ansvar for å etablere egne sikkerhetsavtaler, og kan benytte NVEs mal for hvordan sikkerhetsavtale skal etableres.

5 Petroleumssektoren

5.1 Roller og ansvar

5.1.1 Olje- og energidepartementet

Olje- og energidepartementet (OED) har det overordnede ansvar for forvaltningen av petroleumsressursene på den norske kontinentalsokkelen. Departementet skal se til at petroleumsvirksomheten foregår etter de retningslinjer Stortinget og regjeringen gir, og har i tillegg et eieransvar for de statlige selskapene Petoro AS og Gassco AS og for det delvis statseide oljeselskapet Statoil ASA.

5.1.2 Oljedirektoratet

Oljedirektoratet er administrativt underlagt OED og er et statlig fagdirektorat og forvaltningsorgan for norsk petroleumsvirksomhet. Oljedirektoratet har et nasjonalt ansvar for at data og informasjon fra petroleumsvirksomheten er tilgjengelig. Oljedirektoratet har en sentral rolle innenfor petroleumsforvaltningen og er et viktig rådgivende organ for OED. Direktoratet utøver forvaltningsmyndighet og skal bidra til å skape størst mulige verdier for samfunnet fra olje- og gassvirksomheten gjennom en forsvarlig ressursforvaltning med forankring i sikkerhet, beredskap og ytre miljø.

5.1.3 Arbeids- og sosialdepartementet

Arbeids- og sosialdepartementet (ASD) har det overordnede ansvaret for forvaltning av arbeidsmiljøet og for sikkerhet og beredskap på norsk sokkel. Departementet gir føringer for Petroleumstilsynets prioriteringer gjennom årlige tildelingsbrev.

5.1.4 Petroleumstilsynet

Petroleumstilsynet er et selvstendig, statlig tilsynsorgan med myndighetsansvar for sikkerhet, beredskap og arbeidsmiljø i norsk petroleumsvirksomhet. Petroleumstilsynets myndighetsansvar omfatter petroleumsvirksomheten på den norske kontinentalsokkelen, i tillegg til petroleumsanlegg og tilhørende rørledningssystem på Melkøya, Tjeldbergodden, Nyhamna, Kollsnes, Mongstad, Sture, Kårstø og Slagentangen. Petroleumstilsynet skal også være tilsynsmyndighet for de planlagte gasskraftverkene i Hammerfest, Skogn og Grenland, med tilknyttede rørledninger, og det planlagte reservegasskraftverket i Nyhamna. Petroleumstilsynet er underlagt ASD og har et spesielt samordningsansvar med andre etater som har ansvar på norsk sokkel. Petroleumstilsynet har myndighet til å fastsette utdypende forskrifter for sikkerhet og arbeidsmiljø i virksomheten, og til å fatte enkeltvedtak i form av samtykker, pålegg, tvangsmulkt, stansing av virksomhet, forbud og unntak.

5.1.5 Norsk olje og gass

Norsk olje og gass (NOROG) er en interesse- og arbeidsgiverorganisasjon under Næringslivets Hovedorganisasjon for oljeselskaper og leverandørbedrifter knyttet til utforsking og produksjon av olje og gass på norsk kontinentalsokkel. NOROG har et tett samarbeid med aktuelle myndigheter.

5.1.6 Gassco AS

Gassco AS er et statlig selskap med operatøransvaret for transport av gass fra den norske kontinentalsokkelen. Gassco er operatør for Gassled og den formelle eieren av infrastrukturen forbundet med gasstransporten fra norsk sokkel. Transportsystemet er omfattende og består av flere plattformer og tusenvis av kilometer med rørledninger.

5.2 Lover, regler og styrende dokumenter

Lov om petroleumsvirksomhet (petroleumsloven[25]) regulerer petroleumsvirksomhet på norsk kontinentalsokkel, herunder leting etter petroleum, utbygging av petroleumsfelt, produksjon av petroleum og avslutning av petroleumsvirksomhet. I 2013 ble ansvaret for å ivareta petroleumslovens § 9-3 Beredskap mot bevisste anslag, overført fra OED til ASD. Paragrafen lyder i sin helhet:

> Rettighetshaver 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 som nevnt i første og annet ledd.

Det er utarbeidet flere forskrifter med hjemmel i petroleumsloven, men ingen av disse stiller spesifikke krav til beredskap mot bevisste anslag. Forskriftene fokuserer derimot på helse, miljø og sikkerhet (HMS) med et funksjonsbasert regelverk som i stor grad er basert på bransjens egenutviklede standarder som er funnet akseptable av Petroleumstilsynet. Petroleumstilsynet opplyser at de er i ferd med å tydeliggjøre regelverket knyttet opp mot § 9.3, basert på erfaringer fra tilsyn.

I tildelingsbrevet fra ASD for 2016 beskrives samfunnssikkerhet og beredskap på følgende måte:

[25] Lov om petroleumsvirksomhet (petroleumsloven), LOV-1996-11-29-72

> Petroleumstilsynet har innenfor eget myndighetsområde ansvar for å følge opp og ivareta samfunnssikkerhet og beredskap. Petroleumstilsynet skal med utgangspunkt i en risikobasert tilnærming sørge for oversikt over risiko, sårbarhet og beredskap i sektoren og for egen virksomhet. Oppfølging av samfunnssikkerhet og beredskap skal skje på en systematisk, dokumenterbar og målrettet måte. Det skal regelmessig gjennomføres øvelser. Øvelser og hendelser skal evalueres.
>
> I årsrapporten skal det gis en kortfattet beskrivelse av risikoutvikling og oversikt over gjennomførte øvelser.

I Årsrapport 2014 fra Petroleumstilsynet gis en grundig gjennomgang av virksomheten, innledet med et sitat av tilsynets direktør:

> «HMS arbeid er ferskvare. Det hjelper ikke å være verdensmester i dag hvis det skjer en storulykke i morgen. Petroleumsvirksomheten er kommet dit den er i dag, fordi det gjennom årene er utviklet tydelige regelverkskrav, fordi selskapene tar ansvar og etterlever disse, og fordi myndighetene følger dette opp i nær dialog med næringen. Jeg er bekymret for at den store oppmerksomheten omkring kostnader og kostnadskutt vi nå opplever i næringen, kan undergrave sentrale forutsetninger i det norske sikkerhetsregelverket. Forventningene fra Petroleumstilsynet skal være tydelige, det er null aksept for svekket sikkerhet. Vi forventer at næringen håndterer de økonomiske utfordringene og samtidig forbedrer sikkerheten.»

Så vel dette sitatet som resten av årsrapporten er tungt konsentrert om sektorens viktige HMS-arbeid. Langt ut i rapporten (side 25) finner vi følgende tekst relatert til bevisste anslag:

> Etter at Petroleumstilsynet i 2013 ble delegert myndighet etter petroleumslovens § 9-3 har vi identifisert flere områder hvor det er nødvendig med en gjennomgang for å vurdere hvordan de ansvarlige selskapenes oppfølging av sitt ansvar i hht § 9. 3 innvirker på oppfølgingen av beredskap forøvrig. Dette gjelder både hvorvidt det underliggende regelverket i dag i tilstrekkelig grad dekker ansvaret gitt i § 9-3, og hvorvidt tilsynsmyndigheten må utvikle nye strategier for å følge opp sikringsforhold hos aktørene.

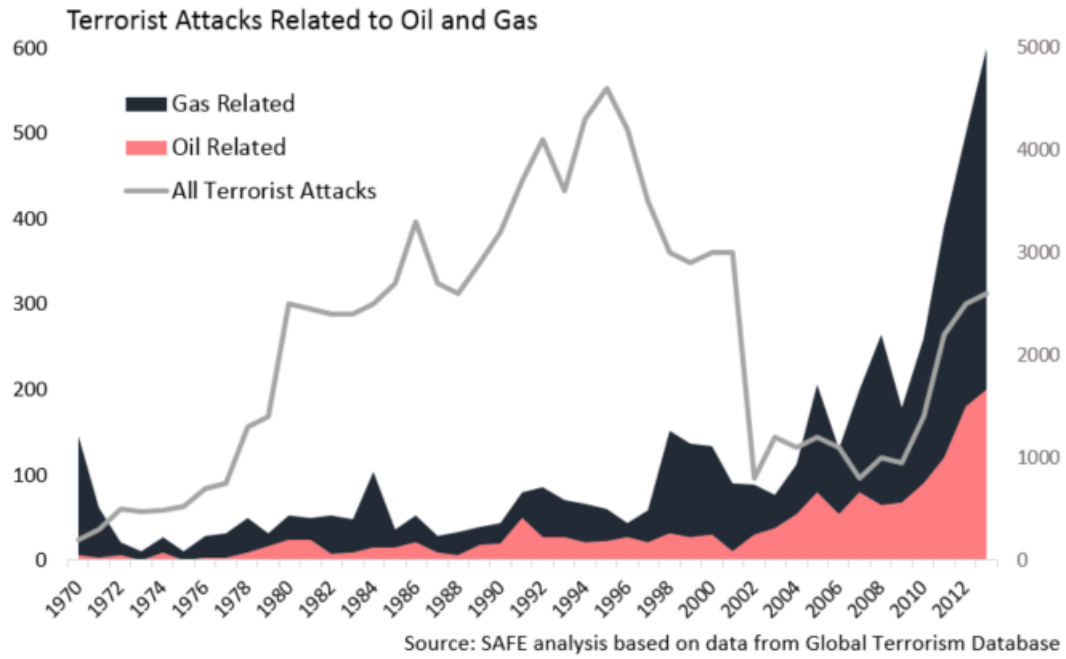
Dette er en interessant problemstilling som går til kjernen av sikkerhetslovens funksjon. For øvrig inneholder ikke årsrapporten noen referanse til mulige bevisste anslag mot bransjen.

Offentlige tilsynsrapporter fra Petroleumstilsynet er tilgjengelige på internett. Et tilfeldig utvalg av disse fokuserer ikke på bevisste handlinger. Flere forhold som blir vurdert, har selvfølgelig relevans for effektiv håndtering av anslag, men blir ikke helhetlig vurdert innenfor rammene av tilsiktede hendelser. Rapportene fokuserer på HMS og sikkerhet i arbeidet. På forespørsel har vi fått tilsendt to tilsynsrapporter som er unntatt offentlighet, en fra 2015 og en fra 2016. Det ene tilsynet er rettet mot sikringstiltak for å hindre bevisste anslag mot selskapets informasjonssystemer og det andre mot logistikk-kjeden for et petroleumsanlegg.

Når det gjelder informasjonssystemene, ble det ikke avdekket avvik, men to forbedringspunkt ble identifisert knyttet til metodikk for risikoanalyser. Tilsynet med logistikk-kjeden avdekket imidlertid en rekke avvik som manglende barrierer, manglende kompetanse i organisasjonen, mangelfullt tilsyn med underleverandører og mangel på dokumentasjon av trening og øvelser.

5.3 Trusselvurdering

Det finnes flere ugraderte databaser på nettet som gir oversikt over terroranslag, kategorisert etter måltype. Svært mange hendelser mot olje- og gassektoren er registrert, men en stor del av dem er rettet mot lett tilgjengelige mål som bensinstasjoner og tankbiler. Dessuten reflekterer de store tallene at noen av de alvorligste konflikter foregår i områder med betydelig petroleumsvirksomhet. Hvis man ser bort fra de finere nyanser, viser figur 5.1 utviklingen i antall terrorangrep mot olje- og gassinstallasjoner i perioden 1970-2013. Trenden er klar; antall anslag øker og de utgjør en økende andel av det samlede antall terrorangrep. På bakgrunn av dette globale bildet, er det vanskelig å tegne det europeiske eller norske trusselbildet, men vi kan slå fast at alvorlige anslag mot olje- og gassinstallasjoner ikke har rammet Norge. Det er sjelden god grunn for å avskrive trusselen.



Figur 5.1: Utviklingen i antall terroranslag mot olje- og gassinstallasjoner i perioden 1979-2013 (venstre skala) opp mot totalt antall terrorangrep i perioden (høyre skala).[26]

[26] https://www.start.umd.edu/gtd/search/Results.aspx?search=oil+and+gas&sa.x=0&sa.y=0

5.3.1 In Amenas - Statoils erfaringer

Globalt er olje- og gassanlegg hyppige mål for terrororganisasjoner. Anslag mot rørledninger, tankskip, raffinerier og oljefelter gjennomføres for å skape frykt, påføre økonomiske tap, svekke regimer og presse ut utenlandske selskaper. I det siste tiåret har det vært flere angrep, først og fremst i Midtøsten, Afrika og Latin-Amerika. Angrepene får sjelden mye oppmerksomhet i vår del av verden og har blitt sett på som en del av «bransjens risiko». Da Statoil engasjerte seg i In Amenas i 2003, var de selvfølgelig kjent med den generelle trusselen og at In Amenas ligger i et politisk ustabilt område. Viktige elementer i trusselbildet i 2013 var sammenbrudd av sentralmyndigheten i nabolandet Libya, uroligheter i nordre Mali og terrorangrep i det sørlige Algerie.

Det Statoiloppnevnte utvalgets rapport «The In Amenas attack»[27], har sammenfattet sin undersøkelse i noen hovedkonklusjoner og utarbeidet en liste med anbefalinger. Dette gjelder både håndteringen av selve hendelsen og Statoils mer generelle organisering av arbeidet med security. I denne sammenheng er konklusjonene og anbefalingene knyttet til securityarbeid mer relevante enn for forløpet av selve hendelsen. Vi har gjort et utdrag av rapportens konklusjoner og anbefalinger som er spesielt relevante for denne studien:

- Statoil has an established security risk management system, but the company`s overall capabilities and culture must be strengthened to respond to the security risks associated with the operations in volatile and complex environments.
- Improve the joint venture`s ability to deter, detect, delay, and stop potential attacks by reinforcing electronic and physical protective measures, enhancing its security management capability and developing a coherent of security training and exercising.
- Strengthen the joint venture`s overall security capability by appointing a joint venture head of security, and establishing a dedicated security committee.
- Seek to establish mutually effective ways of coordinating, planning and exercising between the joint venture and the military.
- Develop a clearly defined ambition for the company`s security capability
- Strengthen security leadership
- Reinforce the total security organization.
- Ensure a holistic approach to security.
- Provide security training to all employees and managers.

[27] http://www.statoil.com/no/NewsAndMedia/News/2013/Downloads/Rapport%20om%20angrepet%20mot%20In%20Amenas.pdf

- Openly and clearly communicate security risks to employees.
- Develop a security risk management system that is dynamic, fit-for-purpose and geared towards action
- Systematically develop and maintain security risk management plans.
- Build effective relationships with host nations to support mutual understanding, joint planning and exercising.
- Coordinate and standardize emergency response planning.
- Increase the frequency of security-related exercises.
- Embed the best practice demonstrated in the next-of-kin arrangements
- Review and assure existing joint venture emergency response plans
- Broaden and deepen cooperation with relevant government agencies and organizations
- Reinforce networks and institutional relationships
- Establish standards for security management and engagement in joint ventures and partnerships

Dette er en lang rekke med gode råd, slik man må forvente ved evaluering av en alvorlig terrorhendelse med mange drepte. Enkelte av utvalgets konklusjoner kan sikkert utfordres, men helheten gir klar melding om at noe må gjøres med organiseringen av securityarbeidet. I samtaler med myndighetspersoner og representanter for bransjen formidles et sterkt inntrykk av at Statoil arbeider seriøst for å etterkomme de gitte anbefalinger.

Det er viktig å merke seg formuleringen: "Statoil should have as high ambitions for its capability in the security area as it has in the domain of safety". Katastrofen skjedde i Algerie og ikke i Norge. Allikevel er det relevant å vurdere utvalgets funn opp mot norsk lovgivning. Vi har påpekt at Petroleumslovens krav til Security er begrenset til § 9.3.

5.4 Kontraterror på sokkelen

Forsvarets spesialkommando (FSK) ble opprettet i 1982 for bl a å kunne bistå politiet i å håndtere terroranslag mot installasjoner på kontinentalsokkelen. Maritime kontraterroroperasjoner kan kreve betydelige ressurser som politiet ikke disponerer. Politimesteren som mottar bistand fra FSK, har den overordnede ledelse av operasjonen, og

definerer behovet for militær støtte innenfor rammen av politiets overordnede plan. Politiets støtte fra Forsvaret er regulert gjennom Instruks om bistand til politiet (bistandsinstruksen[28]).

Nærmere bestemmelser om ansvar og ledelse er utdypet i blant annet Forsvarssjefens direktiv om innsetting av FSK i støtte til politiet i kontraterroraksjoner. Den praktiske saksgang ved innsetting av FSK reguleres av bistandsinstruksen gjennom prosedyrene for håndhevelsesbistand. Ansvarlig politimester retter sin bistandsanmodning til Justis- og beredskapsdepartementet via Politidirektoratet. Justisdepartementet vurderer anmodningen i samråd med Politidirektoratet, og ber deretter eventuelt Forsvarsdepartementet om bistand. Forsvarsdepartementet meddeler Justisdepartementet sin beslutning, og gir samtidig nødvendige retningslinjer. Forsvaret kan i denne sammenheng fremsette vilkår for å yte bistand, for eksempel i forbindelse med sikkerhetsmessige eller andre operative forhold.

God krisehåndtering på kontinentalsokkelen krever øvelser som gir mulighet for å trene prosedyrer og samarbeid, samt skape forståelse for hvordan operasjonen kan utvikle seg og hva som vil kreves av utsyr og kompetanse. I den sammenheng påhviler det også operatørselskapene et stort ansvar. Under den årlige øvelsen Gemini samarbeider Forsvaret, politiet, PST, Petroleumstilsynet og operatørselskaper. Det primære målet er å trene/øve det taktiske nivået, med hovedfokus på Beredskapstroppen (BT) og FSK.

Geminiøvelsen har vært avholdt hvert år siden 80-tallet. Den er ressurskrevende. Forsvaret kan sette inn transportfly, kampfly, undervannsbåter, fregatter, kystvaktfartøyer og helikoptre, samt lettere materiell. Det betyr at samfunnet benytter store ressurser på å trene kontraterroroperasjoner på kontinentalsokkelen. Utbyttet av øvelsen rapporteres å være generelt godt, men ved enkelte anledninger har øvingsmomenter falt ut fordi Forsvaret ikke har sett seg i stand til å mønstre planlagte ressurser.

Alle deltagerne evaluerer øvelsen. Politihøgskolen utarbeider både en gradert og en ugradert evaluering av justissektorens innsats. Forsvarets operative hovedkvarter (FOH) utarbeider en gradert rapport. I tillegg skriver Petroleumstilsynet og bransjen sine rapporter. Rapportene påpeker styrker og svakheter og gir råd om forbedringer. Behov for klarere øvingsmål er en gjenganger. Det er liten tvil om at Gemini og andre øvelser bidrar sterk til å heve kontraterrorevnen både på kontinentalsokkelen og mer generelt. Deltagerne tar med seg sine erfaringer og innarbeider dem i egen beredskap, men det er ingen som systematisk utnytter erfaringene fra øvelsen til å skape en koordinert nasjonal beredskap, med forventninger til Forsvaret, politiet og operatørselskapene. Forsvaret og politiet ville på et slikt grunnlag kunne iverksette forbedringer i samsvar med ansvarsprinsippet og næringen ville kunne pålegges krav som kunne følges opp ved tilsyn.

[28] https://lovdata.no/dokument/INS/forskrift/2012-06-22-581

5.5 Kontraterror ved landanlegg

Det finnes en rekke landanlegg som er tilknyttet felt og rørledninger på norsk sokkel. Disse dekker behov for transport, lagring og behandling av olje og gass. Gassen som leveres videre til kontinentet og Storbritannia blir tørket og komprimert ved landanleggene. Det betyr at angrep mot landanleggene også kan få store konsekvenser og føre til stans i leveransene av gass.

Ved angrep vil politiet rykke ut, men enkelte av landanleggene er lokalisert slik at det vil ta lang tid å nå fram med relevante styrker. Vi har ikke studert hvordan en eventuelt angrep vil arte seg og hvor raskt politiet må kunne mønstre en relevant kapasitet for å kunne avverge angrep eller redusere konsekvensene, men finner en betydelig ubalanse mellom de ressurser som er allokert for å beskytte landanleggene og de sivile og militære ressurser som øves årlig for å kunne settes inn på sokkelen. Det er vanskelig å forstå at dette kan forsvares med store forskjeller i trussel- og konsekvensbildet. Det ansees enklere å komme til et landanlegg enn en plattform, og definitivt enklere å unnslippe etter et angrep. Dessuten står den norske beredskapen i skarp kontrast til den høye antiterrorberedskapen på mottaksanleggene. Dette er påpekt fra flere uten at det har vært mulig å få tilgang til begrunnelsen for en slik forskjell i beredskapsnivå.

5.6 Mulige hendelser

Arbeid med forebyggende sikkerhet må ta utgangspunkt i hva som kan ramme. Dette konkretiseres gjerne i scenarier som utprøves i spill og øvelser. Terrorister og andre potensielle aktører viser stor oppfinnsomhet både når det gjelder angrepsmåte og virkemidler. Det forebyggende sikkerhetsarbeidet må derfor fange opp et spekter av mulige hendelser.

5.6.1 Fysiske angrep

Innenfor oppdragets rammer har det ikke vært mulig å utføre en grundig analyse av ulike anslag som kan ramme landanleggene eller installasjoner på norsk sokkel.

Basert på tilgjengelig ugradert informasjon og samtaler med utvalgte personer, kan det allikevel gjøres noen betraktninger. Angrep på installasjoner på norsk sokkel vil kunne føre til betydelige skader på infrastrukturen og det kan bli tatt gisler. Hvis situasjonen skulle komme ut av kontroll, vil mange liv kunne gå tapt. Opplysninger under intervjuer tilsier at en godt planlagt aksjon vil kunne påføre store skader med langvarig produksjonsstans som konsekvens. Vi er kjent med at flere sentrale aktører arbeider med etablering av redundans i viktige funksjoner og raskere tilgang på kritiske reservedeler, slik at tiden for produksjonsstans kan reduseres til et minimum. Det ligger imidlertid fast at et anslag vil kunne få store konsekvenser i form av materielle skader, miljøforurensning og tap av liv.

Situasjonen er en annen for landanleggene. De faller utenfor offshoreberedskapen som trekker på store ressurser og øves årlig. Den initielle terrorberedskapen ivaretas av bedriftene selv, med bruk av innleide vaktmannskaper med begrensede fullmakter. Ved terroranslag vil politiet bli

varslet og respondere med lokalt tilgjengelige ressurser, før eventuelt beredskapstroppen innkalles og det anmodes om bistand fra Forsvaret. Dette kan være tilstrekkelig for håndtering av forvirrede personer, men et godt planlagt angrep vil være gjennomført før ordensmakten har rukket å mobilisere tilstrekkelige styrker. Forskjellen mellom terrorberedskapen ved norske og britiske landanlegg er påtagelig. Britisk politi står i konstant høy beredskap for å sikre terminalene for mottak av gass.

5.6.2 IKT-angrep

Olje- og gassvirksomheten opplever stadig angrep av ulik alvorlighetsgrad mot IKT-systemene sine. Dette opptar bransjen og både Petroleumstilsynet og Norsk olje og gass har tatt initiativ til aktiviteter for å få satt arbeidet med digitale trusler på dagsorden.

Petroleumstilsynet har bedt virksomhetene vurdere sin egen IKT-sikkerhet opp mot retningslinjene til Norsk olje og gass. Den samlede konklusjon er at både landanleggene og produksjonsinnretningene har relativt gode systemer og rutiner for IKT- sikkerhet. Petroleumstilsynet påpeker at bransjens egen vurdering må utfordres.

Flere sider ved utviklingen innen bransjen kan imidlertid by på utfordringer. Krav til effektiv drift kan komme i konflikt med gode sikkerhetssystemer. Det har foregått en utstrakt automatisering. Overføring av produksjonsdata til informasjonssystemer og fjernvedlikehold gjør det praktisk umulig å holde prosesskontrollsystemene fysisk adskilt fra tradisjonelle informasjonssystemer og åpne nett. Den økende bruken av fjernoperasjon fra naboplattformer eller land kan innebære bruk av felles kommunikasjonssystemer slik at produksjonsutstyr kan være eksponert for nettverksrelaterte sårbarheter. Dersom en angriper bryter gjennom forsvarsmekanismene til kontroll- eller sikkerhetssystemet, kan vedkommende forstyrre kontrollsystemet ved å forsinke eller blokkere flyten av informasjon eller gjøre uautoriserte endringer i kontrollsystemet. Angrepene mot uransentrifugene i Iran (2010), oljerørledningen i Tyrkia (2008) og stålverket i Tyskland (2013) er eksempler på dette, men dette er svært krevende operasjoner. De krever store resurser, omfattende planlegging og kanskje også tilgang til utro tjenere.

Det er viktig å være oppmerksom på at gode overvåkingssystemer, brannmurer og antivirusprogram er nødvendige elementer i et godt sikkerhetssystem, men det er ikke tilstrekkelig. Dårlig sikkerhetskultur eller manglende personsikkerhetskontroll vil øke sårbarheten.

De store internasjonale selskapene har sine egne, ofte sterke, fagmiljøer. Rapporten fra In Amenas kan imidlertid tyde på at myndighetene bør ta et fastere grep om styringen av sikkerhetsarbeidet. Det dramatiske fallet i oljeprisen fra 120 $ til 40 $ pr fat, har ledet til krav om store kostnadskutt i bransjen. Da kan Security-løsningene komme under press. Dette er et argument for sterkere myndighetsstyring.

5.7 Skjermingsverdige objekter

OED har konkludert med at det ikke finnes skjermingsverdige objekter innenfor sektoren. Fra flere hold er det stilt spørsmål ved denne konklusjonen. I samtaler med myndighetsorganer og representanter for bransjen har det fremkommet synspunkter som er lagt til grunn for følgende drøfting.

Petroleumssektoren er en bærebjelke i norsk næringsvirksomhet og økonomi. Tilsiktede anslag kan gi store materielle skader, få alvorlige konsekvenser for miljøet, ta menneskeliv og føre til stans i produksjon og distribusjon. I sikkerhetslovens kriterier for utvelgelse av skjermingsverdige objekter skal det legges vekt på objektets «mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse». Det er åpenbart oppfylt for mange anlegg i petroleumssektoren. Videre skal det legges vekt på objektets symbolverdi. Å kunne ramme en viktig del av infrastrukturen for energiforsyningen til Europa, antas å ha en betydelig symboleffekt. Når det imidlertid gjelder betydningen for «sikkerhetspolitisk krisehåndtering og forsvar av riket» og for «kritiske funksjoner for det sivile samfunn» har petroleumsinstallasjonene liten verdi når vurderingene begrenses til Norge. En betydelig reduksjon i gassforsyningen til Europa, vil imidlertid få store konsekvenser for noen av våre nærmeste allierte og handelspartnere. I dette perspektiv, uavhengig av sikkerhetslovens bokstav, synes det underlig at tilsynsmyndighetene, med støtte fra næringen, ikke har foretatt en bred gjennomgang av ulike anslag sektoren kan bli utsatt for. Det ville også være et nødvendig grunnlag for eventuell utpeking av skjermingsverdige objekter. Dette står også i skarp kontrast til de store nasjonale ressurser som er allokert for kontraterroroperasjoner på sokkelen, og som øves årlig.

Når sikkerhetsmyndighetene mottar informasjon om spesielle trusler mot næringen, må denne formidles videre til sentrale aktører. Mangel på sikkerhetsklarering og dermed mulighet for å motta og bearbeide graderte opplysninger er da et problem. Dersom sektoren hadde meldt inn skjermingsverdige objekter eller ved enkeltvedtak lagt virksomheter inn under sikkerhetsloven, ville sikkerhetsklaring vært en rutinesak. Uansett forholdet til sikkerhetsloven, bør det legges til rette for at utvalgte personer i bransjen kan sikkerhetsklareres.

Representanter for bransjen er åpne for at utpeking av skjermingsverdige objekter kan bidra til å bedre beredskapen overfor spionasje, sabotasje og terrorisme. Det må imidlertid gjennomføres en nøktern og realistisk vurdering slik at ikke bransjen påføres unødvendige kostnader. Bransjen mener at Security-arbeidet ikke må bli isolert, men være godt integrert i den velutviklede HMS-beredskapen.

5.8 Oppsummering/Konklusjon

Utviklingen av petroleumssektoren har vært en enestående nasjonal industrisuksess. Det har dessverre skjedd ulykker underveis, men bransjen har tatt lærdom og fremstår i dag som bunnsolid innen HMS, basert på et velfungerende trekantsamarbeid mellom myndigheter,

bransje og fagforeninger. Lover, forskrifter og standarder regulerer arbeidet, men det legges i utstrakt grad til rette for at bransjen selv skal kunne utvikle og implementere nye løsninger. På denne måten har man utnyttet oljeselskapenes samlede forskning og erfaring, rundt om i verden.

Bildet er imidlertid noe annerledes når det gjelder Security som omhandles av bare en paragraf i petroleumsloven. Security-løsninger utarbeides i utstrakt grad av bransjen selv, med lite føringer fra myndighetene. Denne ubalansen mellom HMS og Security forsterkes trolig av at Petroleumstilsynet er underlagt ASD og ikke OED.

Bransjen utsettes for cyberangrep, men har ikke blitt rammet av fysisk terror på norsk område. Statoils virksomhet i In Amenas ble imidlertid utsatt for et alvorlig terroranslag i 2013 og fem ansatte mistet livet. "Statoil should have as high ambitions for its capability in the security area as it has in the domain of safety" står det i evalueringsrapporten fra Statoil. Dette er klar tale. Den påpekte ubalanse i lovverket finner man igjen i Statoils organisasjon. "Strengthen security leadership", "Reinforce the total security organization", "Ensure a holistic approach to security" er klare formuleringer i rapporten. Vi har hatt tilgang til bare to revisjonsrapporter som spesielt gjelder §9.3 i sikkerhetsloven. Her tegnes imidlertid et bilde som tyder på at ikke bare Statoil har «en jobb å gjøre» med sitt sikkerhetsarbeid.

Gjennom Forsvarets bistand til politiet er det avsatt store ressurser for kontraterroroperasjoner på sokkelen. De gjennomfører tre øvelser årlig, hvorav Gemini er den største og høyest profilerte. Forsvaret setter inn kapasiteter som kystvaktskip, undervannsbåter, transportfly, kampfly og helikoptre. Dette er et klart uttrykk for prioritering av oppgaven.

Landanleggene har imidlertid begrenset beredskap mot terroranslag. Ved hendelser rykker politiet ut med sine tilgjengelige ressurser, i første omgang de lokale. Vakthold ved anlegget utføres av innleide mannskaper med begrensede fullmakter. Et godt planlagt anslag vil ofte kunne gjennomføres før ordensmakten vil kunne sette inn tunge ressurser. Det eksisterer derfor en klar ubalanse mellom kontraterrorberedskapen på sokkelen og beredskapen rundt landanleggene.

Det foregår en effektivisering og automatisering i petroleumsbransjen. Flere fjernstyrte anlegg bygges, der styringen skjer fra land. Det betyr at ødeleggelse av landanlegg vil kunne føre til store skader og stansing av produksjonen i lang tid. Bransjen har nylig grepet fatt i denne problemstillingen og bygger opp lager- og logistikksystemet slik at normal drift skal kunne reetableres raskere enn i dag. Allikevel står det fast at landanlegg for de fleste aktører er lettere tilgjengelige enn offshoreinstallasjonene og det kan påføres skade som vil stanse produksjonen i lang tid.

Fysiske virkemidler som bomber og håndvåpen gir spektakulære virkninger, gisselsituasjoner påkaller verdenspressens oppmerksomhet og cyberaksjoner kan lede til dramatiske fysiske hendelser. Cyberangrep kan imidlertid også utøves mer fordekt, det kan tappes informasjon og legges inn skadevare uten at det umiddelbart oppdages. Dessuten skjer det en rask utvikling av både virkemidler og mottiltak. Noen av dem som er utsatt for en avansert cybertrussel, har

hverken midler eller faglig nettverk til å følge med i trusselutviklingen eller ressurser til å iverksette effektive mottiltak. Dette er en nasjonal rolle, i samarbeid med bransjen.

Tilsiktede handlinger mot petroleumssektoren kan ikke utelukkes. Konsekvensene for bransjen og den nasjonale økonomien kan bli store, menneskeliv kan også gå tapt. Med en viss rett kan man imidlertid hevde at konsekvensene for kritiske funksjoner for det sivile samfunn, sikkerhetspolitisk krisehåndtering og forsvar av riket vil bli begrensede. Derimot vil et vellykket anslag ha stor symbolverdi og mulighet for å utgjøre en fare for miljøet og befolkningens liv og helse. Hvis man i tillegg ser utover sikkerhetslovens gjeldende kriterier for utpeking av skjermingsverdige objekter, og inkluderer økonomisk og finansiell handlefrihet, kan det være naturlig å inkludere sentrale anlegg i sektoren.

ASD har lang erfaring og høy kompetanse innen HMS, men har betydelig svakere fundament for forvaltning av beredskap mot bevisste anslag. Petroleumstilsynet opprettet derfor i 2015 en intern prosjektgruppe for å utarbeide et faglig og strategisk grunnlag for å kunne tilpasse petroleumsregelverket til forvaltning av petroleumslovens § 9-3. Samtidig styrker Petroleumstilsynet sin egen kompetanse innenfor området.

Lovverket må tydeliggjøre krav til bransjen og dette må følges opp og kontrolleres av et tilsynsorgan som søker nærmere samarbeid med de sterkeste nasjonale kompetansemiljøene. Dette innebærer nært samarbeid med NSM om IKT-sikkerhet og etablering av en bransje-CERT som kan tilføre dette samarbeidet nødvendig bransjespesifikk innsikt. Videre bør det søkes tettere samarbeid med Forsvaret og PST for å skape en klarere forståelse av trusselen som bør konkretiseres i noen dimensjonerende scenarier som skal legges til grunn for samfunnets arbeid med forebyggende sikkerhet. I den sammenheng bør også balansen i ressursbruken vurderes.

Dersom OED, innenfor et revidert lovverk, utpeker enkelte skjermingsverdige objekter, vil sikkerhetsklareringer bli rutinemessig gjennomført og formell kontakt etablert med de nasjonale miljøer som kan gi råd til petroleumssektoren i saker som gjelder sabotasje, terrorisme, spionasje og rikets sikkerhet.

Det kan reises tvil om ASD er det riktige departementet for overordnet styring av arbeidet med beredskap mot bevisste anslag. Selv om koordinering mellom forvaltning av HMS-området og Security-området kan gi synergieffekter, kan det bli vanskelig for ASD å etablere tilstrekkelig kompetanse på et område som tidligere ikke var tillagt departementet.

6 Luftfartssektoren

6.1 Viktige aktører

6.1.1 Internasjonalt

Sikkerheten i luftfarten er avhengig av et godt internasjonalt samarbeid. Derfor er det etablert fora under FN og EU for utvikling og harmonisering av regelverk. Lover og forskrifter for sikkerheten i norsk luftfart bygger dermed i stadig større grad på EU-rettsakter. Luftfart er derfor en samfunnssektor hvor det felleseuropeiske regelverket er helt dominerende, noe som i begrenset grad åpner for særnorske bestemmelser. Dette er et viktig premiss for vurdering av hvor effektiv sikkerhetsloven er for den forebyggende sikkerhet, sammenlignet med det sektorspesifikke regelverket som i denne sammenheng stort sett er internasjonalt. Som bakgrunn for den videre lesning, gis korte presentasjoner av de styrende og premissgivende organisasjoner.

Internasjonale organer

- Den internasjonale organisasjonen for sivil luftfart (ICAO) er etablert under FN for å administrere og styre konvensjonen om internasjonal sivil luftfart (Chicago-konvensjonen). ICAO arbeider med medlemslandene og industrigrupper for å oppnå enighet om standarder og retningslinjer til støtte for trygg, effektiv, sikker, økonomisk bærekraftig og miljømessig ansvarlig internasjonal sivil luftfart. Målet er at medlemslandenes nasjonale luftfart skal bli regulert i samsvar med internasjonale normer. Innsatsen er fokusert på å utvikle og koordinere en effektiv global politikk og juridiske rammer som svar på trusselutviklingen mot sivil luftfart, gjennomføre revisjoner som identifiserer sikkerhetsmangler og bistå stater i å implementere sikkerhetsstandarder og løse problemer.

- European Civil Aviation Conference (ECAC) er etablert av FN-organet ICAO og Europarådet for å utvikle luftfarten i Europa. Landene som har medlemskap i European Aviation Safety Agency (EASA) og Eurocontrol, er også medlemmer av ECAC. Organisasjonen er rådgivende. Vedtak og anbefalinger krever godkjenning fra myndighetene i de enkelte medlemsland.

- Regulatory Committee on Civil Aviation Security (AVSEC), ligger under EU-kommisjonen og utarbeider det europeiske Securityregelverket.

- Den europeiske organisasjon for luftfartssikkerhet (Eurocontrol) er en sivil-militær internasjonal organisasjon som arbeider for å fremme sikkerheten i europeisk luftfart, koordinere lufttrafikktjenesten i Europa og utvikle et integrert europeisk system for flykontrolltjeneste.

- European Aviation Safety Agency (EASA) er EUs organ for flysikkerhet. Hovedaktivitetene er strategi og sikkerhetsledelse, sertifisering av luftfartprodukter og tilsyn med godkjente organisasjoner og medlemsstatene i EU. Sammen med EU-kommisjonen utarbeider EASA det felleseuropeiske regelverk for sivil luftfart som i stor grad bygger på anbefalinger fra ICAO.

6.1.2 Nasjonale myndigheter

6.1.2.1 Justis- og beredskapsdepartementet

Kongelig resolusjon 15.6.2012: «I sivil sektor har Justis- og beredskapsdepartementet en generell samordningsrolle for samfunnssikkerhet og beredskap. Departementet skal gjennom sin samordningsrolle sikre et koordinert og helhetlig arbeid med samfunnssikkerhet og beredskap på tvers av sektorgrenser. Direktoratet for samfunnssikkerhet og beredskap understøtter Justis- og beredskapsdepartementets samordningsrolle.»

Det er spesielt viktig at arbeidet med forebyggende sikkerhet (sikkerhetsloven) koordineres med det samfunnssikkerhets- og beredskapsarbeid som bygger på denne resolusjonen.

6.1.2.2 Forsvarsdepartementet

I henhold til sikkerhetsloven har Forsvarsdepartementet det overordnede ansvar for 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. Departementets utøvende funksjoner ivaretas av Nasjonal sikkerhetsmyndighet (NSM).

6.1.2.3 Samferdselsdepartementet

Kongelig resolusjon 15.6.2012: «Det enkelte departement har ansvar for samfunnssikkerhet og beredskap innenfor egen sektor. Departementene har et ansvar for å samordne samfunnssikkerhets- og beredskapsarbeidet i egen sektor med det arbeidet som gjøres i andre departementer. Arbeidet med samfunnssikkerhet og beredskap skal være målrettet, systematisk og sporbart og være integrert i departementets planverk, styringssystemer og i styringsdialogen med underliggende virksomheter.»

Samferdselsdepartementet har det overordnede ansvaret for samfunnssikkerhet innen områdene veg, jernbane, luftfart, post, elektronisk kommunikasjon (ekom), forebyggende sjøsikkerhet, havnesikring og statlig beredskap mot akutt forurensning.

6.1.2.4 Luftfartstilsynet

Luftfartstilsynets hovedoppgave er å bidra til økt sikkerhet i all norsk sivil luftfart gjennom å integrere nasjonalt og internasjonalt regelverk, utarbeide forskrifter for norsk luftfart og føre tilsyn med at aktørene følger gjeldende lover, regler og forskrifter. Tilsynet leder

Sikkerhetsrådet for luftfarten, som er et rådgivende organ for berørte myndigheter med det formål å forebygge anslag rettet mot sikkerheten i sivil luftfart i Norge.

6.1.2.5 Sikkerhetsrådet for luftfarten

Sikkerhetsrådet for luftfarten (SFL) er et rådgivende organ for berørte myndigheter med det formål å forebygge anslag rettet mot den sivile luftfart. Luftfartstilsynet (leder), Samferdselsdepartementet, Forsvarsdepartementet, Justis- og beredskapsdepartementet, Utenriksdepartementet, Politidirektoratet, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet er medlemmer av sikkerhetsrådet. Ekspertgruppen til SFL skal blant annet formidle råd knyttet til sikring av passasjerer, bagasje, frakt, post, objekter, bygninger, samt råd knyttet til forebygging av terrorhandlinger eller annen straffbar virksomhet.

6.1.2.6 Avinor

Avinor AS er et statlig eid aksjeselskap der eierskapet forvaltes av Samferdselsdepartementet. Selskapet har ansvaret for å eie, drive og utvikle et landsomfattende nett av lufthavner for den sivile luftfarten og en samlet flysikringstjeneste for den sivile og militære luftfarten. Avinor Flysikring AS er sertifisert som tjenesteyter for leveranser av flysikringstjenester.

6.2 Gjeldende regelverk

6.2.1 Luftfartsloven

Luftfart i Norge kan bare finne sted i samsvar med lov om luftfart (luftfartsloven[29]) og forskrifter gitt med hjemmel i loven. For luftfart som omfattes av EØS-avtalens bestemmelser, går reglene om utfylling og gjennomføring av EØS-avtalen på luftfartens område i loven foran lovens øvrige bestemmelser. Dette reflekterer det brede internasjonale samarbeidet innen luftfart. Rettsakter gitt av EU utgjør en stor del av det samlede regelverk. Vi skal se nærmere på to sentrale forskrifter, en for operasjon av selve lufthavnen og en for flysikkerhetstjenesten.

6.2.2 Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten mv

Denne forskriften gjelder for all sivil luftfart på lufthavner, som nevnt i Nasjonalt sikkerhetsprogram (jf § 1)[30] og er hjemlet i luftfartsloven og regulerer sikkerhetsgodkjenning og sikkerhetstiltak, sikkerhetskontroll og adgang til sikkerhetsbegrenset område. I teksten stilles det i hovedsak funksjonelle krav, noe som følgende utdrag viser:

- **Sikkerhetsgodkjenning og sikkerhetstiltak**

Lufthavnoperatører, luftfartsselskaper, fraktleverandører og postleverandører skal i samråd med stedlig politi utarbeide og vedlikeholde beredskapsplaner, samt gjennomføre beredskapsøvelser.

[29] Lov om luftfart (luftfartsloven). LOV-1993-06-11-101
[30] http://www.luftfartstilsynet.no/aktuelt/Oppdatert_Nasjonalt_sikkerhetsprogram_for_sivil_luftfart_NASP

Beredskapsøvelse som omfatter anslag mot sikkerheten i luftfarten, skal avholdes minst annet hvert år.

Lufthavnoperatøren skal etablere et sikkerhetsutvalg ved lufthavnen. Sikkerhetsutvalget skal sørge for planlegging, samordning og evaluering av sikkerhetstiltak ved lufthavnen og delta aktivt i planlegging og gjennomføring av beredskapsøvelser.

- **Sikkerhetskontroll**

Lufthavnoperatør er ansvarlig for gjennomføring av sikkerhetskontroll og andre sikkerhetstiltak i henhold til forskriftens bestemmelser, såfremt ikke annet er bestemt i forskriften.

Sikkerhetsgodkjent fraktleverandør og kjent avsender er ansvarlig for gjennomføring av sikkerhetstiltak i tilknytning til frakt og post, såfremt ikke annet er bestemt i forskriften.

Luftfartsselskap og sikkerhetsgodkjent leverandør av forsyninger til flygningen er ansvarlig for gjennomføring av sikkerhetskontroll og andre sikkerhetstiltak i tilknytning til forsyninger til flygingen.

- **Adgang til sikkerhetsbegrenset område**

Luftfartstilsynet foretar bakgrunnssjekk og utsteder autorisasjon på grunnlag av politiattest, i samsvar med kommisjonens gjennomføringsforordning (EU) 2015/1998.

- **EU-rettsakter**

En rekke EU-rettsakter er tatt inn i forskriften. Disse stiller svært konkrete krav til sikkerhetsarbeidet i lufthavnen. Det gis bestemmelser for hvordan lufthavnen skal utformes, hvordan adgangskontroll skal organiseres, hvilke teknologier som kan benyttes ved kontroll av passasjerer og bagasje og hvilke gjenstander som kan forbys. I tillegg stilles krav til vandelskontroll og opplæring for personell og det fastsettes framgangsmåter for inspeksjoner.

Oppsummert er sikkerheten for sivil luftfart på lufthavner detaljregulert gjennom forskrift som i stor grad er basert på felleseuropeiske regler. Det er små muligheter for nasjonale særordninger, med mindre de utfyller grunnkravene stilt av EU. Slik må det være for at den europeiske luftfart skal kunne fungere effektivt og samtidig operere i et nødvendig sikkerhetsregime. Det arbeides systematisk og serøst i alle ledd for å etterleve de pålagte sikkerhetskrav.

6.3 Forskrift om felles krav for yting av flysikringstjenester

Flysikringstjenesten er regulert i bestemmelser for sivil luftfart (BSL) herunder en rekke forskrifter som spenner fra Forskrift om etablering av Det felles europeiske luftrom (BSL G 1-

1[31]) til Forskrift om avgift på flysikringstjenester (BSL G 1-10[32]). Forskrift om felles krav for yting av flysikringstjenester (BSL G 2-2[33]) retter seg mot security ved å fastsette at tjenesteytere innen flysikringstjenesten skal utarbeide et Security Management System.

Forskriften er fastsatt med hjemmel i luftfartsloven og i henhold til internasjonale konvensjoner og avtaler som forplikter Norge til å yte flysikringstjenester, styre lufttrafikkbevegelser og styre luftrommet for allmenn lufttrafikk. Forskriften bygger på tre EU-rettsakter. Den viktigste er Commision implementing regulation (EU) No 1035/2011, et svært omfattende dokument som også beskriver kravene til Security. Disse finner vi i forskriftens Annex 1,4 som i sin helhet lyder:

> Air navigation service providers shall establish a security management system to ensure:
>
> (a) the security of their facilities and personnel so as to prevent unlawful interference with the provision of air navigation services
>
> (b) the security of operational data they receive or produce or otherwise employ, so that access to it is restricted only to those authorized
>
> The security management system shall define:
>
> (a) the procedures relating to security risk assessment and mitigation, security monitoring and improvement, security reviews and lesson dissemination;
>
> (b) the means designed to detect security breaches and to alert personnel with appropriate security warnings;
>
> (c) the means of containing the effects of security breaches and to identify recovery action and mitigation procedures to prevent reoccurrence.
>
> Air navigation service providers shall ensure the security clearance of their personnel, if appropriate, and coordinate with the relevant civil and military authorities to ensure the security of their facilities, personnel and data.
>
> The safety, quality and security management systems may be designed and operated as an integrated management system.

Det betyr at den europeiske reguleringen av sikkerheten på lufthavnene er langt mer detaljert enn for flysikringstjenestene.

[31] Forskrift om etablering og gjennomføring av Det felles europeiske luftrom; FOR-2014-12-19-1846
[32] Forskrift om avgift på flysikringstjenester; FOR-2014-12-19-1846
[33] Forskrift om felles krav for yting av flysikringstjenester; FOR-2014-12-22-1902

6.4 Håndbok for Air Traffic Management (ATM) security

Som det fremgår *av Commision implementing regulation (EU) No 1035*/2011 skal tjenesteyterne innen flysikringstjenesten utarbeide et Security Management System. Dette har Avinor Flysikring AS gjort i «Håndbok for ATM security». Håndboka beskriver mål og strategi for arbeidet med ATM security, hvordan arbeidet er organisert med oppgavefordeling og ansvarslinjer, krav til sikkerhetsklarering, krav om ROS-analyser og trusselvurdering, sikkerhet for anlegg, personell og driftsdata, behandling av sikkerhetstruende handlinger og sikkerhetsbrudd.

6.5 Vurdering av lover og regler

Sivil luftfart reguleres i utstrakt grad av EU-rettsakter som er integrert i lover og forskrifter. Security knyttet til lufthavnen reguleres av Forskrift om forebyggelse av anslag mot sikkerheten i luftfarten mv. Flysikringstjenesten reguleres tilsvarende av Forskrift om felles krav for yting av flysikringstjenester.[34]

Disse to regimene er svært forskjellige. Det er gitt detaljerte bestemmelser for tiltak som skal iverksettes for å hindre terrorisme mot lufthavn eller luftfart. Organisering av tiltakene og valg av utstyr er strengt regulert. På det grunnlag er behovet for nasjonalt regelverk begrenset.

Når det imidlertid gjelder flysikringstjenesten, er kravene fra EU mer funksjonelle, sammenfattet i noen få punkter i forordning 1035/2011[35]. Her har det vært nødvendig å etablere egne retningslinjer i Håndbok for ATM Security.

Sikkerhet rundt flyplassene er regulert gjennom det felleseuropeiske regelverket. På mange områder er det strengere og mer detaljert enn sikkerhetsloven med forskrifter krever for skjermingsverdige objekter. Hensikten med sikkerhetsarbeidet er å hindre sabotasje og terrorisme mot luftfarten. For dette formål er de gjeldende bestemmelser gjennomarbeidede, funksjonelle og forankret internasjonalt. Det sektorspesifikke regelverket er relevant og tilstrekkelig.

6.6 Samferdselsdepartementets føringer til samferdselssektoren

Samferdselsdepartementet har utarbeidet «Strategi for samfunnssikkerhet i samferdselssektoren»[36] I følge denne skal virksomhetene i samferdselssektoren forebygge og være i stand til å håndtere store uønskede hendelser, utilsiktede i form av naturødeleggelser og teknisk- og menneskelig svikt, samt tilsiktede i form av kriminalitet, terror, sabotasje og spionasje. Samferdselsdepartementet forutsetter at virksomhetene i samferdselssektoren

[34] Forskrift om felles krav for yting av flysikringstjenester, FOR-2014-12-22-1902
[35] Commission implementation regulation (EU) No 1035/2011 of 17 October 2011 laying down common requirements for the provision of air navigation services and amending Regulations (EC) No 482/2008 and (EU) No 691/2010
[36] Strategi for samfunnssikkerhet i samferdselssektoren, oktober 2015, www.publikasjoner.dep.no, publikasjonskode N-0562B

oppfyller krav i relevante regelverk med betydning for samfunnssikkerheten, herunder sikkerhetsloven med forskrifter. Det betyr at strategien fanger opp hele krisespekteret.

I strategien prioriteres følgende tre områder:

- Klimatilpasning
- Informasjons- og IKT-sikkerhet
- Sikre kritiske objekter, systemer og funksjoner

Alle tre områdene faller innenfor virkeområdet for kongelig resolusjon av 15. juni 2012[37], mens de to siste også går mot sikkerhetslovens kjernefunksjon. Departementet har dermed valgt en helhetlig tilnærming til utfordringene innenfor hele krisespekteret slik det fremkommer i følgende:

- Viktige IKT-systemer og sensitiv informasjon må sikres mot både tilsiktede og utilsiktede uønskede hendelser. I dette arbeidet vil både forebyggende tiltak og mekanismer for å håndtere uønskede hendelser være viktig.
- Man skal ha oversikt over objekter, systemer og funksjoner som er kritiske for påliteligheten og sikkerheten innen eget ansvarsområde, samt objekter, systemer og funksjoner hvor villede handlinger kan volde stor skade, og dernest etablere adekvate sikringstiltak for disse.

Dette er klart i samsvar med kongelig resolusjon av 15. juni 2012 som krever at departementene skal ha oversikt over risiko og sårbarhet i egen sektor. Denne oversikten understøttes av Nasjonalt risikobilde (NRB), og av PSTs, Etterretningstjenesten (E-tjenesten) og Nasjonal sikkerhetsmyndighet (NSM) årlige trussel- og risikovurderinger. Samferdselsdepartementet bygger sitt arbeid på disse dokumentene, men ingen av scenariene i NRB er relevante for luftfarten innenfor sikkerhetslovens virkeområde.

Departementet har imidlertid under prosjektet KRISIS utviklet egne scenarier som skal legges til grunn for arbeid med samfunnssikkerhet og beredskap. På grunnlag av scenariene er det identifisert utfordringer og anbefalt tiltak. De valgte scenariene er

- Terror
- Utfall av ekom infrastruktur og tjenester
- Utfall av tjenesteyter grunnet strukturelle endringer
- Bortfall av infrastruktur grunnet klimaendringer/ekstremvær

[37] Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering; Kongelig resolusjon, 15. juni 2012, ISBN: 978-82-7768-285-3

- Pandemi

Scenario «Terror» er relevant for det forebyggende sikkerhetsarbeid som faller inn under sikkerhetsloven. Scenariet er imidlertid lite spesifikt og fanger bare opp de mer generelle utfordringer ved terrorisme. Etter gjennomgang av scenariet sammenfattes utfordringene for luftfarten i følgende punkter:

- Bortfall av ekom som følge av terroranslag, vil gi store utfordringer for krisehåndteringen

- Likhetsprinsippet vil bli utfordret ved at Luftfartstilsynet kan ta en mer operativ rolle, i den forstand at BSL Sec 1-1 §14 første ledd gir adgang for luftfartsdirektør til å innføre ytterligere sikkerhetstiltak for lufthavner og luftfartsselskap

- Luftfartsdirektøren skal, dersom det er mulig, søke råd fra Sikkerhetsrådet for luftfarten (SFL) i en situasjon som angitt i forrige kulepunkt. SFL kan sammenkalles på kort varsel. Det er imidlertid viktig at Luftfartstilsynets rolle, særlig i forhold til justissektoren, er avklart.

- Bestemmelser for sivil luftfart security (BSL Sec 1-1 §14, andre ledd) gir politiet og lufthavnoperatør anledning til å innføre ytterligere sikkerhetstiltak, dersom det ikke er tid til å legge spørsmålet frem for Luftfartstilsynet. Dette kan gi en uoversiktlig situasjon, selv om forskriften også angir at eventuelle ytterligere sikkerhetstiltak uten opphold skal rapporteres til Luftfartstilsynet.

- Det er mange aktører involvert i krisehåndteringen på en lufthavn, for eksempel politiet, luftfartsselskap, lufthavnoperatør, handlingselskap, leverandør av sikkerhetskontrolltjenester og så videre. Dette er utfordrende, selv om regelverket til en viss grad regulerer ansvarsforhold, i alle fall slik at politiet vil ha det øverste ansvaret.

- Det er noe uklart hvem som skal bestemme over transportressursene i en krisesituasjon. Samferdselsdepartementet kan, i henhold til luftfartsloven § 12-9 d, pålegge aktører innen luftfart å yte bistand i form av blant annet transporttjenester i alle ledd av transportkjeden.

Utfordringene som her beskrives, er primært rettet mot roller, ansvar og myndighet. De representerer føringer for sikkerhetsarbeidet i underliggende etater hvor problemstillingene er mer detaljerte og konkrete.

6.7 Tildelingsbrev til Luftfartstilsynet for 2016

Under overskriften Samfunnssikkerhet og beredskap [38]står følgende:

> Samfunnssikkerhet og beredskap skal inngå som en integrert del av Luftfartstilsynets virksomhet.

Det overordnede målet for arbeidet med samfunnssikkerhet og beredskap i samferdselssektoren er å unngå tilsiktede hendelser som medfører skader på personer, miljø eller materiell, og minske følgene av slike hendelser hvis de skulle oppstå, samt sikre pålitelighet og framkommelighet i transport- og kommunikasjonsnett både i normalsituasjoner og under påkjenninger.

De overordnede mål og krav for samfunnssikkerhetsarbeidet i Luftfartstilsynet er fastlagt i SDs "Strategi for samfunnssikkerhet i samferdselssektoren" fra 2015[39]. Som det er nærmere redegjort for i strategien, skal Luftfartstilsynet særskilt prioritere følgende tre områder:

- Klimatilpasning
- Informasjons- og IKT-sikkerhet
- Sikring av kritiske objekter, systemer og funksjoner

Luftfartstilsynet bes, i tillegg til kravene omtalt i kapittel 3 (Mål, styringsparametere og oppdrag for 2016), også fortsette arbeidet med å styrke robustheten i de kritiske objektene innenfor eget ansvarsområde, som er identifisert i samferdselsdepartementets prosjekt for risiko og sårbarhetsanalyser (SAMROS II-prosjektet).

6.8 Risikovurdering av anslag mot sivil luftfart

Luftfartstilsynet utgir årlig risikovurdering av anslag mot sivil luftfart. Risikovurderingens hovedkonklusjoner presenteres for Sikkerhetsrådet for luftfarten. De konkrete vurderingene kan ikke gjengis her, da dokumentert er unntatt offentlighet, men metodikken kan beskrives. Dokumentet skal være retningsgivende for sikkerhetsarbeidet i sektoren. Det skal

- Gi relevante aktører eksempler på metodikk for å gjennomføre risikovurdering, samt gi disse et bedre grunnlag for egen kvalitetskontroll og øke bevisstheten knyttet til forebyggende sikkerhet.
- Bidra til å målrette Luftfartstilsynets egen inspeksjonsaktivitet
- Bidra til økt flysikkerhet

[38] Statsbudsjettet 2016 – tildelingsbrev for Luftfartstilsynet 2016, Ref 15/3472-, datert 7.1.2016
[39] Strategi for samfunnssikkerhet i samferdselssektoren, oktober 2015, publikasjonskode N-0562 B

- Bidra til å oppfylle krav til risikovurdering som stilles i Samferdselsdepartementets «Strategi for samfunnssikkerhet og beredskap»

Risikovurderingen er basert på gjennomgang og vurdering av til sammen 21 scenarier; angrep rettet mot luftfartøy, lufthavn og flysikringstjenesten. Trussel, sårbarhet og konsekvens blir kvantifisert, vektlagt og summert til et risikotall for scenariet. Således kan hendelsene rangeres etter estimert risiko som grunnlag for prioritering av tiltak.

Risikovurderingen er basert på informasjon om det globale risikobildet for sivil luftfart, de åpne trusselvurderingene gitt av PST og E-tjenesten, informasjon om sårbarhet innhentet gjennom egne inspeksjoner, samt faktiske anslag der Norge på en eller annen måte har vært involvert.

Metodikken for risikovurderingen er i tråd med Norsk Standard 5830:2012, hvor komponenter som trussel, sårbarhet og konsekvens/verdi utgjør risikobildet. ICAO utgir publikasjonen «Risk Context Statement (RCS)», som også vurderer risiko knyttet til ulike scenarioer. Norge deltar i dette arbeidet i ICAO Working Group on Threat and Risk (WGTR). RCS utgis i en åpent tilgjengelig versjon og en versjon som ikke er offentlig. Den åpne versjonen er tilgjengelig på nett og gjengis her som en illustrasjon (figur 6.1). Her fremgår at improvisert bombe i lasten, passasjerbåret improvisert bombe med lite metallinnhold og MANPADS (Man-portable air defense systems) vurderes som de mest alvorlige risikoscenarioene. Høy risiko fra luftforsvarsmissiler er imidlertid begrenset til områder der kamphandlinger pågår.

THREAT TYPE	Likelihood	Consequence	Vulnerabilities	RISK
AIRBORNE THREATS (conventional hijack)	Medium	Medium	Low	**LOW**
AIRBORNE THREATS (aircraft used as weapon)	Medium-Low	High	Medium-Low	**MEDIUM-LOW**
PERSON-BORNE CONVENTIONAL IMPROVISED EXPLOSIVE DEVICE (IED) (traditional IED with metallic components)	Medium	High	Medium	**MEDIUM**
PERSON-BORNE NON-CONVENTIONAL IED (low or no metal content and/or novel	High	High	Medium-High	**MEDIUM-HIGH**
OTHER WEAPON (firearms, knives or blunt instruments used to attack passengers or crew but not to	Low	Medium-Low	Low	**LOW**
MAN-PORTABLE AIR DEFENSE SYSTEMS (MANPADS) (in combat or proliferation zone)	Medium-High	High	High	**MEDIUM-HIGH**
MANPADS (not in combat or proliferation zone)	Low	High	High	**MEDIUM-LOW**
VEHICLE-BORNE IED	Medium-High	Medium	Medium-High	**MEDIUM**
CARGO IED	High	High	Medium-High	**MEDIUM-HIGH**
LANDSIDE IED (detonated outside security restricted areas)	High	Medium-Low	Medium-High	**MEDIUM**

Figur 6.1 Resultatene av ICAOs globale risikovurdering av sivil luftfart[40].

6.9 Arbeidet med forebyggende sikkerhet innen luftfarten

Samferdselssektoren driver et systematisk og godt arbeid innen samfunnssikkerhet. I departementets «Strategi for samfunnssikkerhet og beredskap» gis det klare føringer for sikkerhetsarbeidet i sektoren. Kravene er i hovedsak utledet fra Kongelig resolusjon av 15. juni 2012, men kravene knyttes også mot Sikkerhetsloven ved at aktørene skal «oppfylle kravene i sikkerhetsloven med forskrifter for å sørge for tilstrekkelig sikring av sikkerhetsgradert informasjon og informasjonssystemer» og «utpeke og sikre skjermingsverdige objekter i henhold til kravene i Objektsikkerhetsforskriften».

Videre har Samferdselsdepartementet utarbeidet relevante krise scenarier for sektoren (KRISIS) og risiko og sårbarhetsanalyser i SAMROS II. Tildelingsbrevet konkretiserer kravene fra strategien.

Scenariene i KRISIS er svært generelle og retter seg primært mot organisatoriske utfordringer ved krisehåndtering. Dette illustreres ved at utfordringene som identifiseres for luftfarten i

[40] http://www.icao.int/Meetings/avsecconf/Documents/Risk%20Context%20Statement/Risk

scenariet «Terror» først og fremst er rettet mot fortolkning av likhetsprinsippet og at det er nødvendig å avklare roller og myndighet.

Risikovurdering av anslag mot sivil luftfart bygger videre på Terror-scenariet ved å definere og analysere 21 mulige hendelser ved bruk av metodikk i tråd med Norsk Standard 5830:2012 og sterkt inspirert av arbeidet i ICAO. Trusselbildet som ligger til grunn for scenariene er svært tradisjonelt, i stor grad basert på hendelser som har funnet sted. Dette er en svakhet fordi vellykket terror ofte inneholder elementer av overraskelse. Det er derfor behov for større kreativitet ved utarbeidelse av scenarier. Scenariene fanger heller ikke opp de bredere samfunnsmessige konsekvenser av terroranslag slik ambisjonen er for de scenariene som drøftes i NRB. Det bør derfor tas initiativ til at luftfartsscenarier inkluderes i NRB.

Under sikkerhetsloven skal det drives forebyggende sikkerhetsarbeid, også med tanke på krisehåndtering og forsvar av riket. Forsvaret driver systematisk scenariobasert analysearbeid som grunnlag for utvikling av forsvarsstrukturen. Dette skal gi Forsvaret bedre innsikt i hvordan utfordringene kan utvikle seg og hvordan de best kan håndteres. Alle typer krigshandlinger vil få konsekvenser for det sivile samfunn, og Forsvaret vil i mange henseender være avhengig av bistand fra det sivile samfunn. Dette er fanget opp i totalforsvarskonseptet. Men det sivile samfunn kan ikke planlegge og øve på støtte til Forsvaret hvis det ikke vet hva som kan bli etterspurt. Relevante deler av Forsvarets planarbeid må derfor gjøres tilgjengelig for de sektorene som kan rammes hardest eller forventes å kunne støtte Forsvaret ved væpnet konflikt. Luftfartssektoren etterspør et slikt plangrunnlag.

6.10 Vurdering av flysikringstjenesten

Flysikringstjenesten er systematisk bygget opp slik at den kan mestre de fleste hendelser med innarbeidede back-up løsninger. Derfor oppfattes tjenesten som relativt robust overfor mulige hendelser som skyldes tekniske eller menneskelige feil.

I tillegg til Risikovurdering av anslag mot sivil luftfart, utarbeider Luftfartstilsynet Risikovurdering av anslag mot kritiske datasystemer i luftfarten, basert på arbeid under ICAOs Threat and Risk Working Group. Det er svært positivt at Luftfartstilsynet har startet dette arbeidet og at sektoren har styrket sin kompetanse innen IKT-sikkerhet. Trusselbildet innen IKT-sikkerhet er imidlertid så komplekst og under så rask utvikling at det hverken er mulig eller klokt at nødvendig kompetanse og kapasitet utvikles sektorvis. NSM fremstår som landets fremste ressurs innen området og må samarbeide tett med sektorens egne ressurser for å kunne bygge opp tilstrekkelig evne til å forhindre eller redusere skadene av IKT-angrep.

En rask økning av flytrafikken i Europa har imidlertid styrket behovet for sterkere integrasjon av de nasjonale flykontrolltjenester under fellesbetegnelsen *Single European Sky*. Dette arbeidet gjennomføres med hjemmel i EU-rettsakter. Grunnlaget er lagt for en rekke forbedringer i norsk og europeisk luftfart gjennom harmonisering av sikkerhetskrav og tekniske standarder. Fellesløsninger og tettere samarbeid om lufttrafikkstyring og flynavigasjon står sentralt. Dette arbeidet vil lede til utfordringer, spesielt innen IKT-security. For å sikre god nasjonal

implementering av løsningene, må arbeidet støttes av et sterkt fagmiljø. Et nært samarbeid med NSM er nødvendig. Samarbeidet om skjermingsverdige objekter sikrer at sentrale medarbeidere underlegges nødvendig sikkerhetsklarering.

6.11 Vurdering av lufthavnsikringen

Sikkerheten rundt lufthavner er detaljregulert av internasjonalt regelverk. Behovet for ytterligere nasjonale tiltak er derfor svært begrenset med unntak av regimet for sikkerhetsgodkjenning av personell. Normalt kreves det bare politiattest, men for sentrale funksjoner bør det stilles krav til sikkerhetsklarering og autorisasjon.

For å styrke arbeidet med forbyggende sikkerhet bør Forsvaret og politiet bidra mer aktivt for å skape bedre forståelse for trusselutviklingen, i tillegg til den informasjon som mottas fra utenlandske partnere. Dette er spesielt viktig fordi slike vurderinger ofte vil være graderte for å unngå at mulige terrorister får ideer og at sårbarheter avsløres.

6.12 Konklusjon

Samferdselssektoren arbeider systematisk og godt med samfunnssikkerhet og beredskap, både det som reguleres av Kongelig resolusjon av 15. juni 2012 og av sikkerhetsloven med forskrifter. I departementets strategiske arbeid er de to regimene godt koordinert. Selv om den utløsende årsak kan være forskjellig (naturkatastrofe, ulykke eller tilsiktede handling), vil håndteringen under de to regimene ha mye til felles. Sektoren har behov for innsyn i relevante deler av Forsvarets planverk og nærmere samarbeid med politiet om terrorhandlinger. Samarbeidet med NSM om IKT-sårbarhet i flysikringstjenesten fungerer godt og bør styrkes. Tilsyn fra NSM oppleves generelt som konstruktivt, men det etterlyses mer rådgivning.

7 Konklusjoner og anbefalinger

Basert på samtaler med utvalgte enheter i sektorene, herunder tilsynsmyndighetene, møter med NSM og NorCERT, samt gjennomgang av relevante lover, forskrifter, veiledere og utredninger, sammenfattes våre funn i noen konklusjoner og anbefalinger. Det gjøres først en samlet vurdering knyttet til oppdragets hovedpunkter. Deretter utdypes dette i noen konkrete anbefalinger.

7.1 Samlet vurdering

De tre studerte sektorene kraft, petroleum og luftfart er svært forskjellige, og har ulike sektorregelverk. Med dette som utgangspunkt er det foretatt en samlet vurdering knyttet til oppdragets overordnede punkter. Disse er;

- hvorvidt sektorregelverket er tilstrekkelig for god sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner,
- om en overordnet lovregulering kan bidra til bedre forebyggende sikkerhet for ivaretakelse av kritiske samfunnsfunksjoner,
- hvilke forhold som eventuelt bør reguleres i et overordnet regelverk (lov og/eller forskrift).

For å sikre en samlet nasjonal håndtering av kriser og forsvar av riket, optimal bruk av ressurser på tvers av sektorene, samt utvikling av en nasjonal sikkerhetskultur, er det behov for et nasjonalt tverrsektorielt regelverk, enten regulert i tverrsektorielle lover/forskrifter, eller gjennom likelydende formuleringer i sektorlover/forskrifter. Konkret gjelder dette;

- etablering av nasjonale tverrsektorielle scenarioklasser som er tverrsektorielt forankret,
- tverrsektoriell håndtering av personklarering,
- tverrsektorielle ordninger innen IKT-sikkerhet. Det bør blant annet gis mulighet for å pålegge deltagelse i NorCERTs VDI-system.
- valg av skjermingsverdige objekter. Lov og forskrift bør kreve at utvelgelse gjøres på grunnlag av nasjonale scenarioer, kritisk infrastruktur og inkludere begrepet «skjermingsverdige systemer».

I lys av de tverrsektorielle behov som er nevnt ovenfor, er det vurdert om dagens sektorregelverk i de tre studerte sektorene, er tilstrekkelig for god sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner.

Kraftsektoren: Dagens sektorregelverk er i stor grad dekkende for forebyggende sikkerhet. Regelverket sikrer god håndtering av sektorens leveringssikkerhet. På noen områder er beredskapsforskriften og veilederen til forskriften for detaljert, noe som medfører at bransjen i begrenset grad inviteres til å finne gode løsninger. Regelverket regulerer tydelige ansvars- og myndighetsroller i beredskapsorganisasjonen. Dette er viktig og må beholdes.

Petroleumssektoren: Petroleumssektorens regelverk bør forbedres innen forebyggende sikkerhet mot tilsiktede handlinger. Det er behov for klarere ansvars- og myndighetsregulering i en nasjonal beredskapsorganisasjon. Det er positivt at sektoren utnytter bransjekunnskap ved ikke å detaljregulere løsninger.

Luftfartssektoren: Innen Luftfartssektoren er dagens regelverk styrt av internasjonale rettsakter, utfylt med nasjonale bestemmelser. Dette gjelder spesielt sikkerheten rundt lufthavner. Det internasjonale regelverket for flysikringstjenester er mindre detaljert og krever mer nasjonalt regelverk.

7.2 Nasjonale scenarioer

Hverken sikkerhetsloven, objektsikkerhetsforskriften eller veilederen til denne definerer hvilke situasjoner, eller scenarioer, som skal legges til grunn for utvelgelsen av skjermingsverdige objekter. Dette til tross for at objektsikkerhetsforskriftens formål er «å gi en helhetlig og overordnet tilnærming på tvers av samfunnssektorene når det gjelder utvelgelse, beskyttelse og tilsyn med skjermingsverdige objekter».

Utpeking av skjermingsverdige objekter skal starte med en verdivurdering. En virksomhet plikter å ha oversikt over sine verdier, og skal i henhold til loven avdekke objektets viktighet av hensyn til rikets sikkerhet og vitale sikkerhetsinteresser. Lovens kriterier for valg av skjermingsverdige objekter er;

- betydning for sikkerhetspolitisk krisehåndtering og forsvar av riket
- betydning for kritiske funksjoner for det sivile samfunn,
- symbolverdi, og
- mulighet for å utgjøre en fare for miljøet eller befolkningens liv og helse

Disse kriteriene er overordnede og gir begrenset grunnlag for utpeking av skjermingsverdige objekter. Det sentrale spørsmål er hva en sikkerhetspolitisk krise og forsvar av riket innebærer.

Direktoratet for samfunnssikkerhet og beredskap (DSB) utarbeider nasjonalt risikobilde[41], og inkluderer tilsiktede handlinger, herunder terrorisme og strategisk overfall. I Forsvarets planlegging legges planscenarioer til grunn for langtidsplanlegging, og for utvikling av doktriner, anskaffelser av utstyr, utdanning og trening av personell, samt organisering av den operative virksomheten. Det bør vurderes etablering av nasjonale tverrsektorielle scenarioer, eller situasjonsbeskrivelser, som startpunkt for utvelgelse av kritisk infrastruktur og dermed skjermingsverdige systemer og objekter. Slike scenarioer bør etableres i et samarbeid mellom Justis- og beredskapsdepartementet og Forsvarsdepartementet, og i nær kontakt med øvrige departementer. Scenarioene bør vedtas i regjeringen og gjøres gjeldende for alle sektorer.

De tverrsektorielle scenarioene bør organiseres i overordnede scenarioklasser for de situasjoner Norge som samfunn skal håndtere, samt en vurdering av til hvilket nivå samfunnsfunksjoner skal opprettholdes innen de ulike scenarioklassene. For å lette konkretiseringen av scenarioklassene bør det utvikles en oversikt over konkrete hendelser innen hver

[41] Nasjonalt risikobilde 2014 – Katastrofer som kan ramme det norske samfunnet. ISBN 978-82-7768-352-2

samfunnsfunksjon. Disse bør legges til grunn for verdivurdering, ROS-analyser, forebyggende tiltak og beredskapsøvelser.

I forsvarssektoren har departementet i hele etterkrigstiden benyttet forskningsbasert rådgivning ved etablering av planleggingsscenarioer og langtidsplaner. I tillegg har anvendt FoU (Forskning og Utvikling) stått sentralt ved utvikling av tiltak for å møte Forsvarets utfordringer. Øvrige sektorer bør vurdere en tilsvarende forsknings- og utviklingsbasert tilnærming for etablering av nasjonale scenarioklasser for forebyggende sikkerhet overfor tilsiktede hendelser.

Hovedanbefaling nr 1: Det bør etableres nasjonale tverrsektorielle scenarioer som dekker hele krisespekteret. Disse bør etableres ved et samarbeid mellom Justis- og beredskapsdepartementet og Forsvarsdepartementet i nær kontakt med øvrige departementer, vedtas i regjeringen og gjøres gjeldende for alle sektorer. De nasjonale scenarioene bør organiseres i overordnede scenarioklasser og legges til grunn for etablering av verdivurdering, ROS-analyser, forebyggende tiltak, samt beredskapsøvelser.

7.3 Forsvarets behov ved sikkerhetspolitiske hendelser og krig

I flere intervjuer er det etterlyst informasjon fra Forsvaret om hvilke behov for støtte som gjelder i sikkerhetspolitisk krise og ved forsvar av riket.

Forsvaret har gjennom rekvisisjonsloven[42] hjemmel til, når riket er i krig, å rekvirere «alt som er nødvendig for krigsmakten og institusjoner som er knyttet til den». Dette gjelder varer og annet løsøre, fartøyer, fly, husrom, bygninger og faste anlegg. Det spesifiseres disposisjonsrett over alle slags transport- og sambandsmidler med eller uten personale og materiell, samt disposisjonsrett over fabrikker, verksteder, lys-, gass- og kraftverk og andre bedrifter med eller uten arbeidsstokk, materiell og lager. Kort sagt kan Forsvaret i krig disponere nasjonens samlede ressurser.

Effektiv bruk av sivile ressurser ved håndtering av sikkerhetspolitisk krise og forsvar av riket krever forberedelser, trening og øving. For å kunne gi effektive bidrag krever dette at Forsvaret informerer øvrige sektorer om sitt støttebehov. Forsvar av riket vil inkludere scenarioer hvor sivilsamfunnet i stor grad må opprettholde normale funksjoner for å understøtte befolkningens basisbehov. Dette må innarbeides i planverket og tilrettelegges for i det forebyggende sikkerhetsarbeidet, noe som betyr at Forsvaret må informere øvrige sektorer om det gjeldende og langsiktige trusselbildet, samt egne planer for forsvar av riket. Sektorene bør pålegges å etablere de systemer og rutiner som kreves for å kunne motta og håndtere gradert informasjon.

[42] Lov om militære rekvisisjoner, ISBN 82-504-1090-4

Hovedanbefaling nr 2: Forsvaret bør pålegges å formidle et tilstrekkelig trusselbilde samt sine operative og planlagte behov for sivil støtte i sikkerhetspolitisk krise og i krig til sektorer med ansvar for kritiske samfunnsfunksjoner. Sektorene bør pålegges å etablere de systemer og rutiner som kreves for å kunne motta og håndtere slik informasjon.

7.4 Sikkerhetslovens kriterier for utvelgelse av skjermingsverdige objekter

Sikkerhetslovens § 17 omhandler utvelgelse av skjermingsverdige objekter. Det er objekteiernes plikt å foreslå skjermingsverdige objekter for ansvarlig departement.

Objektsikkerhetsforskriften presiserer (§ 2-1) at «utvelgelsen skal ikke skje i større utstrekning enn nødvendig». Veilederen til forskriften gir i vedlegg B en stegvis prosess for skadevurderingen og hvor det er utarbeidet et prosessdiagram for valg av skjermingsverdig objekt (veilederens figur B1 «Skadevurderingsprosess og tilhørende elementer). Prosessdiagrammet lister fire kritiske områder for effektiv krisehåndtering. Disse er:

- Opprettholde territoriell integritet
- Opprettholde nasjonal handlefrihet
- Opprettholde økonomisk og finansiell handlefrihet
- Opprettholde juridisk handlefrihet

Det bør vurderes om disse kriteriene skal spesifiseres i lov og forskrift. Særlig bør lovens § 17 utvides og ta inn betydning av økonomisk og finansiell handlefrihet, noe som også er omtalt i NOU 2003:18 «Rikets sikkerhet»[43]

Hovedanbefaling nr 3: Sikkerhetsloven og objektsikringsforskriften bør inkludere «økonomisk og finansiell handlefrihet" ved omtale av hvilke overordnede kriterier som særlig skal tas hensyn til i en skadevurdering ved utvelgelse av skjermingsverdige objekter og systemer.

7.5 Personsikkerhet

Sektorene har i betydelig grad behov for å håndtere sensitiv informasjon, og driver kritiske drifts- og kontrollsystemer, samt anlegg med stor betydning for nasjonalt kritiske

[43] NOU:2003:18 «Rikets sikkerhet», Straffelovkommisjonens delutredning VIII, 30. juni 2003

samfunnsfunksjoner. Cyberangrep i andre land viser at utro tjenere på innsiden av barrierer representerer en stor trussel. Det er derfor ikke nok å sikre datasystemene mot eksterne cyberangrep, men også behov for god kontroll med personell som fysisk eller elektronisk har tilgang til informasjons-, drifts- og kontrollsystemer.

I dag gjennomføres personklarering normalt av sektormyndighetene opp til og med HEMMELIG, og av NSM for klarering av personell med behov for høyere klarering. NSM fører tilsyn med klareringsrutiner for personell med tilgang til skjermingsverdige objekter og med behov for sikkerhetsgradert informasjon. Personell som skal ha tilgang til et skjermingsverdig objekt, klareres i henhold til objektets klasse. Sektorenes tilsynsmyndigheter gjennomfører bakgrunnssjekk og innhenter vandelsattest fra politiet for personell som skal ha tilgang til viktige anlegg.

Utro tjenere på innsiden av barrierer kan påføre anlegget, øvrig personell og nasjonen store utfordringer ved terrorhandlinger, og andre tilsiktede handlinger, herunder bruk av eksplosiver. Samfunnskonsekvensen av en slik tilsiktet handling kan være meget stor, ikke minst økonomisk. Personell med tilgang til fysiske eller elektroniske komponenter innen kritisk infrastruktur bør derfor klareres for tilgang. Ved hendelser eller trussel om hendelser, vil den nasjonale sikkerhetsmyndighet ha behov for nært samarbeid med berørt bransje, hvilket ofte involverer graderte opplysninger. Manglende sikkerhetsklarering vil hemme eller hindre et slikt samarbeid.

Rutiner og ordninger for klarering av personell tilknyttet kritisk infrastruktur bør gjennomgås. Det er viktig å påpeke at dette ikke må påføre tilsynsmyndigheter og selskaper en uhensiktsmessig belastning. Det anbefales at et tverrsektorielt organ gjennomfører personklarering etter anmodning fra departementene, og at denne klareringen ikke bør være mer omfattende enn det den enkeltes stillingskategori krever.

Hovedanbefaling nr 4: Det bør pålegges bakgrunnssjekk av personell som er ansatt, eller har tilgang til objekter og/eller systemer knyttet til kritiske samfunnsfunksjoner. Departementet ved tilsynsmyndigheten bør anmode om klarering. Klareringen bør gjennomføres etter samme kriterier for alle sektorer, og utføres av sentral klareringsmyndighet. Klarering bør skje for to hovedkategorier personell i) personell med tilgang til sikkerhetsgradert eller sensitiv informasjon (sikkerhetsklarering), og ii) personell med adgang til anleggene, men uten behov for tilgang til sensitiv informasjon (adgangsklarering).

7.6 IKT-sikkerhet

Digitaliseringen av samfunnet har åpnet for nye trusler. Det regjeringsoppnevnte utvalget for vurdering av digital sårbarhet (Lysneutvalget) leverte sin rapport[44] 30. november 2015. En av anbefalingene fra utvalget er «å styrke Justis- og beredskapsdepartementets tverrsektorielle virkemidler på IKT-sikkerhetsområdet». Begrunnelsen er særlig knyttet til at ingen sektor alene kan kontrollere sin egen digitale sårbarhet, og at verdikjedene gjør at alle arver digitale sårbarheter fra andre sektorer. En angriper vil heller ikke forholde seg til våre sektorgrenser.

Gjennomgangen av de utvalgte sektorene viser stor forskjell i håndteringen av IKT-sikkerhet. Petroleumssektoren inkluderer store internasjonale konsern med egne «CERT'er» for håndtering av IKT-sikkerhet. Disse selskapene er ofte knyttet til nasjonale ordninger i de land hvor hovedkontoret er lokalisert. I Norge er Statoil knyttet til NorCERTs VDI system. Petroleumssektoren har ikke etablert en egen «PetroleumsCERT». Det er heller ikke opprettet en egen «LuftCERT». I kraftsektoren kjøper en rekke selskaper VDI-tjenester hos NorCERT. I tillegg har NVE tatt initiativ til at bransjen har etablert KraftCERT som eies av Statnett, Statkraft og Hafslund Nett. Vi mener som Lysneutvalget, at tverrsektorielle ordninger innen IKT-sikkerhet for informasjonssystemene må styrkes. Det bør derfor vurderes etablering av bransjespesifikke CERT'er for alle sektorer hvor driftskontrollsystemer er avgjørende for sektorens virksomhet.

Hovedanbefaling nr 5: Sektordepartementene bør kunne pålegge virksomheter innen kritiske samfunnsfunksjoner tilknytning til NorCERTs nasjonale varslingssystem for digital infrastruktur (VDI). Det bør etableres bransjespesifikke CERT'er for alle sektorer hvor driftskontroll-systemer er avgjørende for sektorens virksomhet. Sektordepartementene bør gjennom tilsynsmyndigheten kunne pålegge virksomheter deltagelse i en BransjeCERT. En BransjeCERT bør pålegges samarbeid med NorCERT og organiseres og drives av bransjen.

7.7 Objektsikkerhet

Skjermingsverdige objekter defineres i sikkerhetsloven § 3, og knyttes spesifikt til eiendom «som må beskyttes mot sikkerhetstruende virksomhet av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser». Eiendom er i loven ikke begrenset til fast eiendom som bygg og anlegg, men omfatter også transportmidler, annet materiell eller deler av slikt materiell. Loven åpner dermed for en vid tolkning av begrepet skjermingsverdig objekt.

Ethvert objekt vil på en eller annen måte inngå i et system av objekter. Slike systemer kan være en del av samfunnets kritiske infrastruktur eller samfunnets kritiske funksjoner. Sikkerhetsloven

[44] Norges offentlige utredning (NOU). 2015:13 Digital sårbarhet – sikkert samfunn

og objektsikkerhetsforskriften gir ikke tydelig henvisning til kritisk infrastruktur og kritiske systemer. Derimot gir veilederen ved konkret gjennomgang av prosessen for utplukking av skjermingsverdige objekter, som omtalt i kapittel 8.3, referanser til samfunnets kritiske infrastruktur.

Sektorenes håndtering av objektsikkerhet er meget forskjellig, noe gjennomgangen av sektorregelverk og praksis viser. For å sikre rask og adekvat beredskap i sektorene er det essensielt at ansvar og myndighet er tydelig i regelverket. Dette er særlig tydelig i kraftsektorens regelverk, noe som blant annet skyldes sektorens behov for høy operativ beredskap. Det anbefales at denne operative evnen beholdes, og styrkes i de sektorer hvor den er mer utydelig.

Hovedanbefaling nr 6: Begrepet skjermingsverdige objekter bør i lov og forskrift knyttes til kritiske infrastrukturer. I tillegg til skjermingsverdig objekt bør det innføres et begrep «skjermingsverdig system». Redundans i system og balansering av beskyttelsestiltak på flere objekter uavhengig av objektklasse bør i lov og forskrift anerkjennes som tilstrekkelig beskyttelse og forvaltes av tilsynsmyndigheten. Sektorregelverket bør inkludere tydelig henvisning til ansvar og myndighet i sektorens operative beredskap.

7.8 Anskaffelser til kritiske samfunnsfunksjoner

Ved anskaffelser av tjenester og komponenter til kritisk infrastruktur åpnes skjermingsverdige systemer og objekter for mulige sårbarheter. Dagens sektorregelverk er etter vår vurdering ikke tilstrekkelig innen samfunnskritiske anskaffelser. Realiteten er at økonomiske og tekniske vurderinger i for stor grad er førende for de valg som tas. Et tverrsektorielt regelverk forankret i ny sikkerhetslov vil gi sektormyndighetene hjemmel til i større grad å pålegge virksomhetene sikkerhetsmessige vurderinger ved kritiske anskaffelser.

Hovedanbefaling nr 7: Sikkerhetslovens kapittel 7 “Sikkerhetsgraderte anskaffelser” bør oppgraderes og legges til grunn for anskaffelser knyttet til kritiske samfunnsfunksjoner i alle sektorer. Regelverket bør være tverrsektorielt.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

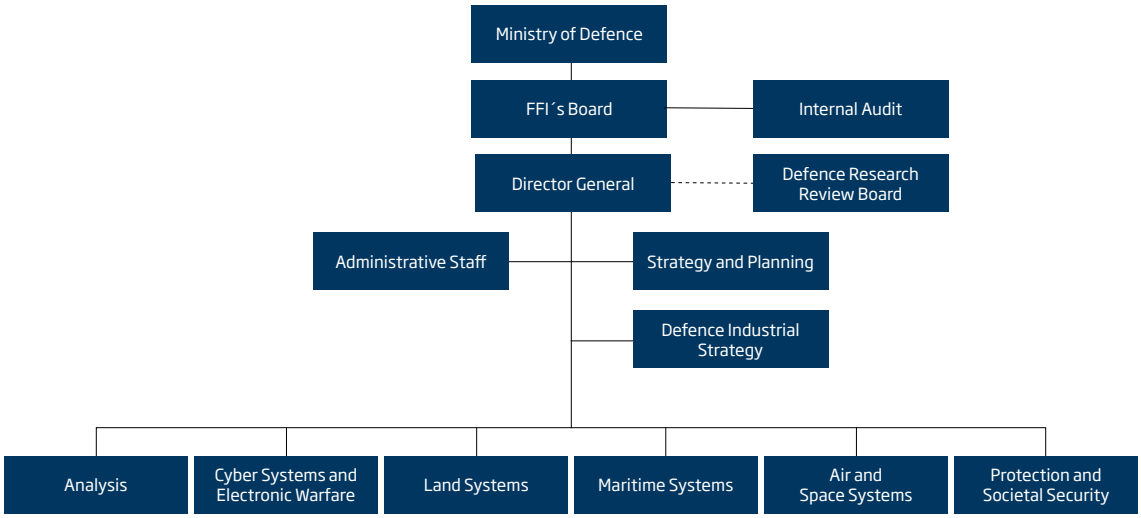
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment