Forsvarets høgskole

våren 2011

Masteroppgave

Fortsatt ansvarsprinsipp eller helhetlig tilnærming til cybersecurity i Norge?

Arild Skillinghaug

Abstract

The government's cyber defense effort is a growing concern in the Norwegian security landscape. The intelligence threat remains high, and the vulnerabilities of the digital infrastructure have become more apparent. The research question for this thesis is: Can the Government of Norway have a comprehensive approach when the principle of responsibility still is the fundamental idea behind the Norwegian crisis management model? First, this paper will shortly address the broader societal interests and values which should be considered when Cyberdefence is used as a term. Secondly, the trends of globalization and the technology dependency will briefly be reviewed. Thirdly, the paper explores how the state has organized itself to handle Cyberthreats to the nation state and their national security interests. This is done by first addressing the Government approach to the new understanding of threats and vulnerabilities, then by addressing the principle of responsibility to the delegation of authority and resources, and lastly by exploring how a comprehensive approach to Cybersecurity, from the Government's point of view, can function alongside the crisis response principle of responsibility. In conclusion, the paper argues that the Norwegian approach to handling threats that come through cyberspace is largely based on the crisis response principle of responsibility and not so much on a comprehensive approach as the Government would like to think. A comprehensive approach must also to a higher degree take into consideration the need for legitimacy both in planning and execution of their efforts.

Summary

The government's cyber defense effort is a growing concern in the Norwegian security landscape. The intelligence threat remains high and the vulnerabilities of the digital infrastructure have become more apparent. This thesis will look into some of the challenges the Government of Norway faces when addressing the threats from cyberspace against the state. The challenge for the Government seems to increase through new adversaries, technology and to a more complex crisis management solution.

The research question of this thesis is: Can the Government of Norway take the comprehensive approach when the principle of responsibility still is the fundamental idea behind the Norwegian crisis management model?

The paper suggests that the threats to the state, facilitated by Cyberspace, must be seen in a wider societal context where the Government's political freedom of maneuver and national economic interests are regarded as national security interests, and should be a part of what must be defended. Different trends of today seems to be self-reinforcing the threats to nation states and their national security interests, and thriving trends demand a constant state of alertness to how national security interests are handled and how they are vulnerable to direct and indirect Cyberthreats.

First, this paper will shortly address the broader societal interests and values whish should be considered when Cyberdefence is used as a term. It is worth noticing that the problem of finding the perpetrator is followed by challenges of prosecuting and trialing criminals. Secondly, the trends of globalization and the technology dependency will briefly be reviewed regarding? this thesis. It is noticeable that these trends seem to be feeding each other, and rapidly changing the scenario of what that is at stake, which the threat actors are and how they operate. Thirdly the paper then explores how the state has organized itself to handle Cyberthreats to the nation state and their national security interests. This is done by first addressing the Government approach to the new understanding of threats and vulnerabilities, then by addressing the principle of responsibility to the delegation of authority and resources, and lastly by exploring how a comprehensive approach to Cybersecurity, from the Government's point of view, can function alongside the crisis response principle of responsibility. In conclusion, the paper argues that the Norwegian approach to handling

threats that come through cyberspace is largely based on the crisis response principle of responsibility and not so much on a comprehensive approach as the Government would like to think. A comprehensive approach must also to a higher degree take into consideration the need for legitimacy both in planning and execution of their efforts.

Forord

Når en nærmer seg 40 år og får lov til å sette av to år til studier med full lønn, blir en ydmyk for det ansvar en har fått og takknemlig for den mulighet dette gir. Så en takk må gå både til FLO/IKT som er min arbeidgiver og FHS som har hatt meg i sin varetekt disse to årene. Tiden fra jeg fikk vite at jeg skulle komme til FHS til nå har gått fort og mang en side har blitt lest i perioden, læringen har vært stor og selv om ikke all pensum har truffet like godt har biblioteket vært en god tilflukt. Biblioteket har også vært en god støtte under tiden med masteroppgaven, og en takk må rettes til Nina og Hege som har gjort livet som søkende student til en uforglemmelig tid. En annen gjeng som ikke må glemmes er studentene jeg har tilbrakt disse to årene sammen med. B2 dere vet selv hvem dere er, takk for at dere tok meg inn, og masterstudentene takk for dette siste året som har gjort oss mer eller mindre til akademikere.

Med denne masteroppgaven har jeg også klart å knytte sammen tidligere utdanning med min arbeidserfaring og personlige interesser. Dessverre er tematikken for oppgaven så altfor relevant i dag, og det har vært en interessant reise inn i ukjente offentlige dokumenter og til sentrale aktører og arenaer. Noen har jeg møtt, flere har jeg snakket med men allikevel kunne ikke alle nås. Jeg vil uansett takke FFI, NSM, NORSIS, NUPI og NSR for reflekterte og interessante samtaler før og undervegs i oppgaveskrivingen.

10-12 år etter siste avsluttede eksamen har gått før denne oppgaven sendes inn, og mye har vært glemt når det gjelder å være student og levere inn skriftlige oppgaver. Jeg vil derfor takke min veileder Palle Ydstebø for å ha troen på dette selv når jeg var usikker, og for sin kritiske gjennomgang av tekstene som har kommet til alle mulige tider av døgnet. I tillegg vil jeg også rette en takk til Kristin B. Sandvik ved PRIO som var en god støtte i arbeidet med å gjøre tankene mine om til et realiserbart prosjekt.

Avslutningsvis må jeg takke min nære familie for akseptansen til min egotripp som en slik oppgave krever. Så Ellen, nå kan bryllupet vårt stå. Ellers må jeg også takke min mor og far for å ha latt meg okkupere kjellerstua og for igjen å ha blitt en del av deres husholdningsutgifter det siste halve året. Svigermor må også takkes for å ha latt meg jobbe når en av guttene, eller begge helst ville ha trøst av pappa. Og til sist må jeg takke Trygve og Sverre for hele tiden å ha vist meg hva som betyr mest i livet.

Innholdsfortegnelse

1. Presentasjon av oppgaven

1.1 Bakgrunn for oppgaven

I Aftenposten i oktober og november i 2010 kunne en finne overskriftene *"Regjeringen tappet for store mengder data"* og *"Nytt dataangrep mot regjeringen"* (Akerhaug & Johansen, 2010; Johansen, 2010c).

Over de siste fem årene har vi fått se konturene av et nytt handlingsrom i internasjonal politikk som åpner for en ny type trusler mot et lands statssikkerhet. Trusselen denne masteroppgaven adresserer er ikke en eksistensiell trussel for staten, men en trussel som kan bidra til å endre maktforholdet både innenriks- og utenrikspolitisk. Det handlingsrommet denne oppgaven tar tak i er definert av de mulighetene som informasjons-, kommunikasjonsteknologiske (IKT) verktøy, internett og cyberspace kan legge til rette for. Ulovlig etterretningsvirksomhet og informasjonsspionasje mot IKT-avhengige sikkerhetsinteresser og verdier som ligger til grunn for Norges statssikkerhet og internasjonale maktposisjon ligger i dette handlingsrommet[1].

Denne oppgaven vil se nærmere på hvordan helhetlig tilnærming til cybersikkerhet i Norge står i et konfliktforhold til det etablerte ansvarsprinsippet i krisehåndtering.

Noen hendelser de siste årene viser klare tendenser på en utvikling hvor IKT brukes på en mer aggressiv måte overfor stater og viktige samfunnsfunksjoner, eksempler på dette er, 1) Estland i 2007. Her ble flere offentlige tjenester og online banktjenester stoppet på en tid hvor det var store politiske reaksjoner mot flytting av et russisk krigsminnesmerke (Kirk, 2007). 2) Iran i 2009, hvor dataormen Stuxnet med stor sannsynlighet lå bak systemsvikten til deres sentrifuger, som brukes til å anrike uran, en nødvendig komponent til bl.a. atomvåpen (NSM, 2010; NTB, 2011). Dette er begge eksempler på en type sjokkhendelser, ofte med politisk motivasjon, som gir en umiddelbar effekt.

Men vi har også en annen type hendelser som kan skape andre og mer langstikige konsekvenser i det internasjonale sikkerhetspolitiske bildet. 3) Wikileaks, nettstedet som ved flere anledninger har publisert sikkerhetsgradert informasjon er en slik trussel. For når frislepp

[1] Begrepene statsikkerhet og informasjonsspionasje vil håndteres og defineres nærmere under Pkt 2.2 & 2.4.

av sikkerhetsgradert materiale i stort omfang kan dette både diskreditere stat og regjering, men også svekke diplomatiet og det internasjonale sikkerhetspolitiske samarbeidet (Reuterdal, Kolberg, & Randen, 2010). 4) Depnett/U som er den øverste statsadministrasjonens ugraderte datanett har vært under angrep, og store mengder informasjon har vært hentet ut av dette nettet. Til tross for at dette er et ugradert system er det allikevel antydet at beskyttet informasjon er ulovlig hentet ut. Den type ubevissthet til egenbeskyttelse av informasjon det her er snakk om har vært gjenstand for kritikk blant annet fra Nasjonal sikkerhetsmyndighet (NSM), Riksrevisjonen og Aftenposten (NSM, 2006, s. 3 & 4; Riksrevisjonen, 2005, s. 16). *"Her ligger blant annet utkast til regjeringsnotater, budsjetthemmeligheter og børssensitiv forretningsinformasjon, samt store mengder følsomme personopplysninger" (Johansen, 2010c).*

Slike hendelser sett i sammenheng med trusselvurderingene til Politiets Sikkerhetstjeneste (PST), og risikovurderingene til NSM gjør at vi må ta IKT-sikkerheten på alvor, både fordi de direkte kan skape konkrete uønskede hendelser eller situasjoner, og fordi de indirekte kan påvirke utviklingen av det samfunnet vi ønsker å leve i. *"Eksempler på informasjon som søkes av andre lands etterretningstjenester er fortrolige politiske samtaler, forhandlingsposisjoner og -strategier, forsvarshemmeligheter, bedriftshemmeligheter, beredskapsplaner samt opplysninger om enkelte innvandrermiljøer og enkeltpersoner (PST, 2006, s. 2)*". Faktisk går PST ennå lenger i sin trusselvurdering ved å si at *" I tillegg til informasjonsinnhenting forsøker etterretningspersonell også å påvirke premissleverandører og enkeltpersoner som deltar i politiske beslutningsprosesser. Det synes åpenbart at etterretningsvirksomhet i vesentlig grad kan bidra til å undergrave Norges og ulike norske aktørers interesser"(PST, 2006, s. 2). "NSMs erfaring er at flere virksomheter ikke i tilstrekkelig grad tar hensyn til at etterretningstrusselen er betydelig. Sagt på en annen måte er flere offentlige virksomheter ikke bevisste nok i utøvelsen av egenbeskyttelse mot etterretningstrusselen" (NSM, 2006, ss. 3-4).*

Statssikkerheten har tradisjonelt vært sidestilt med begrepet rikets sikkerhet og vært sterkt knyttet til trusler mot nasjonens selvstendighet i gjennom konvensjonelle militære angrep mot vårt territorium. Men nå er det er ikke lenger så innlysende om hva vi kjemper for, de territoriale truslene mot Norge er ikke lenger styrende for Forsvaret og sikringen av staten (FD, 2009, s. 22)? Til tross for dette vet vi noe om hva vi kjemper mot, en fortsatt høy internasjonal terror- og etterretningstrussel, samt risikoene knyttet til samfunnssikkerheten (NOU, 2006:6, s. 36; PST, 2010b). Det finnes også trusler mot interesser og verdier som

Norge har i en internasjonal kontekst (St.prp., nr. 48 (2007-2008), ss. 23-26). Ikke minst har miljøvern og levedyktig forvaltning av ressurser i havet og i havbunnen, gjennom olje og gass, hatt en sentral plass i Norges utenrikspolitikk. Kampen om disse godene er uavhengig av landegrenser, de har økt i senere tid og har ført til at det i dag også kan sies å være konkrete trusler mot disse fellesgodene. Dette er trusler mot for eksempel muligheten til å benytte internasjonal farevann, trusler mot overfiske eller til å kunne fritt benytte seg av internett.

Men selv om myndighetenes evne til å utøve suveren kontroll på territoriet ikke er truet utelukker ikke det at statssikkerheten er truet. Dette kan gjøres ved å svekke myndighetens politiske og økonomiske handlefrihet og således gjøre staten som forhandlingsaktør sårbar for press og/eller påvirkning utenfra (PST, 2010b). Denne oppgaven har til hensikt å se nærmere på håndteringen av statssikkerheten, med et utgangspunkt trusler fra cyberspace.

Hvem truer statssikkerheten i dag? I cyberspace, er en av de store utfordringene det som kalles attribusjonsproblemet. Dette problemet dreier seg om vanskeligheten med å finne kilden ved sikkerhetshendelsen (Sommer & Brown, 2011, s. 8). Med en slik utfordring, så vil det også skape utfordringer for håndteringen av hendelsen fordi, som i Norge, så har vi et skille i mellom Etterretningstjenesten og Politiets sikkerhetstjeneste som skal forebygge mot ytre kontra indre trusler. På hver sin side av forsvarssektoren og justissektoren finnes det også operative enheter som evt skal slå tilbake, hindre eller minimere skade. I justissektoren skal enn også evt straffeforfølge. Så dersom kilden forblir ukjent, vil dette også skape krisehåndteringsutfordringer da utfordringen vil havne i gråsonen i mellom flere aktørers ansvarsområder. Denne oppgaven vil redegjøre nærmere for de nasjonale apparatet for å forebygge og håndtere slike trusler og hendelser.

Virkemiddelbruken har endret seg i takt med at globaliseringen har satt sine spor og at aktørbildet for hvem som kan påvirke internasjonal politikk har endret seg. I tillegg har den teknologiske utviklingen og avhengigheten vi nå har til IKT, gjort oss enda mer sårbare. Denne oppgaven vil derfor redegjøre for noen sentrale begreper og trender til oppgavens kontekst.

Med usikkerheten til attribusjonsproblemet, og datanettverkenes økte tilknytninger til internett og/eller andre datanett blir truslene til statssikkerheten raskt et tverrsektorielt foretakende. Dette har også blitt forsterket i gjennom en økt privatisering av offentlige tjenester. Konsekvensene av dette er at kompleksiteten til håndteringen av hendelser også har økt. Er så

ansvarsprinsippet tilpasset denne nye type trusler, og kan myndighetene få til en helhetlig tilnærming?

1.2 Problemstilling og forskningsoppgaver

Innledningen har pekt på at utfordringene med å ivareta statssikkerheten i Norge i dag baserer seg både på forebyggende virksomhet og operativ krisehåndtering. Utfordringene med å ivareta statssikkerheten er strategisk og tverrsektoriell i sin natur. Dette setter noen krav til hvordan dette arbeidet bør tilnærmes. Ikke bare må krisehåndteringsprinsippene være aksepterte og forstått, men de må kunne virke i et samspill med andres oppgaver og ansvar. Definerte grensesnitt i forhold til ansvars- og myndighetsforhold må være avklart. Har en ansvar må en også ha myndighet og tilgang til ressurser og kompetanse, i tillegg kreves det også prioritering. Det må være definerte eskaleringsmuligheter vertikalt mellom sektorer og horisontalt mot strategisk nivå.

I denne oppgaven er det de kritiske samfunnsfunksjonene samt deres interesser og verdier som er viktige. For når disse kritiske samfunnsfunksjonene settes ut av spill, eller deres interesser og verdier ikke ivaretas vil dette bli kritisk for statssikkerheten. Bak begrepene sårbare samfunnsfunksjoner, interesser og verdier ligger blant annet politiets evne til å utføre sine oppgaver og kraftforsyningens evne til å distribuere strøm, gode bilaterale sikkerhetspolitiske bånd, inntekter fra oljesektoren og til slutt blant annet demokrati og ytringsfrihet (NOU, 2000:24, s. 8; 2006:6, s. Kap. 4).

Problemstilling for denne oppgaver: *Vil det være mulig å ha en helhetlig tilnærming til cybersikkerhet i Norge, når ansvarsprinsippet skal ligge til grunn?*

I tillegg til problemstillingen som vil drøftes eksplisitt har oppgaven også noen flere generelle hensikter.

Først vil oppgaven være med på å skape en større tverrsektoriell forståelse av noen av utfordringene, mot statssikkerheten som kan komme gjennom cyberspace. Deretter vil oppgaven også bidra med å skissere dagens og fremtidens utfordringer fra cyberspace, når enkelte trender ser ut til å virke selvforsterkende på sårbarheten i samfunnet. Det redegjøres så videre for noen av de mest sentrale aktørene og arenaene knyttet til forebygging og krisehåndtering. Disse redegjørelsene danner et nødvendig grunnlag for drøftingsdelen av oppgaven. Drøftingen tar for seg noen utfordringer i grensesnittet i mellom helhetlige

tilnærminger og ivaretakelse av ansvarsprinsippet i forbindelse med forebyggende arbeid og utøvelse av krisehåndtering i forbindelse med IKT-hendelser.

1.3 Avgrensninger og avklaringer

I dag sitter Fornyings- Administrasjons- og Kirkedepartement (FAD) med det overordnede ansvaret for regjeringens IKT-politikk. FAD har også samordningsansvaret for forebyggende IKT sikkerhet, og løser dette i et samarbeid med departementene justis-, forsvars- og samferdsel. Dette samarbeidet kalles også for Koordineringsutvalget for informasjonssikkerhet (KIS) og er ansvarlige for utarbeidelsen av *"Retningslinjer for å styrke informasjonssikkerheten",* som har statsforvaltningen som adressat (FAD, 2007). Dette firkløveret var også gjenstand for Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur (Riksrevisjonen, 2005). I tillegg til FADs ansvar har Justisdepartementet (JD) tilsynsansvaret for IKT sikkerhet i sivil sektor (St.meld., nr. 17 (2006-2007)).

Til tross for FADs forebyggende koordineringsrolle, har JD og FD med underliggende etater, det overordnede ansvaret for den forebyggende og utøvende sikkerhetstjenesten for henholdsvis sivil og militær sektor. I det forebyggende arbeidet står Politiets Sikkerhetstjeneste (PST) og Nasjonal Sikkerhetsmyndighet (NSM) sentralt. Av disse to igjen er NSM her i en særstilling siden de danner båndet i mellom JD og FD ved at de rapporterer til JD i sivile saker og FD i militære saker (St.meld., nr. 22 (2007-2008), s. 13).

FAD, JD (PST& DSB), inkl. NSM i FD og SD danner oppgavens indre kjerne av aktører, utover dette vil andre aktører underlagt FAD, JD, FD og SD også være viktige. I tillegg vil evt offentlige og ugraderte samarbeid de i mellom også bli adressert. Når kjernen av aktørene også inkluderer noen av de hemmelige tjenestene, blir også Stortingets kontrollutvalg for Etterretnings-, Overvåknings- og Sikkerhetstjenestene (EOS-utvalget) relevant, fordi det er deres oppgave å føre kontroll med de hemmelige tjenestene.

Aktørene nevnt over er de strategiske og forebyggende aktørene, som ivaretar statssikkerheten i henhold til lovverk og instrukser, gjennom blant annet rådgivning og veiledning (PST Instruks, 2005; Sikkerhetsloven, 1998). Statssikkerheten kan i dag også rammes i gjennom

rettede digitale angrep mot installasjoner og samfunnsviktige tjenester (bl.a. mot kritisk digital infrastruktur og nettbaserte tjenester) som igjen er eid og styrt av private aktører[2] (St.meld., nr. 47 (2000-2001), s. 18). I en helhetlig tilnærming har sektorene, og virksomhetene også en viktig forebyggende rolle i gjennom blant annet tilsyn, men også for virksomhetenes del et direkte ansvar for beredskap og krisehåndtering innen virksomhetene, noe som også inkluderer egen IT-sikkerhet og -beredskap.

Her møter vi på ett par dilemmaer knyttet til oppgaven og tolkningen av helhetlig tilnærming. Det første dilemmaet er knyttet til i hvilken grad oppgaven skal inkludere både forebyggende og operative aktører. Mens det andre dilemmaet adresserer utfordringen med hvor langt en skal gå i beskrivelsen av og inkluderingen av både offentlige og sivile aktører. Spørsmålet knyttet til disse dilemmaer er i hvor stor grad skal enn, og kan en ofre dybde for bredde i en slik oppgave?

Denne oppgaven vektlegger behovet for en mer helhetlig tilnærming i større grad enn å løse alle fremtidige utfordringer med ansvarsprinsippet i det forebyggende, skadereduserende og normaliserende arbeidet i krisehåndteringen.

	Offentlig	Sivilt/Privat
Forebyggende	Justissektoren (PST, PDMT, DSB/DNK) Forsvarssektoren (NSM, Etj, INI, FLO/IKT) NorSIS FAD SD (Post og Teletilsyn)	Næringslivets Sikkerhetsråd(NSR) Andre bransjespesifikke rådgivere
Operativt	JD (NorCERT, KRIPOS, Politiets Datakrimsenter, KSE) FD Forsvarets INI FAD (DSS)	IKT Driftssentre i de privatiserte bransjene med kritisk infrastruktur

Figur 1 Aktørinndeling

[2] I denne oppgaven vil uautorisert tilgang til, manipulering av, nedlasting eller kopiering av beskyttet informasjon forstås med et rettet digitalt angrep. Dette tilsier at oppgaven har et fokus på de angrep som gjennomføres av en aktør med intensjon og de nødvendige kapabiliteter (evne og vilje) til å gjennomføre et angrep med den hensikt å fremtvinge et ønsket resultat.

Kildetilfanget for oppgaven består av hovedsakelig de dokumenter som er produsert av Stortinget, departementer, direktorater med underliggende enheter og evt spesifikke utredningsgrupper nedsatt av disse. Det er viktig å påpeke at valgt problemstilling, og at oppgaven blant annet adresserer de hemmelige tjenestene, vil det kunne påvirke oppgaven i drøftingsdelen. Sentrale sider ved disse tjenestene er ikke offentlig tilgjengelig informasjon og deler av det som er interessant å drøfte grenser mot informasjon som enten er unntatt offentlighet eller også sikkerhetsgradert etter sikkerhetsloven. Oppgaven vil allikevel drøfte problemstillingen på bakgrunn av tilgjengeliggjort ugradert informasjon fra sikkerhetstjenestene og fra offentlige dokumenter, forskning og rapporter.

Siden avslutningen av den kalde krigen har det nå gått 20 år, og faren for at vi skal rammes av en ny konvensjonell krig vurderes fortsatt som veldig liten. At vi i dag er i en fredstidssituasjon og at vi sannsynligvis vil forbli det i de nærmeste årene, er førende for min oppgave (FD, 2009, s. 23). Det vil si at oppgavene og ansvaret vurderes ut fra regelverk og ansvarsfordeling i fredstid.

Dette får dog noen konsekvenser for oppgaven. For det første så vil da den offensive bruken av IKT-virkemidler i krigstid ikke bli adressert i denne oppgaven (St.prp., nr. 48 (2007-2008), s. 88). Dette er selvsagt viktige komponenter i Regjeringens helhetlige tilnærming til å håndtere IKT-trusler, men dette er også en type informasjon som i stor grad er unntatt offentligheten og hemmeligstemplet av sikkerhetsmessige hensyn etter Sikkerhetsloven. Det er derfor lite sannsynlig at en kunne ha fått et stort nok kildetilganget rundt regjeringens offensive tiltak, til å kunne gjøre en god vurdering av disse tiltakene.

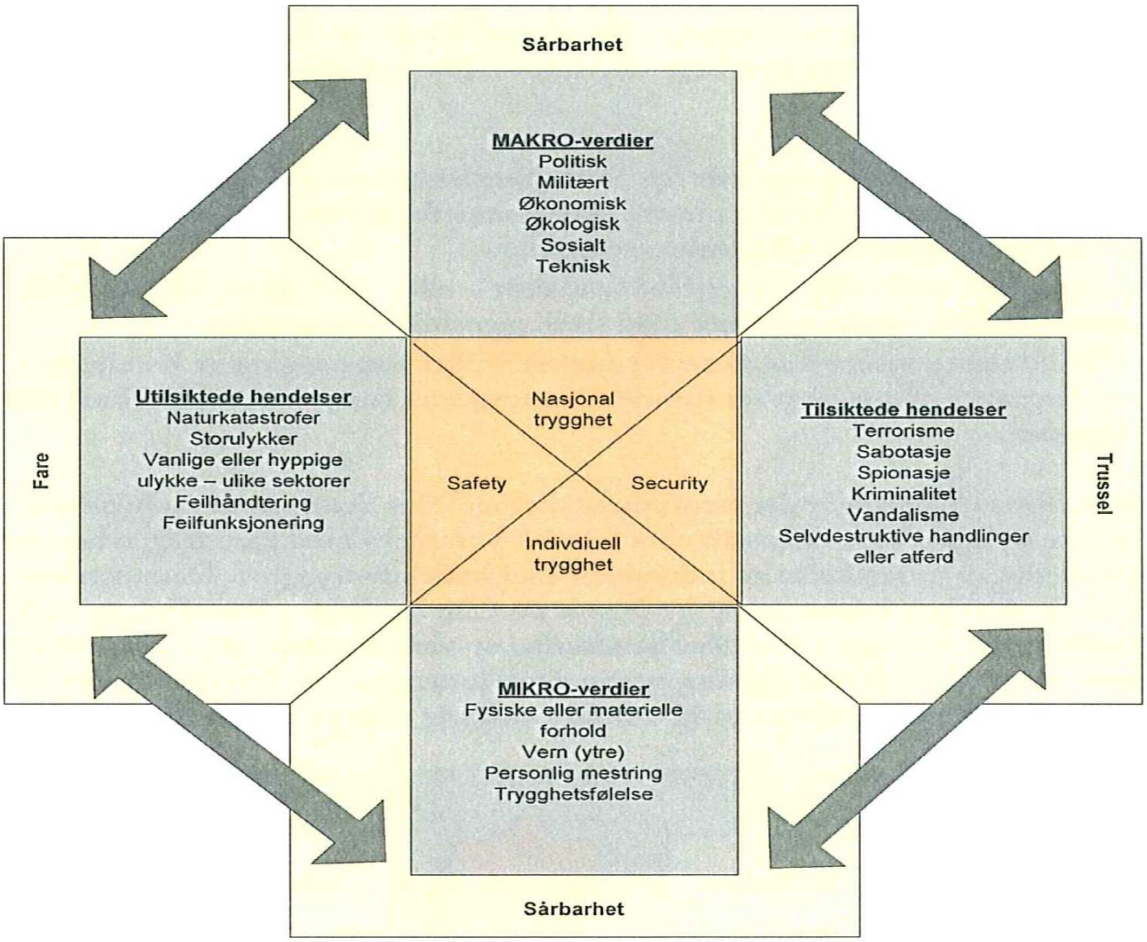
Avslutningsvis vil jeg avklare overfor leseren at når denne oppgaven skrives arbeides det med mange relevante saker i tilknytning til denne oppgaven. 1) Det er påbegynt et arbeid med revidere den nasjonale strategien for informasjonssikkerhet (FAD, 2007). 2) Det er i ferd med og etableres en ny norsk strategi for cybersikkerhet (NSM, 2009a). 3) FD har meddelt at Sikkerhetsloven skal evalueres dette året. 4) Forskrift for objektsikkerhet, er akkurat tredd i kraft og må således finne sin funksjon i samfunnet. 5) NATO leverte på tampen av 2010 sitt seneste strategiske konsept hvor Cybersikkerhet nå også er tatt inn under de sikkerhetsområdene som anses som viktigst for NATO (2010a). Avslutningsvis er det også relevant å kommentere at den nye foreslåtte straffeloven fra 2005, ennå ikke er trådd i kraft, noe som får den konsekvensen at det er Straffeloven av 1902 som er den gjeldende pr. i dag.

1.4 Om annen forskning

Som sivil student ved Forsvarets Høgskole, med interesse for samfunnssikkerhet er grensesnittet mellom sivil og militære krisehåndtering spesielt interessant. I det sivile har en også grensesnittet mellom offentlig og privat noe som gjør bildet for nasjonal krisehåndtering interessant og komplekst. Jeg vil derfor her gi et kort innblikk i den strategiske og sektorovergripende forskningen. Denne oppgavens utgangspunkt har vært å bidra med komplementær informasjon i forhold til den allerede eksisterende forskningen på området. Det er derfor ikke gjort noe stort forsøk på å kritisere annen forskning, men heller på å utfylle der det fortsatt er rom for mer. Dog vil annen forskning brukes aktivt for bl.a. å utdype og underbygge påstander når nye sammenhenger knyttes.

Forskningsrådet har kjørt flere programmer med mer tverrfaglige og tverrsektorielle tilnærminger innen denne oppgavens kontekst, de forskningsprogram og prosjekter som ligger nærmest opptil denne oppgaven er:

SAMRISK, er et forskningsprogram som ser på samfunnssikkerhet i lys av både globaliseringskonsekvenser og teknologiutvikling (SAMRISK, 2006, s. 4). I utgangspunktet er ikke dette ulikt denne oppgavens innretning. Jeg mener det i SAMRISK er en vesentlig mangel og svakhet som bør bli adressert. I programplanen for SAMRISK henvises det til Forsvarets langtidsplan fra 2005-2008 når de avgrenser sitt arbeid slik at de ikke vil omhandle oppgaver som sammenfaller med Forsvarets primære oppgaver om å forsvare rikets sikkerhet og suverenitet (St.prp., nr. 42 (2003-2004)). Til tross for dette vektlegges det også i SAMRISK at de nye samfunnsutfordringene krever en tilnærming på tvers av sektorer og med en høy grad av tverrfaglighet (SAMRISK, 2006, s. 7). På grunn av den avgrensning som er lagt til grunn i SAMRISK adresserer ikke SAMRISK viktige elementer ved dagens utfordringer med tilsiktede hendelser mot makroverdier, selv om SAMRISK erkjenner viktigheten av en helhetlig tilnærming som inkluderer forsvaret i samfunnssikkerhetskontekster på andre områder. Denne oppgaven vil bidra med komplementær informasjon til SAMRISK.



Figur 2. hentet fra SAMRISK programplan 2006 (SAMRISK, 2006, s. 6).

IKT Sikkerhet og Sårbarhet, forkortet IKTSoS var et forskningsprogram som gikk fra 2003-2007 og som fokuserte på å generere ny viten og kunnskap, som ett bidrag til å øke sikkerheten og redusere sårbarheten ved bruk av IKT-systemer (IKTSoS, 2008, s. 2). Hovedhensikten bak dette programmet var todelt, på den ene siden ønsket man å heve tilliten til elektronisk samhandling, på den andre siden ville den også bidra til å utvikle en sikkerhetskultur i samfunnnet (IKTSoS, 2004, s. 5). Det siste punktet sammenfaller godt med de behovene NSM så for samfunnet og som ble presentert i deres første offentlige risikovurdering i 2003[3] (NSM, 2003, s. 19).

Programmet IKTSoS har også flere overordnede målsetninger som ligger tett opptil denne oppgavens tema. Det vises dog ikke til en eksplisitt avgrensning til trusler mot rikets sikkerhet, nasjonale sikkerhetsinteresser og verdier som tilsier at dette skal håndteres eller

[3] Den første ugraderte risikovurderingen la blant annet vekt på at en mer helhetlig sikkerhetstjeneste måtte inneholde både administrative, kompetansemessige og rapporteringsmessige sikkerhetskrav m.m.

ikke. De relevante målsetningene i IKTSoS, for denne oppgaven, som lå inne i IKTSoS er a) redusere sårbarheten ved alminnelig bruk av IKT og i kritisk IKT-infrastruktur og b) støtte nasjonale strategier innen IKT sikkerhet og sårbarhet (IKTSoS, 2004, s. 6). Relevansen til denne oppgaven er knyttet til BAS-5 og deres leveranser. BAS-5 har vært en sentral del av mitt kildegrunnlag i denne oppgaven (Fridheim & Hagen, 2007; Henriksen, Sørli, & Bogen, 2007; Sørli, Henriksen, Bogen, & Mørkestøl, 2007/00875).

Det teknologifokuserte forskningsprogrammet VERDIKT har også bidratt med interessante prosjekter og leveranser, som har relevans for denne oppgaven. Det er dog ikke vektlagt i oppgaven da dette programmet satte teknologien i første rekke.

1.5 Disposisjon av oppgaven

Oppgavens kapittel 1 er en introduksjon til temaet, hvor temaet og oppgaven presenteres og avgrenses. I tillegg er det gitt plass både en gjennomgang av relevant forskning samt en presisering av de metodiske valg som er gjort og hvilke konsekvenser dette har for oppgaven.

Kapittel 2,3 og 4 er alle kortere redegjørelser for å sette begreper, trender og aktører inn i denne oppgavens kontekst.

Kapittel 2 avklarer og definerer først begrepene cyberspace og statssikkerhet. Deretter vil oppgavens forhold til nasjonale sikkerhetsinteresser avklares, og ansvarsprinsippet presenteres. Avslutningsvis redegjøres det også for etterretning og kontraetterretning,

Kapittel 3 beskriver trendene globalisering og den økende teknologiavhengigheten i samfunnet.

Kapittel 4 redegjør kort for hvilke aktører som i dag har et forebyggende og/eller et utøvende ansvar i beskyttelsen av statssikkerheten i Norge.

Kapittel 5 er oppgavens drøftingsdel og her vil jeg drøfte om truslene fra cyberspace, mot statssikkerheten håndteres på en helhetlig måte, og om hvordan forholdet til ansvarsprinsippet løses. Argumentene er: 1) Opprettholdelse av ansvarsprinsippet stenger for en helhetlig tilnærming. 2) Med ansvar følger ikke nødvendigvis myndighet eller ressurser. 3) Det eksisterer ingen legitim tverrsektoriell aktør for å håndtere en helhetlig tilnærming.

I Kapittel 6 vil jeg oppsummere oppgaven med en vurdering av om forskningsspørsmålene kan ansees å være besvart, og hvilke konklusjoner enn kan dra av dette samt hvilke videre implikasjoner dette gir for aktiviteten og den videre forskningen på dette området.

1.6 Metodiske valg og konsekvenser

Det er valgt en kvalitativ tilnærming til oppgaven fordi den er godt egnet til denne oppgavens tema. Fleksibiliteten i en kvalitativ tilnærming er i tillegg er nyttig virkemiddel for å få frem et mer nyansert bilde av stort tema (Jacobsen, 2005, s. 129). Valget er i tråd med det som Creswell peker på når han ser forskningsdesign i sammenheng med verdensbildet for deg som forsker, den strategi og de metoder en velger å benytte (Creswell, 2009, s. 16). Han knytter dette med å ha et sosialkonstruktivistisk verdensbilde for forskeren, med både en deltakende og observerende rolle som metode.[4] En sosial konstruktivistisk forsker søker å forstå eller tolke meningen andre har om verden (Creswell, 2009, s. 8). I bunnen av dette ligger også en personlig overbevisning om at meningsdannelse alltid er sosial og er et resultat av interaksjon i mellom mennesker. Det utelukker ikke at meninger også dannes uten interaksjon. Men i forhold til denne oppgaven så er tanken om den sosialt betingede meningsdannelsen styrende. *"There is an agreement, though, that the elusive and unsubstantiated nature of cyber-threats means that approaches rooted in the constructivist mindset with a subjective ontology are particularly suitable for its analysis (Cavelty, 2007, s. 21)"*

Enhetene som undersøkes i oppgaven er de aktørene som har et forebyggende og/eller utøvende IKT-ansvar i beskyttelsen av statssikkerheten. Materiellet til denne oppgaven vil hentes hovedsakelig ut fra tekstanalyser av offentlige dokumenter. Jacobsen trekker frem tre situasjoner der kildegransking vil være spesielt godt egnet, hvor av to stemmer veldig godt overens med hensikten med min oppgave (Jacobsen, 2005, s. 164).

1.6.1 Metodologisk kollektivisme

> *Hvis vi tar utgangspunkt i individet, vil vi ikke være i stand til å forstå noe som helst av det som foregår i en gruppe. … Følgelig er det slik at hver gang et sosialt fenomen blir direkte*

[4] Det er her viktig å påpeke at under prosessen med oppgaven har jeg måttet innta en sterkere deltakende rolle en først forutsatt da, temaets lille utbredelse i forskningssammenheng har medført at jeg har vært helt avhengig av å skape dialog basert på nye sammenhenger oppgaven har fokusert på.

> *forklart ved å vise til et psykologisk fenomen, så kan vi være sikre på at forklaringen er gal.*
>
> *Emile Durkheim (Gilje & Grimen, 1993, s. 176)*

Metodisk velges det en kollektivistisk fremfor individualistisk fremgangsmåte for oppgaven, en av grunnene til dette ligger i en grunnleggende usikkerhet hos meg som forsker til det å få frem mest mulig objektiv informasjon ved individualistiske fremgangsmåter. En annen årsak er at en kollektivistisk tilnærming vil støtte opp under tanken om at samspillet mellom individ og i situasjon er styrende for resultatet (Jacobsen, 2005, s. 30). For det som står i de offentlige dokumenter er nettopp et resultat av gruppeprosesser i politiske miljø, departementer, deres underliggende enheter og i dialog med det private næringsliv. Og dersom en ser på enheten som skal studeres, så er det et kollektiv (myndighetene, på vegne av regjeringen), og ikke et individ (evt statsministeren som er leder av regjeringen).

Det er viktig å få frem et mest mulig objektivt bilde av helheten for å kunne bidra til en bedre felles tverrsektoriell forståelse av utfordringene. Med større bruk av, eller en økt prioritering av individuelle og subjektive tilbakemeldinger som grunnlag for å skrive en slik oppgave, vil en også bryte med det verdensbilde jeg tidligere har presentert. Dog er oppgavens tema og forskningsmessig bredde slik at det har vært nødvendig med dialogpartnere i arbeidet.

Min skepsis til en fremgangsmåte hvor personlige intervjuer og samtaler ligger til grunn for informasjonsinnsamlingen har også påvirket mitt metodiske valg. Når personlige intervjuer og samtaler i forskningsprosesser ligger til grunn for analysearbeidet vil dette kunne prege forskeren og forskningsprosessen negativt. For under samtaler og intervjuer vil forskeren i større grad kunne påvirke resultatet i gjennom styring av dialogen (Creswell, 2009, s. 9). Dersom forskeren i tillegg har en misjonerende rolle i forskningsarbeidet, vil det forsterke den negative konsekvensen av å bruke samtaler og intervjuer som metode i informasjonsinnhentingen.

Som ansatt ved FLO/IKT og med informasjonssikkerhet som hovedarbeidsoppgave og med samfunnssikkerhet som personlig interesse, kan det stilles spørsmålstegn til mitt ønske om å inneha en misjonerende rolle som kommentert. Dette er jeg som forsker klar over og dialogpartnernes bidrag er i så måte tenkt å positivt påvirke den rollen jeg spiller som forsker i gjennom å bidra med perspektiver jeg selv ikke ser. Jeg vil derfor også benytte anledningen til å understreke at det som presenteres i denne oppgaven ikke er å anse som et produkt av min

arbeidsgiver, eller mine samtalepartnere og heller ikke bør brukes som et utgangspunkt for deres syn på temaet for oppgaven. Forøvrige er alle feil mine egne.

1.6.2 Intersubjektivitet

I sosialkonstruktivistisk baserte meningsdannelser snakker vi ikke om *"rene"* objektive sannheter, men en felles enighet mellom deltakerne som er en del av den gruppen som diskuterer. Alle de dokumenter jeg legger til grunn i denne oppgaven er et reultat av gruppearbeid. Intersubjektivitet blir derfor helt essensielt å beskrive nærmere for denne oppgaven. Den delte enigheten her er ikke nødvendigvis den hele og fulle sannhet, og gruppeprosesser har i seg flere utfordringer som igjen kan påvirke resultatet, både gruppens interne personkjemi og medlemmenes kompetanse og personlighet er noen av de utfordringene som følger gruppeprosesser (Jacobsen, 2005, s. 155).

Innsamlingen av kilder/dokumenter har gått utover de departement som har blitt presentert som den indre kjernen av aktører. Dette fordi en finner viktige ansvarsforhold også i andre departement og underliggende enheter når det gjelder håndtering av trusler fra cyberspace, sett fra regjeringens side. Ansvaret for å koordinere IKT-sikkerheten ligger hos FAD, ansvaret for telekommunikasjon som ligger hos Samferdselsdepartementet (SD). Forholdet til intersubjektivitet har fått den konsekvens for oppgaven at det har vært et fokus i prosessen om å få et så bredt utvalg som mulig når det gjelder kilder.

2. En bredere plattform med flere perspektiver

For å kunne skape en bredere plattform for en felles forståelse av de nye utfordringene på tvers av sektorer vil denne delen av oppgaven se litt nærmere på noen viktige definisjoner og nødvendige begrepsavklaringer. Av hensyn til det videre arbeidet med drøftingen vil ulikheter i tolkning mellom JD og FD vektlegges. FAD og SDs rolle slik jeg har tolket dette støtter i større grad tanken om utvikling som en åpning av muligheter enn de sikkerhetsmessige utfordringer de skaper, selv om dette ikke er et entydig bilde (Riksrevisjonen, 2005, s. 13; St.meld., nr. 17 (2006-2007), s. 14).

2.1 Om Cyberspace

Forfatteren William Gibson, og bøkene hans *"Burning chrome"* og *"Neuromancer"* fra henholdsvis 1982 og 1984 er ofte brukt for å gi begrepet cyberspace et opphav. Men som andre begreper innen IT- bransjen har de ofte kort levetid, eller en tidsavhengig tolkning. Herunder vil jeg derfor se på hvordan noen relevante organisasjoner og dokumenter i senere tid har definert dette begrepet.

Internasjonalt finner vi både forsøk på å definere cyberspace, og utfordringer med å gi dette et konkret innhold. Til tross for at USA har operert med sin tolkning og definisjon har ikke NATO inkludert begrepet i sin offentlige ugraderte ordbok (US Army CAC, 2008, s. 139).

NATO bruker dog cyber-begrepet til å forklare hva som menes med Computer Network Attack (NATO, 2010b). Men dette er dessverre til liten hjelp, da dette impliserer at leseren både forstår konteksten av hva et angrep er, og om avgrensningen av begrepet er gjort etter en vid eller smal tolkning av hva innholdet dekker. I vurderingen om en skal bruke vid eller smal tolkning av begrepets innhold må en se på i hvilken grad en skal ta høyde for om, 1) mennesket selv, og de minnepinner, disketter eller andre lagringsmedier vi bærer med oss, skal være med i tolkningen. 2) Om tidsaspektet er viktig dvs skal en se på hendelser som bare skjer i nåtid eller skal en også inkludere hendelsers konsekvenser og ringvirkninger.

NATO har etablert et Cooperative Cyber Defence Centre of Excellence i Tallinn, Estland. Og ved denne institusjonen har man utarbeidet en definisjon[5]. *"Cyberspace is a time-dependent*

[5] Denne definisjonen er igjen bygget blant annet på følgende: *" …the virtual space in which the electronic data of worldwide PCs circulate*" laget av European Commission og gjengitt i deres ordbok .

set of interconnected information systems and the human users that interact with these systems" (Ottis & Lorents, 2010).

Utfordringen nasjonalt er at relativt mange dokumenter bruker begrepet cyber-, og/eller cyberspace uten å definere dette nærmere. Bruken forutsetter at leseren implisitt forstår konteksten det brukes i og dermed også hvordan begrepet avgrenses mot andre begreper.

Stortingsmelding nr. 17 2006-2007 og NOU 2006:6 bruker både begrepene cyberangrep og cybertrussel, og i Forsvarets strategiske konsept "Evne til innsats", brukes også begrepet cyber-angrep uten å definere dette videre (FD, 2009; NOU, 2006:6; St.meld., nr. 17 (2006-2007)). Verken JD, FD eller FAD har bidratt til en bedre forståelse av begrepet gjennom offentlige dokumenter. NSM, med bånd til både JD og FD, har i sin cybersikkerhetsstrategi fra desember 2009 henvist til en udatert tolkning av begrepet cyberspace fra Wikipedia[6]. Til tross for at Wikipedia, muligens ikke er det anbefalte leksikon av akademikere, er allikevel likhetene mot den amerikanske tolkningen av begrepet cyberspace stor. *"the interdependent network of information technology infrastructures (ITI), telecommunications networks—such as the internet, computer systems, integrated sensors, system control networks and embedded processors and controllers common to global control and communications" (NSM, 2009a, s. 5).*

Det denne gjennomgangen viser er at det på departementalt nivå ikke ser ut til å være en omforent tolkning. Og at det på direktoratsnivå foreligger det en teknologifokusert tilnærming til tolkningen av begrepet cyberspace. Denne er ikke like helhetlig som det NATOs Cooperative Cyber Defence Centre of Excellence i Tallinn, legger til grunn. Her vektlegges mennesket og tidsaspektet som en del av dynamikken i cyberspace. En teknologisk basert definisjon mener jeg er interessant, men feil pga av bl.a disse årsakene.

For det første så sementerer den problematikken som et teknologisk problem og anliggende for IKT-avdelingene, og reduserer dermed muligheten for en helhetlig tilnærming mellom utøvende og strategiske nivåer og aktører. For det andre forsterker NSMs definisjon, fokuset på symptomene og ikke problemet, dvs IKT virkemidlene og ikke lovbryterne som skal straffes. Ved å gjøre dette så forblir det ingen trussel for lovbryterne å utføre digitale angrep, fordi fokuset ikke ligger på å straffeforfølge lovbryterne.

[6] Dessverre kan ikke teksten i samme form gjenfinnes på Wikipedia i dag, men denne tolkningen vil allikevel kunne stå på egen bein sett fra NSMs side dersom dette er ønskelig. Under forutsetning av dette vil den gi oss i hvertfall en pekepinn på hva vår nasjonale sikkerhetsmyndighet legger til grunn når de bruker begrepet cyberspace.

Med tanke på dette, er det viktig å påpeke at NSM i cybersikkerhetsstrategien har lagt inn flere tiltak for å styrke samordningen av cybersikkerhetsarbeidet samt evnen til å oppdage, varsle, håndtere & etterforske IKT-hendelser (NSM, 2009a).

2.2 Statssikkerhet og grunnleggende nasjonale sikkerhetsinteresser

Rikets suverenitet, selvstendighet og rettigheter er sammen med Norges interesser og verdier alle sterke og tunge uttrykk i en nasjonalstat. Begrepet statssikkerhet er kanskje noe mer ukjent. For denne oppgaven er dog statssikkerhet et sentralt begrep. Men hva legges så i dette begrepet? Forsvarsdepartementet har i Stortingsproposisjonen om "Et forsvar til vern om Norges sikkerhet, interesser og verdier", lagt følgende til grunn i vurderingen av hva statssikkerheten innholder, og hvordan dette har endret seg de siste 20 årene.

> *"Den viktigste oppfatningen av sikkerhetspolitikkens formål har vært og er fortsatt **statssikkerheten,** som det grunnleggende sikkerhetsbehov knyttet til statens eksistens, suverenitet og integritet. Mens statens eksistens, suverenitet og integritet. Mens statssikkerheten i vår del av verden før 1990 var knyttet til trusselen om invasjon, har situasjonen etter 1990 først og fremst vært preget av faren for **ulike former for politisk og militært press,** og begrensede episoder, kriser og anslag[7]" (St.prp., nr. 48 (2007-2008), s. 24).*

Hvis vi ser på JD, så peker de tilbake på FDs langtidsplan for Forsvaret (2005-2008) i sin tolkning av begrepet statssikkerhet (NOU, 2006:6, s. 42). Prof. Erling Johannes Husabø skrev i Problemnotatet til utredningen om rikets sikkerhet at kapitteloverskriftene i gjeldende straffelov ikke gir et godt nok bilde av hva som var ønsket å verne av verdier, men at en må se nærmere på hver enkelt paragraf for å finne de vernede rettsgoder[8] (NOU, 2003:18, s. 175).

Utover straffelovens bestemmelser kan følgende lover og instrukser utdype hva som ligger i begrepet statssikkerhet: Instruksen til Politiets sikkerhetstjeneste (PST), Lov og Instruks om Etterretningstjenesten (Etj) samt Sikkerhetsloven[9]. Dette er relevant fordi det er PST, Etj og

[7] Originalteksten er gjengitt med den kursivering som er gitt i stortingsproposisjonen.

[8] Mer om forskjellene i mellom gjeldene og ny straffelov er håndtert nærmere i kap. 7.2 (NOU, 2003:18, ss. 87-119).

[9] Nasjonal Sikkerhetsmyndighet er forvalter av Sikkerhetsloven, se §9 (Sikkerhetsloven, 1998).

NSM`s å drive myndighetsutøvelse overfor både ytre og indre trusler mot det statssikkerheten er beskrevet som.

Avslutningsvis vil jeg peke på to andre relevante dokumenter i denne sammenhengen som vil gi leseren en bedre kontekstuell forståelse av statssikkerhet for denne oppgaven. Det første dokumentet er NSMs Veiledning i Verdivurdering (NSM, 2009b). Her defineres begrepene rikets selvstendighet og sikkerhet samt begrepet andre vitale nasjonale sikkerhetsinteresser, i tillegg vurderes også begrepet nasjonal handlefrihet som er at interesse for denne oppgaven (NSM, 2009b, s. 7).

Det andre dokumentet jeg vil vektlegge her er FFIs Bakgrunnsstudie til metode for identifisering og rangering av kritiske samfunnsfunksjoner. Her benyttes begrepene kritiske samfunnsfunksjoner og infrastruktur, ordet *"bærbjelker"* brukes også for å understreke kritikaliteten til funksjonen eller infrastrukturen[10] (Sørli, et al., 2007/00875, s. 17). Bakgrunnsstudien fremhever følgende momenter fra denne utredningen: Samfunnet skal sikres mot utfordringer mot sentrale samfunnsverdier som liv, folkehelse og velferd, livsmiljøet, det demokratiske system og dets lovlige institusjoner, nasjonal styringsevne og suverenitet, landets territoriale integritet, materiell og økonomisk trygghet og kulturelle verdier (Sørli, et al., 2007/00875, s. 20).

Et bidrag til vurderinger rundt statssikkerhet og de grunnleggende nasjonale sikkerhetsinteresser, fra denne oppgavens side er å peke tilbake til den samfunnskontrakten som er i mellom stat og individ i våre samfunn. Innholdet i denne kontrakten har vært mye vurdert av filosofer i flere århundrer, og selv om denne oppgaven ikke vil gå i gjennom alle disse forskjellige vurderingene, ønsker jeg heller å vektlegge at det i en viss grad alltid vil være en form av overenskommet samfunnskontrakt mellom stat og individ. Og dersom det oppleves at denne kontrakten ikke oppfylles når det gjelder de fysiske behovene samt behovene for trygghet i befolkningen over tid, så vil statssikkerheten kunne være eller bli truet. Politiet har adressert behovet for å ivareta denne trygghetsfølelsen overfor befolkningen som en del av denne samfunnskontrakten, men uten at det også er å anse som et virkemiddel til å ivareta statssikkerheten (St.meld., nr. 42 (2004-2005), ss. 57 & 60-61).

[10] Når ord som "bærebjelke" brukes om en samfunnsfunksjon eller infrastruktur legges det i denne oppgaven til grunn at ved bortfall, så vil dette skade statssikkerheten igjennom at samfunnets strukturer gir etter.

Det er vanskelig å finne en omforent tolkning av innholdet i begrepet statssikkerhet mellom JD og FD, men etter en gjennomgang av en del offentlige dokumenter fra JF og FD, kan det tyde på en ikke helt lik praksis, verken mellom aktørene eller innen sektorene.

2.3 Ansvarsprinsippet

De overordnede prinsippene om ansvar, nærhet og likhet ligger til grunn for alt nasjonalt sikkerhets- og beredskapsarbeid. Men det viktigste og bærende prinsipp for den praktiske fordelingen av beredskapsansvar i samfunnet er ansvarsprinsippet. Dette prinsippet vektlegger at den som har ansvaret for et fagområde i fredstid også har ansvaret for å håndtere ekstraordinære hendelser og kriser på området (St.meld., nr. 22 (2007-2008), s. 10).

I forhold til denne oppgavens kontekst er ansvarsprinsippet å forstå med følgende oppgaver, for det enkelte fagdepartement: 1) Vurdere, beslutte og iverksette tiltak av forebyggende karakter i egen sektor. 2) Forberede beredskapstiltak (jf. krise og krig). 3) Planlegge for (og ev. iverksette) krisehåndtering innen egen sektor. Og 4) Føre tilsyn med, og følge opp egne underlagte etater (FAD, 2011).

2.4 Etterretningstrusselen

Den type trusler som denne oppgaven dreier seg om er hovedsakelig ulovlig etterretningsvirksomhet mot beskyttet informasjon, og som kan skape store utfordringer for ivaretakelsen av den norske statssikkerheten. En definisjon av hva begrepet ulovlig etterretningsvirksomhet rommer, er gjengitt i utredningen om Politiets overvåkningstjeneste tilbake i 1998. Hensikten med kontraetterretning er da å forebygge og motvirke ulovlig etterretningsvirksomhet (PST, 2011a). *"… enhver aktivitet som utføres mot Norge for på ulovlig vis å skaffe til veie informasjon om militære, politiske, økonomiske, teknologiske eller andre samfunnsmessige forhold, og som kan være til skade for landets sikkerhet" (NOU, 1998:4, s. 78).* Denne type trussel er blitt en viktigere del av trusselbildet de siste 20 årene. Dette gjentas også i PSTs åpne trusselvurderinger utover hele 2000-tallet. Det rapporteres at flere staters etterretningstjenester er aktive, og informasjonsinnhenting og påvirkning av myndighetenes beslutninger forekommer (PST, 2004, 2007). PST bruker og definerer begrepene *"cyberetterretning og datanettverksetterretning"*, som andre staters etterretningstjenesters data- og internettbaserte operasjoner. Det som preger disse

operasjonene er datainnbrudd, for å kopiere, endre eller slette informasjon (PST, 2011b, ss. 10, Fotnote 13).

> *"Transnasjonale trusler, herunder terrorisme og spredning av masseødeleggelsesvåpen, utgjør en sentral del av Etterretningstjenestens aktivitet. Innenfor arbeidet med terrorisme står samarbeidet med Politiets sikkerhetstjeneste sentralt for å kunne sikre Norge og nasjonale interesser. Dette samarbeidet ble ytterligere styrket i 2010. Da iverksatte tjenesten arbeidet med å styrke Forsvarets evne til å forstå og møte trusler fra det digitale rommet. Som ledd i arbeidet ble Forsvarets avdeling for Computer Network Operations overført til Etterretningstjenesten, med virkning fra 1. januar 2001" (FSJ, 2011, s. 93).*

Avslutningsvis vil jeg peke på at uansett om cyberetterretning gjøres av politiske eller økonomiske årsaker, så viskes skillene ut i mellom etterretningsaktivitet, diplomatisk aktivitet og kriminell aktivitet (Johansen & Foss, 2011). Etterretningstjenesten i Norge har på 2000-tallet ved flere anledninger påpekt det økte antallet forespørsler fra sivil sektor (Grandhagen, 2011a, s. 2; Hagen, 2006, s. 2). Dette er ikke uproblematisk, og grensesnittet i mellom PST, Etj og NSM har i flere år vært gjenstand for et utfordrende samarbeid, godt fulgt opp av kontroller fra EOS-utvalget.

3. Selvforsterkende trender

Globaliseringen og teknologiutviklingen er to sentrale drivkrefter bak omreguleringen av offentlig virksomhet de siste tiårene. Dette har også påvirket hvilke sikkerhets- og beredskapshensyn som har blitt vektlagt og ivaretatt under omreguleringer og omorganiseringer den siste tiårsperioden (NOU, 2006:6, s. 84). En kort redegjørelse av disse to trendene vil være med på å danne et grunnlag for å sette dagens utfordringer inn en større sikkerhetsmessig kontekst.

3.1 Globaliseringens konsekvenser

Før vi går inn på globaliseringens konsekvenser må begrepet gis et innhold, som er knyttet til denne oppgaven, dens formulering og målsetning. Dette fordi begrepet i seg selv rommer mange tilnærminger. Jan Aarte Scholte kategoriserer noen forskjellige tilnærminger til globalisering. En kan velge å se nærmere på 1) Internasjonalisering, 2) Liberalisering, 3) Universialisering, 4) Vestifisering (modernisering) og 5) Deterritorialisering[11] (Scholte, 2000, ss. 15-16). Basert på Scholtes inndeling vil jeg kort ta for meg internasjonalisering og liberalisering for å vise til en uheldig utvikling som er av interesse for denne oppgaven. En utvikling som også vil påvirke myndighetenes evne til å styre sårbarheten i samfunnet.

1) Internasjonalisering som globaliseringstrend er adressert som en utfordring både av Justisdepartementet og av Forsvarsdepartementet (FD, 2009, s. 14; NOU, 2006:6, s. 40). I begrepet internasjonalisering legger man bl.a. den økte trafikken over landegrensene av mennesker, varer og tjenester, kulturimpulser, ideologier og religion. Det er selve grensekryssingen som vektlegges og at hyppigheten av grensekryssing har økt. I den senere tid har det også vært meldt om både angrep mot regjeringen og aktører som Norge som stat identifiserer seg med (Akerhaug & Johansen, 2010; Johansen, 2010b, 2010c). Det kan derfor være interessant å se på noen sårbarheter knyttet til demokrati og autoritære styreformer.

a) En kan hevde at regimeskiftene i 2011(Egypt og Tunisia) kan være et resultat av en blanding av en ideologisk, kulturell og politisk internasjonalisering. For tanken om at med

[11] Dette er mine oversettelser, og spesielt er begrepet vestifisering problematisk da dette ikke har en naturlig oversettelse i norsk språk. Utgangspunktet her er at det er en tilnærming

demokrati kommer fred er ingen ny tanke, andre igjen vektlegger at IKT, internett og cyberspace som virkemiddel også har bidratt i mobiliseringen til vesentlige samfunnsendringer (Dragnes, 2011; galrahn, 2011).

Det finnes også kritiske røster som maner til varsomhet med å konkludere med at internett og sosiale medier er å anse som sentrale aktører og arenaer i slike revolusjoner (Vassnes, 2011). Det er også en grunn til å være kritisk til IKT, internett og cyberspace som virkemiddel til vesentlige samfunnsendringer. For til tross for at ett undertrykket folk i en åpen stat kan bruke IKT, internett og cyberspace som virkemiddel, vil det dette også kunne brukes av myndighetene i en lukket stat til å fortsette undertrykkelsen av befolkningen, gjennom sensurering, propaganda og elektronisk kommunikasjonskontroll.

b) Her ligger også utfordringen for den vestlige verden. For verdier som demokrati, rettssikkerhet og yttringsfrihet er også under press her. Motstanden i Norge i forbindelse med innføringen av Datalagringsdirektivet og statens involvering (gjennom NATO og med FN mandat) i ikke internasjonale væpnede konflikter, viser folkets misnøye både med å øke statens muligheter for overvåkning og inngripen overfor individet, men også for deres utenriks- og sikkerhetspolitikk (Torgersen, Ege, Johnsrud, & Johnsen, 2011).

2) I den nye og globaliserte verden, utfordres nå også handlingsrommet i internasjonal politikk av private aktører i en global økonomi. En liberalistisk tilnærming til globaliseringen tar i større grad tak fjerningen av tidligere nasjonale handelsbarrierer, slik at de globale markedene får større makt enn de tidligere nasjonale beskyttede markedene. Det tilsier også at de aktørene som er så store at de kan agere transnasjonalt har økt sin mulighet til å påvirke mellomstatlige forhold, enkeltstater og deres interesser og verdier. Det er ikke nytt å peke i retning av store transnasjonale aktører for å vise til hvordan disse kan påvirke internasjonal politikk, men her er det skjedd noen endringer. Dette er knyttet til både til a) eierskapet i kraftforsynings- og telekommunikasjonsbransjen, men også til b) globaliseringen spesielt i sistnevnte bransje.

a) Privatiseringen av kraftforsynings- og telekommunikasjonsbransjen en har sett i Norge på 1990-og 2000-tallet, har medført at nasjonalstaten har gitt slipp på mulighetene til å kontrollere og påvirke tilgangen til elektrisk kraft og telekommunikasjon (Rutledal, Hagen, Nystuen, & Østby, 2000, s. 9; St.meld., nr. 47 (2000-2001), s. 3).

b) IT selskaper har vokst i størrelse og omfang i samme takt som samfunnet har økt sin avhengighet til teknologiske infrastrukturer og systemer. Dette har også styrket deres mulighet til å påvirke den praktiske politikken.

Det kan derfor være interessant å se litt på slike IT-selskapers agendaer, for å vurdere hvordan de ser sin rolle nasjonal og internasjonal politikk. Google på sin side har i sin filosofi vektlagt blant annet at demokrati på internett fungerer, og at behovet for informasjon krysser alle grenser (Google, 2011). Nettsamfunnet Facebook derimot har i sine prinsipper vektlagt åpenhet og transparens for å skape en større forståelse og kontakt (Facebook, 2011).

> *"What do we make of an American corporation …basically declaring war on the government policies of a strategic partner of the United States by inventing a new technology and offering free services to the political opposition of the Egyptian government? Whether one agrees or disagrees with what Google is doing – when you remove the morality element of Google's action that can easily impact ones opinion – we are left with a few American corporations actively supporting a revolution* ***as a free service*** *against the current government of a strategic partner of the United States"*[12] *(galrahn, 2011).*

Jeg mener det er viktig å anerkjenne den akkumelerte virkningen av utviklingen når to prosesser som gjensidig påvirker hverandre får utvikle seg. I dette tilfellet har vi på den ene siden en økning av internasjonal handel og veksten av globale aktører. Mens det på den andre siden også gjennomføres en privatisering av samfunnskritisk infrastruktur fra stat til private sektor. En av konsekvensene av dette er redusert mulighet for myndighetene å kunne styre og påvirke samfunnets sårbarhet.

3.2 Om Teknologiavhengighet

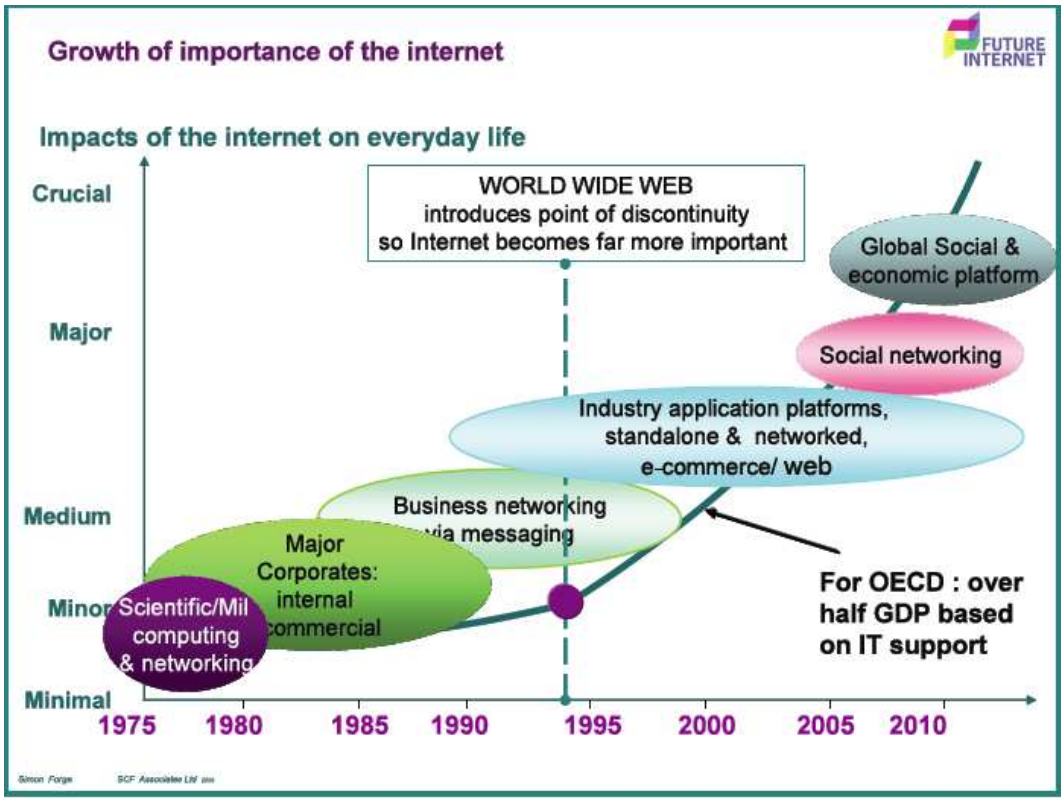
Teknologiutviklingen førte til en utvikling av måten å arbeide på, men vil også teknologiavhengigheten forandre måten å beskytte seg på? Teknologien har vært en sentral byggesten i, og blitt et bortimot uunnværlig redskap i vestlige samfunn. Dette har medført økt

[12] Uthevelsen er gjort da dette i den opprinnelige teksten var i skravur, og at dette ikke ville komme frem i teksten ved å legge hele teksten i skravur. Jeg vil også kommentere at teksten er hentet fra en blogg, og til tross for at dette muligens ikke er veldig vanlig i en masteroppgave er dette gjort pga 1) at dette er bloggen til U.S. Naval Institute, *"Founded in 1873, … a non-profit, professional military association …. An independent, nonpartisan forum on global security issues, it creates books, magazines, blogs and conferences …"(U.S. Naval Institute, 2008).* 2) Og selv om det er et anonymt innlegg, så har jeg fått godkjent bruken av sitatet, og oppbevarer navnet og e-postadressen selv etter avtale.

sårbarhet for feilbruk, driftsfeil og intenderte angrep på bl.a. kritisk infrastruktur i samfunnet. Forsvarets forskningsinstitutt (FFI) har siden 1994 arbeidet med et forskningsprogram som går inn til kjernen av dette punktet, i disse dager er FFI i ferd med å etablere BAS6[13]. *I alle BAS-prosjektene så man hvordan IKT-systemer var viktige for å opprettholde tjenester i kritisk infrastruktur. Samtidig ble det vurdert slik at IKT-sårbarheter kunne utnyttes for å ramme samfunnskritisk virksomhet" (Fridheim & Hagen, 2007, s. 9).*

Maskiners kraft, systemer og nett kan brukes i krig, terrorsammenheng eller med en kriminell intensjon, og selv om en var tidlig ute og så farene som i utredningen om POT i 1998, kan vi nå i 2011 supplere dette med flere faktiske hendelser (Lewis, 2011).

> *Mange norske interesser er blitt mer sårbare for terror- og sabotasjeanslag, bl a pga IT-utviklingen og vår rolle som energiprodusent. Vernet om rikets sikkerhet kan derfor bli en mer mangfoldig, variert og kanskje også mer komplisert oppgave enn tidligere" (NOU, 1998:4, s. 10).*



Figur 3 Internetss økte betydning. Kilde: OECD/IFP Project on *"Future global shocks"*, report *"Reducing Systemic Cybersecurity Risks"* (Sommer & Brown, 2011, s. 18).

[13] BAS6 er det 6 prosjektet i rekken av prosjekter knyttet til forskningsprogrammet "Beskyttelse av samfunnet".

Figuren over gir et godt bilde på utviklingen av avhengigheten til internett, og at vi mer eller mindre nå er ligger på en sosial avhengighet, er vist tidligere i oppgaven (galrahn, 2011). Før samfunnets overlevelse, gjennom blant annet globale økonomiske plattformer blir avhengig av internett vil tiden som kommer bli kritisk for hvilke valg myndighetene velger å gjøre. I Norge vil vi finne flere eksempler på hvordan avhengigheten til internett både forklares og beskrives, basert på hvilke aktører som omhandlet temaet (NOU, 2000:24, ss. 38-39; St.meld., nr. 17 (2006-2007), s. 14). Teknologiavhengighet er noe vi samfunnet har et ambivalent forhold til. For på den ene siden vil teknologiutviklingen gi så mange muligheter for effektivisering og kostnadsbesparelser, realiseringer av demokratisk og liberalistisk politikk samt integrasjon i en stadig mer internasjonal og globalisert verden at det er vanskelig å takke nei til dette (St.meld., nr. 17 (2006-2007)). På den andre side vil det også gi økt sårbarhet og usikkerhet i samfunnet, når sårbare systemer for organisasjonene nå har blitt til sammenvevde nett som går over sektorer og landegrenser.

4. Aktører som håndterer statssikkerheten

Først vil det kort gjøres rede for de mest sentrale aktørene som har et ansvar for å ivareta den forebyggende informasjonssikkerheten. Dette er aktører på politisk og strategisk nivå. Deretter vil det også redegjøres kort for noen viktige aktører på også på operativt nivå, som har et ansvar for å bidra i sikringen av staten. Hensikten med presentasjonen er å klarlegge hvilke aktører og arenaer som bidrar helhetlig og sektorielt til cybersikkerheten i samfunnet i dag.

4.1 Justissektoren

JD har en unik posisjon med tanke på deres samordningsrolle for å sikre en helhetlig og koordinert beredskap i Norge. Ellers i justissektoren finnes det flere aktører som både har et strategisk og utøvende ansvar i å beskytte statssikkerheten.

PST har i henhold til Politilovens §17b ansvaret for å forebygge og etterforske lovbrudd etter straffelovens kapittel 8 & 9, lov om forsvarshemmeligheter og sikkerhetsloven (Politiloven, 1995). Andre aktører i Justissektoren er mer praktisk utøvende og har et operativt ansvar. Dette tilsier at de er med på å møte konsekvensene av utfordringene som kommer fra IKT, internett og cyberspace. Kripos inkl. Politiets Datakrimsenter og Politiets Data og Materiellteneste vil også bli presentert her, noe mer kortfattet.

4.1.1 Departementenes samordningsråd for samfunnssikkerhet

I forbindelse med JDs samordningsrolle etablerte JD dette rådet i 2007, og erstattet dermed det tidligere rådet for sivil beredskap og Redningsrådet. Dette forumet utveksler informasjon- og erfaringer mellom departement når det gjelder samfunnssikkerhet, beredskap, redningstjeneste og sivilt-militært samarbeid. Alle departement og SMK er representert (St.meld., nr. 22 (2007-2008), s. 12).

4.1.2 Politiets sikkerhetstjeneste (PST)

Dersom vi ser på ansvarsfordelingen i fredstid vil vi se at trusler mot staten, også de som kommer i gjennom cyberspace, er knyttet til PSTs ansvarsområde. PST er underlagt og

regulert både i gjennom Politiloven og egen instruks (Politiloven, 1995; PST Instruks, 2005). PST er i den forebyggende virksomhet underlagt Justisdepartementet, mens de i etterforsknings- og påtalespørsmål er underlagt Riksadvokaten og statsadvokatembetene (PST, 2011a).

Arbeidsoppgavene til den forebyggende sikkerhetstjenesten er gjengitt i 1) Politilovens § 17b, og i 2) Straffelovens bestemmelser i Kapittel 8 og 9 som handler mer konkret om forbrytelser mot Norges selvstendighet, statsforvaltning, ulovlig etterretningsvirksomhet samt sabotasje eller politisk motivert tvang (Politiloven, 1995; Straffeloven, 1902). Formuleringen av PSTs overordende oppgave, utenom etterforskning, er gjengitt i deres instruks: ***"§ 4.*** *Overordnet oppgave: Politiets sikkerhetstjeneste skal bidra til å sikre viktige samfunnsinteresser og gjennom sin virksomhet være et ledd i samfunnets samlede innsats for å fremme og befeste borgernes rettssikkerhet, trygghet og alminnelig velferd" (PST Instruks, 2005).*

PST har et nært samarbeid med andre aktører innad i Justissektoren og nasjonalt, da fortrinnsvis med Forsvarssektoren gjennom hovedsakelig Etterretningstjenesten og NSM[14] (Sælør, 2010, s. 284). PST ved DSE har siden 2004 utgitt åpne trusselvurderinger i tillegg til de graderte som er forbeholdt politiske myndigheter.

4.1.3 Kripos & Politiets Datakrimsenter

Kripos håndterer i dag organisert og alvorlig kriminalitet, i tillegg er de også politiets 1) kompetansesenter for metodeutvikling, 2) kriminaltekniske laboratorium, og 3) har behandlingsansvaret for sentrale informasjonssystemer (KRIPOS, 2006). Det siste tilsier således at Kripos har et viktig grensesnitt til PDMT angående IKT.

> *"Teknologiutviklingen har dramatisk økt muligheten for analyse av tekniske og elektroniske bevis i forbindelse med politiets etterforsking. Skal politiet forfølge ambisjonene om effektiv og troverdig kriminalitetsbekjempelse, må politiet ha tilstrekkelig nivå på utstyr og kompetanse. Nye Kripos med Politiets datakrimsenter er det sentrale politiorganet med spisskompetanse på disse områdene" (St.meld., nr. 42 (2004-2005), s. 87).*

[14] Samarbeidet med Forsvarssektoren er regulert både i gjennom Instruks om Forsvarets bistand til Politiet og i gjennom Instruks for samarbeid i mellom Etterretningstjenesten og Politiets sikkerhetstjeneste.(Bistandsinstruksen, 2003; Samarbeidsinstruksen, 2006)

4.1.4 Politiets Data og Materielltjeneste

Politiets data- og materielltjeneste (PDMT) ble etablert 1. januar 2004. Særorganet er et rådgivnings- og utviklingsorgan med oppgaver innen bl.a. materiellforvaltning, drift og utvikling av sentrale politiregistre, IKT-løsninger og andre tekniske løsninger.

Virksomhetsområdet IKT består av enhetene Produktledelse, Utvikling og Drift. I forhold til ivaretakelse av statssikkerheten er det her viktig å påpeke følgende om PDMTs ansvar. Som eier av alle produkter/tjenester som leveres til politi- og lensmannsetaten har de ansvaret for 1) arkitekturen til IKT systemene, 2) prosessene rundt utvikling, testing og realisering av nye systemer og integrasjoner mot andre systemer og 3) kvalitetssikre tilgjengeligheten og kapasiteten på leverte tjenester (PDMT, 2011).

4.1.5 Direktoratet for samfunnssikkerhet og beredskap (DSB)

DSB har oversikt over risiko og sårbarhet i samfunnet, og skal være en pådriver i arbeidet med å forebygge bl.a. kriser og andre uønskede hendelser. De skal også sørge for god beredskap og effektiv og krisehåndtering innen sitt ansvarsområde. Av vesentlig betydning for denne oppgaven er deres ansvar for å forvalte lov om elektriske anlegg og utstyr.

Årsaken til at dette er satt som en vesentlig oppgave er realiseringen av trusler(Stuxnet) mot elektroniske prosess og kontrollsystemer som for eksempel SCADA(Supervisory Control And Data Acquisition), (NSM, 2010). Her er det dog et grensesnitt også mot de respektive fagdirektoratenes ansvar. Det er også DSB som er ansvarlig for gjennomføring av JDs tilsynsansvar overfor departementene når det gjelder samfunnssikkerhet.

4.2 Forsvarssektoren

Som i Justissektoren har Forsvarssektoren også noen aktører som både har et strategisk, forebyggende og utøvende ansvar i å beskytte statssikkerheten. Her vil kun NSM inkludert NorCERT sees nærmere på i denne redegjørelsen. Etterretningstjenesten ansvar er knyttet til utenlandsetterretningen og vil ikke bli videre redegjort for da PST, med ansvaret for innenlandsetterretningen og kontraetterretningen er en mer sentral enhet for denne oppgaven. Siden PDMT i justissektoren er tatt med, kunne jeg også ha valgt å ta med Forsvarets Logistikkorganisasjon / IKT divisjonen (FLO/IKT) og Forsvarets informasjonsinfrastruktur

(INI), siden de har et ansvar som har noen prinsipielle likheter med PDMT. Men av hensyn til de respektives ansvarsområder i fredstid kontra krig vil ikke de omtales nærmere.

4.2.1 Nasjonal Sikkerhetsmyndighet inkl NorCERT

Nasjonal Sikkerhetsmyndighet (NSM)

> *FO/S [Forsvarets Overkommando/ Sikkerhetsstaben] ble allerede etter ikrafttredelsen av sikkerhetsloven 1. juli 2001 gitt funksjon som Nasjonal Sikkerhetsmyndighet (NSM). Funksjonen som stab i Forsvarets overkommando og betegnelsen FO/S opphørte imidlertid først med virkning fra 1. januar 2003, i forbindelse med omorganiseringen av stabsfunksjonene mv i Forsvaret, og etablering av NSM som eget direktorat under Forsvarsdepartementet* (EOS, 2002, s. 9).

NSMs oppgaver er beskrevet nærmere i Sikkerhetslovens §§8-9, og beskriver deres forebyggende nasjonale rolle til å koordinere og kontrollere både sikkerhetstiltak og –tilstand for de virksomheter som er underlagt sikkerhetslovens bestemmelser. Som en forebyggende aktør vektlegges både det å komme ut med informasjon, gi rådgivning og veiledning. Deres kontrollfunksjon er beskrevet nærmere i Sikkerhetslovens §10 og dekker både skjermingsverdig informasjon og objekt. Som både PST og Etterretningstjenesten, følges NSM opp av EOS-utvalget. NSM, er et eget direktorat men har rapporteringsplikt til JD i sivile saker og FD i militære saker. Forholdet til henholdsvis JD og FD er regulert i egen forskrift, og sier i hovedsak at mens JD og FD har det overordnede ansvaret i sivil vs militær sektor, mens NSM det utøvende forebyggende ansvaret i begge sektorer (FD, 2003).

I tillegg til å bli eget direktorat i 2003 tok NSM også over ansvaret for lokalisering og drifting av Varslingssystemet for Digitalt Infrastruktur (VDI), som fra 2001 hadde vært pilot prosjekt under ledelse av PST, ved den sentrale enhet (DSE), (EOS, 2003, s. 12). VDI-prosjektet var i perioden 2001-2003 et fellesprosjekt mellom EOS-tjenestene. Oppgaven til systemet var å detektering uautoriserte forsøk på inntrengning i viktige datasystemer og å varsle IT-driftsmiljøene og sikkerhetspersonellet ved de involverte virksomhetene.*”Da VDI ble startet som er samarbeidsprosjekt mellom EOS-tjenestene(*) høsten 2000, var det det første*

nasjonale intrengningsdeteksjonssystemet (IDS) i verden som baserte seg på samarbeid mellom offentlige og private aktører[15]" (NorCERT, 2011).

Det er viktig for oppgaven å ta med seg at det å koble seg opp til å bli med i VDI, i dag er valgfritt for de virksomheter som er underlagt Sikkerhetsloven, og at en medlemsavgift også må betales.

Norwegian Computer Emergency Response Team (NorCERT)

"Når NorCERT blir fullt operativt i løpet av 2006, skal det ha ansvar for beredskap og krisehåndtering samt funksjonsgjenoppretting etter dataangrep. VDI og NorCERT er samlokalisert og vil til dels benytte det samme personellet" (EOS, 2005, s. 13).

NorCERT har i dag ansvaret for å utrede det nasjonale trusselbildet, innen sitt domene. I forbindelse med det forebyggende bør det nevnes at PST anerkjenner, NSM, og NorCERTs ansvar og kompetanse på feltet IKT-trusler. Men til tross for dette er NSMs fremlagte Cybersikkerhetsstrategi møtt med en viss motstand. *"PST finner imidlertid ikke at det forslag til strategi for cybersikkerhet som nå er sendt på høring er et tilstrekkelig grunnlag for spesifikke tiltak i sin nåværende form" (PST, 2010a).* Det er relevant å ta med seg at NSM og NorCERT har grensesnitt overfor PST i Justissektoren og Etterretningstjenesten i Forsvarssektoren når det gjelder utredelser av trusselbildet mot og i Norge, sett i denne oppgavens kontekst.

4.3 Andre forebyggende og operative aktører

4.3.1 Fornyings- og Administrasjons- og Kirkedepartementet (FAD)

Siden de første retningslinjene for å styrke informasjonssikkerheten kom ut i 2003, etter et initiativ fra Nærings- og Handelsdepartementet, gikk stafettpinnen til

[15] *"(*) EOS-tjenestene (alle har skiftet navn siden VDI ble startet): Etteretningstjenesten (E) (het Forsvarets overkommando etteretningstjenesten i 2000) Politiets sikkerhetstjeneste (PST) (het Politiets overvåkningstjeneste i 2000) Nasjonal sikkerhetsmyndighet (NSM) (het Forsvarets overkommando sikkerhetsstaben i 2000)",(NorCERT, 2011).*

Moderniseringsdepartementet, før dette skiftet navn til Fornyingsdepartementet og deretter også til FAD pr. 1.1. 2006.

FADs samordningsansvar for forebyggende IKT-sikkerhet

FAD skal være 1) pådriver overfor fagdepartementene, og bidra med ressurser til aktiviteter i regi av fagdepartementene. 2) Avdekke og følge opp sikkerhetsspørsmål som spenner over flere sektorer, samt å ta initiativ til og koordinere tiltak for å løse disse. 3) Utarbeide oversikter og strategier. 4) Koordinere departementenes sikkerhetsaktiviteter gjennom å legge til rette for at aktører med ulikt ansvar har arenaer hvor de kan utveksle erfaringer og drøfte felles problemstillinger (FAD, 2011).

FAD: Avdeling for IKT og fornying

FAD har i dag det overordnede ansvaret for IKT-politikk i Norge som ivaretas av deres avdeling for IKT og fornying. FAD har ansvaret for utgivelsen av de nasjonale retningslinjene for å styrke informasjonssikkerheten, men utarbeidelsen av retningslinjene gjøres i samarbeid med FAD, JD, FD og SD. Denne strategien er kommet ut for to perioder og er nå, i 2011, igjen under revisjon (FAD, 2007; NHD, FD, & JD, 2003).

Departementenes Service Senter (DSS)

DSS er en underliggende etat i FAD og IKT ansvaret i DSS er lagt til to enheter (DSS, 2011): 1) Informasjons og kommunikasjonsavdelinga (IKT). Denne avdelingen har drifts- utviklings og realiseringsansvaret for alle IKT løsninger i 13 av 17 departement, noen sentrale IKT løsninger for de andre departementene samt noen virksomheter[16]. 2) Informasjonsforvaltningsavdelinga (IFA). Denne avdelingen har ansvaret for informasjonstjenestene på IKT løsningene som tilbys.

Norsk senter for informasjonssikring (NorSIS)

NorSIS er et forebyggende og rådgivende ressurssenter innen informasjonssikring for små og mellomstore bedrifter samt offentlige myndigheter på regionalt og kommunalt nivå i Norge.

[16] DSS har ikke drifts- utviklings og realiseringsansvaret for blant annet FD, JD og Finansdepartementet.

Som et ressurssenter bidrar NorSIS både med å utvikle behovsrettede veiledninger og inn forskjellige prosesser, prosjekter og samarbeid med kunder og FOU miljøer.

4.3.2 Samferdselsdepartementet (SD)

Post – og Teleseksjonen v/ Luft, Post og Teleavdelingen

Samferdselsdepartementet har i gjennom politikkutforming, etat og virksomhetsstyring og forvaltning ansvaret for rammevilkårene i markedet for elektronisk kommunikasjon. En av de viktigste oppgavene sett i forhold til denne masteroppgavens kontekst er deres ansvar med å forvalte loven om elektronisk kommunikasjon (Ekomloven, 2003). Med ansvaret for rammevilkårene menes også forvaltningen av deler av den digitale infrastrukturen i Norge.

Post og teletilsynet

Post og teletilsynet er knyttet til samferdselsdepartementet som en egen virksomhet og underlagt Instruks for Post og teletilsynet. Post- og teletilsynet ivaretar tilsynsfunksjonen innen telemarkedene. Tilsynsoppgavene omfatter blant annet kontroll av kvaliteten på tjenestene og sikring av konkurransen i markedet for telekommunikasjon. PTs oppgaver er i henhold til stortingsmeldingen om telesikkerhet og –beredskap fra 2001 som følger: (St.meld., nr. 47 (2000-2001), s. 32).

4.4 Fellesaktører

I tillegg til rene organisasjoner er det også noen andre sammenslutninger og formaliserte samarbeid som bør nevnes, da de har relevante roller og funksjoner i informasjonssikkerhetsarbeidet i Norge i dag.

4.4.1 Koordinerings- og rådgivningsutvalget for etterretnings- og sikkerhetstjenestene

På det øverste strategiske nivået i embetsverket vil vi finne dette fora, her håndteres de overordnede mål, koordinering av prioriteringer og arbeidsoppgaver ved felles problemstillinger, knyttet til trusselbildet for PST, Etterretningstjenesten og NSM. I tillegg til sjefene for PST, Etterretningstjenesten og NSM inkluderer dette fora også representanter fra DU, JD og FD. Koordinerings- og rådgivningsutvalget for etterretnings- og sikkerhetstjenestene (KRU) er underlagt egen instruks og EOS-utvalgets kontroll (EOS, 2007;

JD, 2002).*"Det er etablert et fast sekretariat for utvalget med representanter for de tre departementer som skal tilrettelegge for og følge opp saker som behandles i utvalget" (NOU, 2006:6, s. 48).*

For denne oppgavens kontekst vil det være hensiktsmessig å påpeke KRU instruksens §2 hvor det står følgende i tredje ledd.*"Utvalget kan etter behov anmode representanter fra andre departementer, direktorater, institusjoner og virksomheter mv., om å møte i utvalget for å redegjøre om aktuelle emner eller saksforhold" (JD, 2002).* Overfor de berørte statsrådene har de deretter en rådgivende rolle.

4.4.2 Koordineringsutvalget for forebyggende informasjonssikkerhet (KIS)

KIS er et tverrsektorielt samarbeid mellom overordnede myndigheter med regelverks og tilsynsansvar i staten, og deres underliggende enheter. Dette ble etablert i 2004 som en konsekvens av en bevisst satsing på å øke den nasjonale koordineringen av regelverk og tilsyn innen informasjonssikkerhet (NHD, et al., 2003, s. 21).

I dag ledes KIS av FAD, i nært samarbeid med Justisdepartementet og NSM spesielt. KIS` koordineringsoppgaver går i hovedsak ut på å drøfte, anbefale og samordne regelverk, standarder, normer, metoder for å ivareta informasjonssikkerheten, og den helhetlige tilnærmingen til dette fra statens side (St.meld., nr. 22 (2007-2008), s. 41). Dette tilsier at KIS også skal identifisere tverrsektorielle utfordringer på IKT-sikkerhetsområdet. Og for å sikre en helhetlig beskrivelse av det IKT-trusselbildet som kan skape utfordringer har NSM v/NorCERT, Politiets sikkerhetstjeneste og Etterretningstjenesten etablert en egen koordineringsgruppe hvor oppgaven konkret er lagt til å beskrive IKT-trusselbildet (JD, 2008, s. 125).

KIS v/FAD som lederdepartement er også ansvarlig for utgivelsen av de nasjonale retningslinjene for informasjonssikkerhet (FAD, 2007). Dette dokumentet er planlagt revidert i 2011, et arbeid som sammenfaller i tid med revideringen av Sikkerhetsloven og behandlingen av den Cybersikkerhetsstrategien[17].

[17] I tillegg til dette gjenstår ikraftsettelsen av den nye straffeloven.

Det er viktig for oppgaven videre og påpeke dette, fordi disse tre arbeidene vil både måtte koordineres og det må også evt. vurderes hvordan endringene de i mellom påvirker hverandre, så fremt en velger å gå videre med alle tre oppgavene samtidig.

5. Helhetlig tilnærming kontra ansvarsprinsipp

5.1 Innledning til drøftingen

Drøftingsdelen vil bruke begrepet helhetlig tilnærming. Derfor er det også et behov for å klargjøre dette begrepet noe mer, siden begrepet ikke er redegjort for dette tidligere i oppgaven. Ved Forsvarets Høgskole ble det i 2010 skrevet en egen mastergradsoppgave om dette begrepet. Oppgaven til Hokstad ser på begrepet, tolkningen og bruken i et perspektiv hvor tilnærmingen til komplekse militære operasjoner er utgangspunktet. Dette gjør ikke bruken av begrepet i denne oppgavens sammenheng feil, men jeg vil her vektlegge det prinsipielle med en slikt tilnærming uavhengig av type sak. *"**Helhetlig tilnærming** framstår derfor som verktøyet for å samordne sivil–militær innsats i forfølgelsen av samfunnets verdier og interesser, …[18]" (Hokstad, 2010, s. 58).*

Problemstillingen til denne oppgaven er: *Vil det være mulig å ha en helhetlig tilnærming til cybersikkerhet i Norge, når ansvarsprinsippet fortsatt skal ligge til grunn?*

For å besvare denne problemstillingen har jeg tatt tak i tre argumenter som jeg vil drøfte nærmere. Disse tre argumentene tar tak i sentrale utfordringer rundt håndhevelse av ansvarsprinsippet i en tid hvor helhetlig tilnærming også anses som et krav (St.meld., nr. 17 (2006-2007), s. 10).

Drøftingen vil se nærmere på 1) tolkningen av rammene til en helhetlig tilnærming. Her adresseres utfordringer vi ser i dag knyttet til organisasjonenes egen tolkning av sitt ansvarsområde kontra en helhetlig tilnærming. Dette gjøres ved å ta et utgangspunkt i 2 akser som en kan vurdere helhetlig tilnærming til. Aksene som vil bli brukt er a) sektor kontra helhetlig tilnærming og b) offentlig kontra private aktører. Drøftingen av argument 1 vil kunne danne et grunnlag for å vurdere om helhetlig tilnærming, gitt myndighetens tilnærming, er realiserbart med et fortsatt eksisterende ansvarsprinsipp.

[18] I Hokstads oppgave er begrepet "Helhetlig tilnærming" satt i kursiv, derfor er dette uthevet i min gjengivelse av hans tekst.

2) Det andre argumentet: Med ansvar følger ikke nødvendig delegert myndighet eller egen prioritering fra organisasjonens side. Argumentet er ment å følge opp det foregående argumentet, men vil ta nærmere for seg det dialektiske forholdet mellom myndighetens delegering av myndighet til aktørene og aktørens eget ansvar for prioritering av sine ressurser og oppgaver. Resultatet av drøftingen til dette argumentet kan bidra med å klarlegge i hvilken grad ansvarsprinsippet i dag faktisk er implementert og om ansvarsprinsippet eller helhetlig tilnærming er styrende for myndighetenes og virksomhetenes tilnærming til cybersikkerheten.

3) Det siste argumentet: Det finnes ingen legitim aktør for å kunne håndheve en helhetlig tilnærming. Dette argumentet vil ta tak i et av myndighetenes forsøk på å etablere èn aktør som skal kunne fungere i en helhetlig tilnærming, til tross for at ansvarsprinsippet skal holdes i hevd. Argumentet vil drøftes ved å se nærmere på tiltak 22 i den nasjonale strategien for cybersikkerhet, utarbeidet av NSM (NSM, 2009a). Resultatet av denne drøftingen vil kunne gi en pekepinn på om myndighetene er modne for en helhetlig tilnærming til cybersikkerhet, eller om ansvarsprinsippet bør videreføres.

5.2 Argument 1): Ingen enighet om rammene for en helhetlig tilnærming

5.2.1 Akse 1: Sektor kontra helhetlig ansvar

Internett og tjenester på internett (sektoransvar) kontra helhetlig koordineringsansvar for informasjonssikkerhet, kritisk IKT infrastruktur og ansvar i krisesammenheng:

Her vil jeg se nærmere på to kjente utfordringer innenfor den helhetlige tilnærmingen. Ansvarsfordelingen i mellom FAD og SD er i grove trekk slik at FAD har det helhetlige ansvaret for IKT-politikk og koordineringsansvaret for informasjonssikkerhet, mens SD har ansvaret for de forhold som er lagt inn under loven om elektronisk kommunikasjon (ekomloven)[19]. Dette tilsier at en har et grensesnitt mot hverandre med tanke på ansvaret for

[19] Ekomloven **§ 1-2.** *Saklig virkeområde*: Loven gjelder virksomhet knyttet til overføring av elektronisk kommunikasjon med tilhørende infrastruktur, tjenester, utstyr og installasjoner. Forvaltning og bruk av det elektromagnetiske frekvensspekteret og nummer, navn og adresser er omfattet. Det samme gjelder all utstråling av elektromagnetiske bølger fra elektronisk kommunikasjon og all utilsiktet utstråling av elektromagnetiske bølger som kan forstyrre elektronisk kommunikasjon (Ekomloven, 2003).

helheten innenfor IT sikkerhet eller ansvaret for sikringen av nettverk, driftssystemer for nettverk og kommunikasjonstjenester (Riksrevisjonen, 2005). Dette grensesnittet er vurdert i riksrevisjonsrapporten fra 2005.

Den andre utfordringen i forhold til en helhetlig tilnærming er tolkningen av JDs ansvar for kritisk IKT-infrastruktur, og JD praktiske rolle i en krisesituasjon (Riksrevisjonen, 2005, s. 8). Den andre utfordringen er sentral pga av JD samordningsrolle for samfunnssikkerheten i Norge (Riksrevisjonen, (2007-2008)).

Internett og tjenester på internett(sektoransvar) kontra helhetlig koordineringsansvar for informasjonssikkerhet

Den utfordringen jeg vil adressere her er grunnet de forskjellene som eksisterer i oppfatninger mellom aktørene. De har hver sine helheter, hvor FAD i tillegg opplever at SDs helhet bare er en mindre del av deres helhet. Helheten FAD ser begrenser seg dog til en forbyggende rolle og ramme i forhold til koordinering som oppgave. SD med sitt sektoransvar, beveger seg dypere ned i den teknologiske materien for informasjonssikkerhet knyttet til kommunikasjonsbærerne (Riksrevisjonen, 2009a, s. 32).

På den ene siden har IKT-avhengigheten og sårbarheten fått et større tverrsektorielt fokus, og dermed skjøvet både FADs forebyggende og JDs og krisehåndterende ansvar i forgrunnen (NOU, 2006:6, s. 56). Noe som har bidratt til fremveksten av KIS, NORSIS, VDI og NorCERT, og som igjen kan føre til at forebyggende tverrsektorielle oppgaver spiser seg inn på sektorenes operative ansvar. KIS og NORSIS er begge tilknyttet FAD, og gjennom disse etableringene utvidet FAD både sin koordinerende forebyggende rolle og sitt ansvar for å fange opp trusler mot IT-infrastrukturen. Det er derimot interessant at VDI som i utgangspunktet var et prosjekt knyttet til JD og PST, ble overført til FD og NSM i forbindelse med etableringen av NorCERT. En av konsekvensene av dette er at JDs samordningsansvar for samfunnssikkerhet og beredskap ikke lenger har VDI som et virkemiddel til sitt arbeid.

Undersøkelsen som riksrevisjonsrapporten bygger på viser at 1) etableringene av NORSIS (i pilotperioden var de benevnt med forkortelsen SIS) og VDI har klart å fange de logiske truslene mot IT-infrastrukturen. De har dog ikke klart å nå vesentlige mål for sin virksomhet som går utover ansvaret om å fange opp truslene mot IT-infrastrukturen (Riksrevisjonen, 2005, s. 9). 2) FAD har både få virkemidler knyttet til forebyggende IT-sikkerhet, og at de selv har avsatt beskjedne ressurser til denne oppgaven (Riksrevisjonen, 2005, s. 79). En kan

stille seg spørsmålet om forholdet mellom årsak og virkning i denne uttalelsen. Har FAD få virkemidler på grunn av at de skal kun ha en koordinerende rolle, eller har de satt av beskjedne ressurser fordi de har få virkemidler?

Det som er relevant for denne oppgaven er at den koordinerende rollen er i tråd med flere sentrale dokumenter laget både før og etter riksrevisjonsrapporten (FAD, 2007; NHD, et al., 2003; St.meld., nr. 17 (2006-2007)). Dette bekrefter en felles tolkning av ansvaret for den koordinerende oppgaven i det offentlige innen informasjonssikkerhet, mellom FAD, JD, SD og FD.

På den andre siden har vi også sett en konvergens i mellom tele-, data- og mediesektoren som tilsier at innholdet i SDs ansvarsportefølje har blitt mer kompleks (St.meld., nr. 17 (2006-2007), s. 30). Tidligere avgrensede løsninger og ansvarsforhold har blitt mer integrerte og mer diffuse. Konsekvensen av dette er att SDs ansvar har på et teknologisk nivå, allerede blitt et bredere fagområde hvor sårbarheten vil medføre tverrsektorielle utfordringer.

Hvis en ser SDs tilnærming til sitt ansvar opp mot FAD, kan vi utlede noen antagelser om hva som ligger bak SDs tilnærming til sitt sektorielle ansvar. Det kan virke sannsynlig at SD mener deres egen ansvarsavgrensning kan virke uhensiktsmessig i en helhetlig sammenheng. Èn av denne konvergensens effekt er å viske ut tidligere tradisjonelle skillelinjer i mellom teknologi, og de funksjoner som teknologien utfører. *”Når dei tekniske grensene forsvinn, oppstår det likevel utfordringar på politisk nivå. Regulering av TV var til dømes enkelt den gongen TV berre blei levert på éin måte. Det same gjeld telefoni, publiseringsverksemd m.v.” (St.meld., nr. 17 (2006-2007), s. 30).*

Konsekvensen av dette for SD er at det i dag ikke konsekvente skillelinjer, bilde og lyd leveres av mange forskjellige elektroniske komponenter. I tillegg er funksjoner som tidligere ble utført av personer med organisatorisk tilhørighet og ansvar, nå erstattet med elektroniske virkemidler hvor ansvaret rundt leveranseforholdene er diffuse i et privatisert telekommunikasjonsmarked.

Sett i forhold til den teknologiske konvergensen så har også dette påvirket FADs tilnærming til sitt tverrsektorielle ansvar. For når teknologiske informasjonssikkerhetstiltak blir tverrsektoriell IKT-politikk, så møttes flere parters ansvar og myndighet hverandre. Et av tiltakene fra FADs side som kan eksemplifisere deres økte fokus mot informasjonssikkerhetsteknologi er deres arbeid med PKI, elektronisk ID (eID) og elektronisk

signatur (e-signatur), (St.meld., nr. 17 (2006-2007), s. 117 & 119). FADs tilnærming til sitt tverrsektorielle ansvar er ikke upåvirket av kritikken om gjennomføringskapasitet og for lite samordnet politisk trykk på den digitale satsingen (Difi, 2011; Riksrevisjonen, 2005). Dette kan være noe av årsaken bak at flere av de store statsetatene nå krever en sterkere sentral styring av IKT-politikken hvor også de tverrdepartementale virkemidlene skal forbedres (Zachariassen, 2011).

JDs samordningsansvar for kritisk IKT infrastruktur og ansvar i krisesammenheng

Basert på riksrevisjonens undersøkelse 2005 om av myndighetenes arbeid med å sikre IT-infrastruktur ble det påpekt flere uklarheter rundt JDs samordningsansvar for samfunnssikkerhet og beredskap. Dette gjelder både i JDs forhold til sektorielt eid kritisk infrastruktur, IT-sikkerheten i den kritiske infrastrukturen og ansvarsfordeling i en krisesituasjon (Riksrevisjonen, 2005, s. 8). Riksrevisjonsrapporten sier også videre at selv om det er satt i gang flere tiltak, så har heller ikke myndighetene en oversikt over hva som er kritisk infrastruktur, og hvilke systemer denne består av (Riksrevisjonen, 2005, s. 9).

To av de tiltakene som var satt i gang, men ikke ferdigstilt ved riksrevisjonens gjennomgang var 1) infrastrukturvalget og 2) forskningsprogrammet BAS-5. Infrastrukturutvalget leverte sin utredning ”Når sikkerhet er viktigst” i april 2006 (NOU, 2006:6). Fra denne rapportens anbefalinger om ansvar for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner er det spesielt to forslag som er relevante. Forslagene er knyttet til tydeliggjøring av JDs rolle, og til forholdet i mellom NSM, PST og DSB. Forslagene møter altså her riksrevisjonens kritikk om uklarheter rundt JDs samordningsrolle.

I forlengelsen av infrastukturutvalgets utredning, er det her også viktig å nevne den stortingsmeldingen som kom i 2007, som het ”Eit informasjonssamfunn for alle”. I denne stortingsmeldingen blir riksrevisjonens funn, og de politiske kommentarene adressert. Det ble også presisert om samfunnskritisk IKT-infrastruktur, at dette er system som er helt nødvendig for å opprettholde kritiske funksjoner og som dekker grunnleggende behov i samfunnet (St.meld., nr. 17 (2006-2007), s. 146).

Til tross for myndighetenes oppfølging av riksrevisjonsrapporten, gikk også riksrevisjonen videre og gjennomførte en undersøkelse av JDs samordningsansvar for samfunnssikkerhet i 2007. Denne undersøkelsen viser at JDs rolle som samordningsdepartement oppleves av

enkelte departementer som noe utydelig, både i det forebyggende arbeidet men også som lederdepartement i en krisehåndteringssituasjon (Riksrevisjonen, (2007-2008), s. 9).

I den overordnede evalueringen av Sivil nasjonal øvelse (SNØ) 2008 Øvelse IKT-08 virker det som kritikken delvis gjentas ved at prinsipielle problemstillinger rundt ansvaret mellom fagdepartementer ikke er avklart (DSB, 2009, s. 8). I dette tilfellet gjaldt det en myndighetsavklaring i forhold til hvem som tar avgjørelsen vedrørende en nedstengning av et nettsted.

Den andre prosessen som var påstartet, men ikke avsluttet når riksrevisjonen gjorde sin undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur, var forskningsprosjektet BAS-5. En av hovedmålsettingene for dette prosjektet var å utvikle og anvende metodikk for identifisering og rangering av kritiske samfunnsfunksjoner (Fridheim & Hagen, 2007, s. 10). Dette prosjektet adresserer også delvis riksrevisjonsrapportens kritikk. Selv om prosjektet adresserer temaet, kritiserer riksrevisjonsrapporten at ikke prosjektet ble satt i gang før høsten 2004 (Riksrevisjonen, 2005, s. 9). JD svarer på denne kritikken med at det viste seg vanskelig å skaffe til veie økonomiske midler til prosjektet (Riksrevisjonen, 2005, s. 12).

I BAS-5 er det lagt et fokus på identifisering og rangering av kritiske samfunnsfunksjoner, slik at dette igjen kan danne grunnlag for en senere prioritering. For å finne, rangere og prioritere mellom kritiske samfunnsfunksjoner forutsetter dette at det foretas risiko- og sårbarhetsundersøkelser (RoS) på sektor- og virksomhetsnivå (Fridheim & Hagen, 2007, s. 18). Ansvaret for å følge opp RoS analyser i departementene er DSBs ansvar på vegne av JD. Rapporten fra riksrevisjonens undersøkelse vedrørende JD samordningsrolle, viser at DSBs funn ved deres tilsyn, genererer en oppfølgingsplan fra departementene. Oppfølgingsplanens tiltak er departementenes egne prioriteringer, da JD ikke har myndighet til å overprøve departementenes egne vurderinger. Når det gjelder informasjonssikkerhet har ikke DSB fagansvar for dette, men søker å inkludere informasjonssikkerhet inn i det nasjonale beredskapsplanverket (Riksrevisjonen, 2005, s. 34).

Etter riksrevisjonens undersøkelse vedrørende JD samordningsrolle har diskusjonen og avklaringen rundt kritisk IKT-infrastruktur og ansvar i krisesammenheng fortsatt. Et slikt eksempel er objektsikkerhetsforskriften. Først og fremst ligger ansvaret til denne forskriften hos FD og ikke JD, men da det er NSM som ivaretar denne vil jeg allikevel adressere dette da

NSM har en faglig rapporteringslinje også til JD. Den nye objektsikkerhetsforskriften har klarlagt sektoransvaret, men har den ikke på samme måte bidratt til å klarlegge forpliktelsene til samordningsansvaret (Objektsikkerhetsforskriften, 2010). Da NSM er underlagt FD kan mangelen på klarleggingen av samordningsansvaret til JD forstås. Det viser derimot at til tross for en faglig tilknytning, er ikke dette nok til at samordningsansvaret til JD klarer å påvirke forskrifter som gjelder på tvers av sektorene.

5.2.2 Akse 2: Offentlig kontra privat

Helhetlig tilnærming sett i forhold til offentlig og private aktører.

Hvordan løser så FAD og JD sitt helhetlige koordinerings og samordningsansvar? Offentlig og privat samarbeid skjer i dag i hele spektret fra forebyggende og koordinerende arbeid til krisehåndtering. I denne delen av oppgaven vil spektret for offentlig og privat samarbeid avgrenses til FADs koordineringsrolle for informasjonssikkerhet og JDs samordningsrolle for samfunnssikkerhet og beredskap.

Når det gjelder FADs koordineringsrolle og JDs samordningsrolle hviler begge på ansvarsprinsippet (Forsvars- og Justiskomiteen, Innst. S. nr. 9 (2002-2003), s. 7). I utøvelsen av ansvaret deres står to sentrale fora. Når det gjelder FAD, løser de sin koordineringsoppgave for informasjonssikkerhet i gjennom KIS, sammen med FD, JD og SD. Deres helhetlige tilnærming sett fra et aktørperspektiv er avgrenset til å adressere andre regelverksforvaltere og fagmyndighetsrepresentanter fra departementer, direktorater og tilsyn (Riksrevisjonen, 2005, s. 33). JDs samordningsrolle for samfunnssikkerhet og beredskap har også et eget tverrdepartementalt samordningsråd som ivaretar informasjons- og erfaringsutveksling for samfunnssikkerheten (St.prp., nr. 48 (2007-2008), s. 65). De viktigste aktørene som i praksis utøver samordningsrollen overfor andre myndigheter og private aktører i forhold til samfunnssikkerheten er DSB, PST og NSM.

Fagdepartementene har dog i tråd med ansvarsprinsippet et overordnet ansvar for å verne kritisk IKT-infrastruktur i sektoren. Men det er DSB som fører tilsyn mot departementene og de statlige virksomhetene på vegne av JD, det er PST som er i direkte dialog med NSR om

trusselbilde, og statlige og private virksomheter må søke NSM om etablering av nye graderte informasjonssystemer [20] (NSM, 2011a; NSR, 2011a; St.meld., nr. 22 (2007-2008)).

Utøvelsen av helhetlig tilnærming for FAD og JDs koordinerings og samordningsansvar begrenser seg derfor kun til andre offentlige aktører på lukkede arenaer. Denne praksisen har èn vesentlig svakhet fordi i en helhetlig tilnærming i Norge kommer vi ikke utenom de private aktørene. Det er flere grunner til dette, men ikke minst pga av privatiseringen av tele- og kraftforsyningsbransjen på 1990 og 2000 tallet. Praksisen med å lukke myndighetenes tilnærming kun til egne myndighetsinterne aktører samtidig som eierskap og ansvar har blitt privatisert kan det stilles spørsmålstegn ved. Historisk sett har også myndighetene selv vurdert dette noe forskjellig fra periode til periode etter bortfallet av den kalde krigen (Riksrevisjonen, 2005, s. 35). Men dersom private aktører rammes økonomisk av vedtak fattet i forum som KIS, hvor det private næringsliv ikke er representert vil dette påvirke forholdet i mellom det offentlige og private negativt (FAD, 2007, s. 5). Konsekvensen til at denne praksisen er alarmerende, er at det vil blant annet føre til større avstand mellom de offentlige og private aktørene, og skade legitimiteten til det offentlige. I en tid hvor økt ansvar er lagt til det private er ikke dette en ønsket utvikling.

En annen årsak til at en slik praksis er alarmerende er at samfunnssikkerheten nå vil inngå i bedriftsøkonomiske regnestykker, som igjen vil sette kostnader til samfunnssikkerhetsspørsmål opp mot bedriftsøkonomiske krav om overskudd.

Myndighetenes praksis om å utelukke det private næringsliv fra KIS og departementenes samordningsråd for samfunnssikkerhet samt vedtak om privatisering av telekommunikasjonsbransjen har medført en økt samfunnsmessig risiko.

5.2.3 Oppsummering av delkonklusjoner til Argument 1

FAD og SD har begge utvidet sitt ansvar basert på deres egen tolkning av deres ansvar og den teknologiske utviklingen. Disse utvidelsene har medført en overlapping av hva de anser som sitt ansvar. Det vil si at FADs helhetlige ansvar for IKT-politikk og forebyggende informasjonssikkerhet nå også tolkes til å inkludere konkrete teknologiske tiltak som ønskes implementert i statsforvaltningen generelt. SD på den annen side har utvidet sitt sektorielle

[20] I St.meld. nr. 17 er DSB ansvar for tilsyn i departementene presentert i Tabell 3.1.

ansvar som en konsekvens av den konvergensen en ser i den teknologiske utviklingen og den økte tverrsektorielle IKT-avhengigheten. Denne utvidelsen går utover det tradisjonelle sektorielle ansvaret og bidrar derfor til en mer diffust skille mellom et sektorielt og helhetlig ansvar.

Diskusjonen om innholdet i kritisk IKT-infrastruktur og rammene av samordningsrollen til JD er spørsmål som kontinuerlig er under vurdering. Et sett av arbeider har adressert dette, i tillegg har det også vært relevante øvelser, hendelser og revisjoner som viser at det fortsatt er behov for å se nærmere på dette (DSB, 2009; Nilsen, 2007; NOU, 2006:6; Riksrevisjonen, (2007-2008)). Det kan virke som om sektoransvaret i den senere tid har blitt bedre klarlagt, men at den helhetlige tilnærmingen og samordningsansvaret ikke har det på samme måte. En slik utvikling mener jeg styrker ansvarsprinsippet som styrende for nasjonale krisehåndteringen.

Private aktører regnes som partnere til staten i en helhetlig tilnærming knyttet til IT-sikkerhetssamarbeidet, i forbindelse med implementeringen av nye tiltak og når en evt. kostnadsnøkkel skal beregnes og betales. Men når nye strategier eller endringer til lov og regelverk vurderes, reduseres det helhetlige samarbeidet til et offentlig og tverrdepartementalt foretakende.

5.3 Argument 2): Med ansvar følger ikke myndighet eller ressurser

Krisehåndteringsprinsippene sier oss at den som har ansvaret fredstid, også skal ha dette under den operative krisehåndteringen (St.meld., nr. 17 (2006-2007), s. 161). Utgangspunktet her er at ingenting skal endres under krise, fordi det ligger en omforent tolkning til grunn om at den som har det daglige ansvaret har best forutsetning for å løse utfordringene i en krisesituasjon (Forsvars- og Justiskomiteen, Innst. S. nr. 9 (2002-2003), s. 6). I riksrevisjonenes undersøkelser samt i andre dokumenter kommer en stadig tilbake til utfordringene rundt ansvarsforhold og tolkning av ansvarsprinsippet i krisehåndteringen (Riksrevisjonen, 2005, s. 8; St.meld., nr. 22 (2007-2008), s. 10). Ved flere anledninger er det også påpekt at dette er på grunn av at det ikke følger myndighet eller ressurser med til ansvaret (NSR, 2011b; Riksrevisjonen, 2005; SD, 2009).

Oppgaven videre vil undersøke et par aspekter ved ansvarsprinsippet for å danne et grunnlag til å svare på i hvilken grad ansvarsprinsippet er implementert og styrende for myndighetene og virksomhetene i deres tilnærming til cybersikkerhetsarbeidet.

5.3.1 Ansvar & myndighet

Om legal myndighet[21]: I denne delen av oppgaven vil jeg fokusere på den legale eller formelle myndigheten, da jeg under Argument 3 vil belyse noen utfordringer knyttet til legitimitet.

Når det så gjelder formell myndighet så har de sentrale aktørene fått delegert et ansvar i form av lov og/eller forskrift. Politiloven og sikkerhetsloven kan være eksempler på dette (Politiloven, 1995; Sikkerhetsloven, 1998). Disse lovene gir henholdsvis politiet, PST og nasjonal sikkerhetsmyndighet et legalt utgangspunkt for sin tjeneste. Det utarbeides også forskrifter for å konkretisere legal myndighet. Forskrift kan etableres for å regulere samarbeid mellom aktører med legal myndighet. I tillegg kan instrukser pålegges i gjennom forskrift, eller utarbeides etter eget ønske av aktøren som har et spesifikt ansvar (FSA Instruks, 2010; JD, 2002; PST Instruks, 2005).

Til tross for at legal myndighet formaliserer både ansvarsavgrensning, presiserer hvordan ansvaret skal forvaltes og er fordelt, er ikke dette nok. Hvordan et ansvar forvaltes er den ansvarliges privilegium, men kan fort bli samarbeidspartneres frustrasjon dersom forvaltningsregimet ikke gjøres kjent.

- FAD og JD har ikke etablert et nødvendig forskrift til, eller instruks for sitt koordinerings- og samordningsansvar innen forebygging, IKT-beredskap og krisehåndtering.

- Det eksisterer i dag to overlappende regimer for å sikre beskyttelsen til informasjon som ved frigivelse kan medføre utfordringer til statssikkerheten.

1) Tilbake i 1994 ble en kongelig resolusjon som omhandlet samordningsfunksjonen og det generelle samordningsansvaret etablert. Med en slik generell tilnærming har JD, senere tid, utfordret utstrekningen av dette ansvaret sett i forhold til IKT-infrastruktur, IT-sikkerheten til disse systemene og deres rolle i krisehåndteringen. JD har søkt å avklare samordningsansvaret

[21] I den videre teksten vil begrepene legal myndighet og formell myndighet brukes synonymt.

de senere år (Fridheim & Hagen, 2007; NOU, 2006:6; St.meld., nr. 17 (2006-2007)). Men riksrevisjonen gav JD kritikk i forbindelse med BAS-5 hvor JD ikke valgte å prioritere dette arbeidet som var etterlyst helt tilbake til 2002 (Riksrevisjonen, 2005, s. 9). Når det gjelder den helhetlige tilnærmingen på tvers av fagdepartementene sier igjen infrastrukturutvalget følgende om det helhetlige ansvaret. *"Det foreligger [altså] ikke et «helhetsprinsipp» for* ***organiseringen*** *av sikkerhets- og beredskapsarbeidet som innebærer at et departement skal ivareta helheten på tvers av fagdepartementene*[22]*" (NOU, 2006:6, s. 52).*

Dette utsagnet bestrider ikke samordningsansvaret, men påpeker derimot at JD ikke har et ansvar for en helhetlig organisering, som går på tvers av fagdepartementenes ansvar. Selv om organiseringsansvaret i sikkerhets- og beredskapsarbeidet ikke er tillagt JD, er det etter min vurdering viktig at JD har en formening om hvordan et helhetsbilde bør se ut. Nettopp fordi hensikten bak et samordningsansvar er å kunne se forebyggende sikkerhetsarbeid og beredskap i alle sektorer samlet (Forsvars- og Justiskomiteen, Innst. S. nr. 9 (2002-2003), s. 25). På bakgrunn av dette at JD bør vurdere en videre formalisering av sitt samordningsansvar, og nivellere dette mot fagdepartementenes sektoransvar. Å unnlate å adressere dette er derfor en for defensiv tilnærming til samordningsansvaret som vil kunne få uønskede ringvirkninger.

Den overordnede evalueringen av Nasjonal Øvelse 2008/IKT øvelse-08 påpekte også at samordningsrollen var knyttet til det forebyggende arbeidet, og at det ikke er noen klar basis for at JD skal ha denne rollen operativt (DSB, 2009, s. 7 & 13).

Ansvarsprinsippet sier at ansvaret består uavhengig av fred, krise eller krig. Mener JD og DSB da at samordningsansvaret ikke skal ligge hos JD i krise som den gjør under normalsituasjon? En av utfordringene en får ved å ikke etablere en policy for hvordan en velger å løse sitt samordningsansvar, vil være økt usikkerhet blant ens samarbeidspartnere. Rolleforståelsen er viktig ikke bare innad i egen organisasjonen, men den har også en verdi overfor ens nærmeste samarbeidspartnere

Basert på utfordringene knyttet til ansvars- og oppgavefordeling, under normalsituasjon kontra krisesituasjon, er det nødvendig å se nærmere på myndighetsfordelingen. JD påpeker at ansvaret for kritisk infrastruktur følger ansvarsprinsippet og ikke er skilt ut som eget fagområde (Riksrevisjonen, 2005, s. 12).

[22] Klammen og uthevelsen i teksten er satt inn av forfatteren av denne oppgaven.

I forbindelse med samordningsansvaret har JD også ansvaret for at det føres tilsyn med at departementene gjennomfører internkontroll på sikkerhets- og beredskapsområdet. Som presentert tidligere i oppgaven utfører DSB tilsynet på vegne av JD, men er dog avgrenset slik at informasjonssikkerhetstilsyn skal løses i samarbeid med NSM. Her er det også viktig å huske NSMs begrensning i ansvarsområde som er knyttet til graderte informasjonssystemer (Sikkerhetsloven, 1998, s. §9). Sett i forhold til denne oppgavens tematikk er dette interessant da denne ansvarsfordelingen i praksis vil unnta departementenes ugraderte datasystemer fra JDs tilsynsansvar.

De sterke begrensningene i KIS` mandat kan også hevdes at er så sterke, at dette påkrever utarbeidelse av en instruks som kan regulere dette arbeidet.

2) Det eksisterer i dag to overlappende regimer for å sikre beskyttelsen til informasjon som ved frigivelse kan medføre utfordringer til statssikkerheten. Disse regimene har hjemmel i hver sin lov, og håndheves gjennom en forskrift og en kongelig resolusjon, i form av en instruks[23]. At det finnes to kontra ett regime kan ha flere funksjoner. På den ene side er behovene som er generert i gjennom Norges NATO-deltakelse viktig for at vi har en graderingsspesifikasjon som i stor grad sammenfaller innad i NATO. På den andre siden kan beskyttelsesinstruksens eksistens forsvares med at behovet for beskyttelse går utover de rent forsvars- og sikkerhetspolitiske interessene en stat har.

Det en også kan lese ut av at det eksisterer to regimer er at sektorinteresser har fått en fortsatt prioritering i forhold til en mer helhetlig tilnærming. Dersom en hadde hatt et regime som ivaretok både nasjonale og allianseforhold, ville en i større grad ha kunnet kalt dette en helhetlig tilnærming.

Men påvirker det cybersikkerheten at en har to overlappende regimer? Og hva gjør de egentlig overlappende? Sikkerhetsloven, sammen med informasjonssikkerhetsforskriften har som oppgave å være et redskap som kan bidra til et effektivt forsvar av informasjon som ved offentliggjøring kan skade for Norges eller dets alliertes sikkerhet (Sikkerhetsloven, 1998). Offentleglova derimot sier at informasjonen i utgangspunktet alltid skal være åpen og tilgjengelig, men at finnes noen muligheter for at dokumenter kan bli unntatt fra

[23] Dette er sikkerhetsloven, med forskrift om informasjonssikkerhet og offentleglova inkl. beskyttelsesinstruksen.

offentligheten. Noen av paragrafene som i forhold til denne oppgaven er relevante er §§20-21 utanriks-, forsvars- og tryggingsinteresser og §23 av omsyn til det offentlege sin forhandlingsposisjon (Offentleglova, 2006). Offentleglova bruker graderingsnivåene fra beskyttelsesinstruksen. Beskyttelsesinstruksen er en instruks i forskrifts form og omhandler de dokumenter som trenger beskyttelse av andre årsaker enn nevnt i sikkerhetsloven og dens forskrifter (Beskyttelsesinstruksen, 1972).

For denne oppgaven er det viktig her og se på overlappet i mellom offentlighetslovas unntaksbestemmelser, §§20-21 utanriks-, forsvars- og tryggingsinteresser og sikkerhetslovens formålsparagraf. Årsaken til at dette er viktig er at samme type informasjon har her to forskjellige graderingsregimer å forholde seg til. Mens ivaretakelsen av sikkerhetsloven gjøres av NSM, så blir ivaretakelsen av Beskyttelsesinstruksen ivaretatt av statsministerens kontor (SMK). Det forvaltningsorganet som utsteder dokumentet som er unntatt offentligheten er også ansvarlig for at dokumentet er beskyttet i henhold til instruksen (§5.1), (Beskyttelsesinstruksen, 1972).

Konsekvensen av dette setter store krav til forvaltningsenhetene, fordi der som NSM fungerer som veileder, godkjenner og tilsynsansvarlig i forbindelse med sikkerhetsloven, der har hvert enkelt forvaltningsorgan nå også dette ansvaret. I hvilken grad de klarer å ivareta dette ansvaret er vanskelig å si men i denne oppgaven har tidligere vist at forvaltningen har hatt store utfordringer knyttet til sin håndtering av beskyttet informasjon (Johansen, 2010c; Johansen & Overn, 2010).

I tillegg ønsker jeg her, på grunn av oppgavens tilnærming også å påpeke Offentleghetslova §23 som grunngir unntaket fra offentligheten med hensynet til det offentliges forhandlingsposisjon. Det vil si at staten har vurdert forhandlingsposisjoner som beskyttelsesverdig informasjon. Forhandlingsposisjoner er ikke nevnt i sikkerhetslovens bestemmelser. Dersom en ser i utredningen om rikets sikkerhet, har straffelovkommisjonen der argumentert for at forhandlingsposisjoner er en del av det som kan påvirke forholdet til andre stater og således bør inkluderes i den type informasjon som det skal være straffbart å

frigi (NOU, 2003:18, s. 101). Her kan det også være greit å presisere at forslaget om ny straffelov fra 2005, pr. 2011 ikke er i kraftsatt, men at dette er forventet gjennomført i 2012[24].

Statens forhandlingsposisjoner er sentrale utenriks- og sikkerhetspolitiske virkemidler i maktpolitiske og alliansepolitiske diskusjoner overfor enkeltstater eller internasjonale organisasjoner som for eksempel FN og NATO. Denne type forhandlingsposisjoner inngår både i NSMs definisjon av vitale nasjonale sikkerhetsinteressert og i den nye straffelovens tolkning av begrepet grunnleggende nasjonale interesser (NOU, 2003:18; NSM, 2009b). I tillegg er etterretningstrusselen mot statens forhandlingsposisjoner blant PSTs hovedkonklusjoner, når forhold som kan påvirke norsk sikkerhet og skade nasjonale interesser ble vurdert i 2011 (PST, 2011b).

Men vil forhandlingsposisjoner som er viktige for 1) rikets sikkerhet og vitale nasjonale sikkerhetsinteresser eller 2) utenriks-, forsvars- og sikkerhetsinteresser, bli gradert etter sikkerhetsloven eller beskyttelsesinstruksens graderingsmuligheter? Et slikt overlapp er er uheldig og potensielt en trussel for informasjonssikkerheten. Dersom du har to graderingsregimer og to aktører som ivaretar veiledningen, godkjenningen og tilsynet med beskyttelsen/sikringen[25]. Så er det en fare for at den som sitter med informasjonen som skal beskyttes/sikres, velger minste motstands veg når han/hun som informasjonseier skal vurdere hvilke krav, som skal etterleves i den enkelte sak.

Delkonklusjon ansvar og myndighet

Drøftingen viser at den formelle myndigheten gitt instanser under sektordepartementene både er godt hjemlet, tolket og forstått i eget departement og andre departement. Tverrsektoriellt ansvar som FADs koordinerende ansvar for informasjonssikkerhet og JDs samordningsansvar for samfunnssikkerhet og beredskap, er ikke i samme grad verken tolket eller forstått av eget eller andre departement. Kritikken reist mot disse i gjennom riksrevisjonsrapporten fra 2005 generelt, og JD spesielt i den overordnede evalueringen av SNØ 2008/Øvelse IKT-08 viser dette (DSB, 2009, s. 4; Riksrevisjonen, 2005, s. 11). På bakgrunn av dette drar jeg slutningen

[24] Iverksettelsen av ny straffelov avhenger av en fornyelse av politiets IT-systemer (Riksrevisjonen, (2007-2008), s. 61).

[25] Med to aktører som representanter for de to regimene menes NSM på den ene siden, mens forvaltningsenheten som skal utstede dokumentet er den andre representanten.

om at ansvarsprinsippet ser mer gjennomarbeidet ut en den helhetlige tilnærmingen når en ser på myndighetsdelen.

5.3.2 Ansvar, ressurser og prioritering

Ansvar skaper behov for ressurser og evne til å prioritere. I de senere år har det skjedd mye relevant når ansvar, ressurser og prioriteringsegenskaper skal sees nærmere på. På den ene siden har en prosjektene og organisasjonsetableringene (VDI, NorCERT m.fl.), og på den andre siden så har noen sentrale rammebetingelser også endret seg, som for eksempel eierskapsforhold i telekommunikasjonsbransjen. Ressursene er virkemidler som objekteier og/eller virksomhet har, og som i større eller mindre grad prioriteres til å løse de oppgavene som følger med et sikkerhets- og beredskapsansvar knyttet til virksomhetenes behov for informasjonsbeskyttelse. Når trusselbildet har endret seg så har også ressursbehovet endret seg. Har endringene hos myndighetene bidratt til å forsterke eller redusere den helhetlige tilnærmingen til fordel for sektorinteressene?

Ressursendringer som har forsterket eller redusert den helhetlige tilnærmingen eller sektorinteressene

Justissektoren

Justissektoren har gjennomført noen omorganiseringer og omprioriteringer for å møte kravet om en mer helhetlig tilnærming. Med tanke på JDs samordningsrolle for samfunnssikkerhet og beredskap, er det også naturlig at dette har fått en sentral plass i deres reformer i de siste 10 årene. Noen av omorganiseringene og prioriteringsendringene som for JD har bidratt til en mer helhetlig tilnærming innen denne oppgavens tematikk er 1) etableringen av DSB og 2) etableringen av den faglige rapporteringskanalen fra NSM.

1) Etableringen av DSB fikk satt JDs samfunnssikkerhetsansvar på kartet og har utvilsomt bidratt til en mer helhetlig tilnærming. Det mest fremtredende ved DSBs i forhold til denne oppgaven er deres tilsynsrolle overfor statsforvaltningen, som utøves på vegne av JD (NOU, 2006:6, s. 53). Deres årlige arbeid med å lage nasjonale sårbarhets- og beredskapsrapporter og ansvaret de tok på seg som leder av Sivil nasjonal øvelse (SNØ) 2008 og Øvelse IKT-08 (DSB, 2005, 2009).

2) Etableringen av den faglige rapporteringskanalen fra NSM sikrer den tverrdepartementale dialogen mellom JD og FD. Dette er dog ikke det eneste båndet i mellom disse to departementene, men kan representere det nære samarbeidet som er i mellom de to sikkerhetsdepartementene. For å eksemplifisere dette samarbeidet vil jeg vise til arbeidet knyttet til VDI (NorCERT, 2011). Et annet eksempel er Koordineringsgruppen for IKT-risikobildet, bestående av PST, NSM og Etterretningstjenesten som stod bak bakgrunnsnotatet til NSMs cybersikkerhetsstrategi (NSM, PST, & Etterretningstjenesten, 2010).

Til tross for at flere tiltak knyttet til en helhetlig tilnærming er gjennomført har det kommet kritikk til JD på flere områder. Kritikken er både knyttet til JDs samordningsrolle, og arbeidet tilknyttet IKT-infrastruktur. Når det gjelder deres samordningsrolle viser funnene fra riksrevisjonen og DSB departementstilsyn at andre departementer opplever at JDs samordningsrolle er utydelig og lite konkret (DSB, 2005; Riksrevisjonen, (2007-2008)). Til tross for at samordningsansvar søkes klarlagt i stortingsmeldingen ”Eit informasjonssamfunn for alle”, så blir også samordningsansvarets uklarheter adressert i den overordnede evalueringen av SNØ 2008/Øvelse IKT-08 (DSB, 2009, s. 9; St.meld., nr. 17 (2006-2007), ss. 160-161). At samordningsutfordringene også er et tema i dag bekreftes ved at dette er listet opp som en av hovedmålene i cybersikkerhetsstrategien som NSM har lagt frem (NSM, 2009a, s. 13).
Kritikken som riksrevisjonen har reist mot JDs håndtering av arbeidet med IKT-infrastruktur er også på sin plass. Nedprioriteringen av kompetanseutviklingen om- og manglende avgrensning av hva som er samfunnskritisk IT-infrastruktur reduserer JDs evne til å kunne utføre sin samordningsrolle.

Noen av omorganiseringene og prioriteringsendringene i JD har bidratt mer til å ivareta sektorinteressene enn en helhetlig tilnærming. Det er innen denne oppgavens tematikk to områder som har styrket JDs sektorinteresser spesielt det gjelder JDs interne omorganiseringer og prioriteringen av samarbeidet med NSR.

Når det gjelder JDs interne reformer vil jeg spesielt peke på organisasjons og prioriteringsendringene knyttet til PST og PDMT. Endringene og omprioriteringene i PST har fått vokse frem under den nye trusselsituasjonen etter bortfallet av den kalde krigen (PST, 2004, s. 4). Når en ser på hensikten bak omorganiseringen av PST var dette å forbedre samvirket med politiet og de andre sikkerhetstjenestene (St.meld., nr. 42 (2004-2005), s. 22).

PDMT som ble etablert i 2004 i tråd med Politireform 2000 hadde et fokus på å forbedre effekten av ressursbruken i justissektoren (St.meld., nr. 22 (2000-2001), s. 3).

NSR har som formål å forebygge kriminalitet i og mot næringslivet. JDs Dette samarbeidet oppleves som så positivt fra JDs side at det har blitt foreslått å etablere et femårig prøveprosjekt med en forsterket samarbeidsstruktur, med oppstart i 2011.

JD styrking av sitt sektorielle ansvar har heller ikke vært uten kritiske tilbakemeldinger. Til tross for JDs styrking har EOS utvalget påpekt de økende utfordringene PST har i forbindelse med konsekvensene av teknologiutviklingen (EOS, 2002, s. 3). Dette gjelder blant annet kommunikasjonsavlytting i en tid hvor en har en konvergens i tele-, data- og mediesektoren (St.meld., nr. 17 (2006-2007), s. 30). Disse utfordringene har både en politisk og en teknologisk side. De politiske utfordringene har blitt søkt løst i gjennom å etablere både nye metoder, rutiner og formaliserte samarbeid (JD, 2002; PST Instruks, 2005; Samarbeidsinstruksen, 2006; St.meld., nr. 42 (2004-2005)). I tillegg til dette har de teknologiske utfordringene blitt adressert av PDMT. Dessverre har PDMT etter sin etablering blitt kritisert både som anskaffende myndighet og ansvarlig IKT forvalter i justissektoren i en årrekke (Riksrevisjonen, 2008, s. 142). Det er derfor ikke overraskende at riksrevisjonen understreker viktigheten av å prioritere det å få etablert stabile og sikre driftsløsninger for IKT i politi- og lensmannsetaten. Riksrevisjonen har dog bemerket i revisjonen av budsjettåret 2009 at politidirektoratet nå har prioritert IKT forvaltningen (Riksrevisjonen, 2009b; 2010, s. 168).

I tillegg til den kritikken som er reist både i forhold til JDs helhetlige tilnærming og sektorielle styrking er det to elementer som jeg mener også bør komme frem i lyset. Det første gjelder tilsyn i forvaltningen som i utgangspunktet er lagt til DSB, men som i informasjonssikkerhetssammenheng løses i samarbeid med NSM. Pga av begrensningene som ligger i NSMs mandat knyttet til sikkerhetsgradert informasjon, så bør en løsning for periodisk ekstern revisjon av statsforvaltningens ugraderte datasystemer etableres. For det andre bør det prinsipielle ved JDs samarbeid med NSR også kunne benyttes overfor statsforvaltningen, der dette er relevant.

Delkonklusjon justissektoren

Justissektoren har hatt store utfordringer både i forhold til teknologiutviklingen, ny trusselsituasjon og behov for reformer i egen organisasjon. Til tross for dette har omorganiseringer og prioritetsendringer bidratt til å styrke både deres evne til helhetlig tilnærming og deres eget sektorielle ansvar. Kritikken som er reist mot både deres samordningsevne og sektoransvar mener jeg viser at JD i størst grad lar ansvarsprinsippet generelt sett være styrende. Når en ser på tilnærmingen til cybersikkerhet kan det derimot se ut til at den helhetlige tilnærmingen er mer fremtredende.

Fornyings- administrasjons- og kirkedepartementet inkl. KIS, DSS & NORSIS

FAD har i utgangspunktet allerede et helhetlig ansvar, både i forbindelse med myndighetenes IKT-politikk men også for koordineringen av informasjonssikkerhet overfor regelverksforvaltere og tilsynsmyndigheter i staten. Koordineringsgruppa for informasjonssikkerhet (KIS), etablert i 2004, brukes som er en arena for myndighetsintern dialog. KIS kan ta opp spørsmål som omfatter alt fra alminnelig IT-sikkerhet til spørsmål knyttet til rikets sikkerhet (Riksrevisjonen, 2005, s. 35). KIS er også ansvarlig for utarbeidelse av de nasjonale retningslinjene for å styrke informasjonssikkerheten (FAD, 2007). Utover etablering av KIS er NORSIS også et positivt bidrag som i FADs helhetlige tilnærming. NORSIS var i utgangspunktet et midlertidig prosjekt for å fange opp IKT-trusler, men dette endret seg etter vedtaket om et permanent NORSIS relokalisert på Gjøvik. NORSIS ble da endel av et nasjonalt konsept for varsling og rådgivning for informasjonssikkerhet (Riksrevisjonen, 2005, s. 13). I hovedtrekk ligger nå oppgavene mer på et forebyggende nivå enn tidligere (St.meld., nr. 17 (2006-2007), s. 162).

Det er dog rettet kritikk til både FAD, KIS og NORSIS. Med utgangspunkt i ansvarsprinsippet og i KIS sitt begrensede mandat, er nettopp gjennomføringskapasiteten til KIS et problem. Dette gjelder blant annet den nasjonale strategien for informasjonssikkerhet, og gjennomføringen av tiltak fra denne. Riksrevisjonens undersøkelse påpeker her at det mangler gode handlingsplaner for tiltakene (NHD, et al., 2003; Riksrevisjonen, 2005, s. 79). Gjennomføringskapasiteten til KIS kan også vises ved en annen tverrsektoriell utfordring som ser ut til å ha evig liv. Samordning av regelverk for informasjonssikkerhet ble tidlig adressert som en stor utfordring det skulle arbeides med i gjennom den første nasjonale strategien for informasjonssikkerhet (NHD, et al., 2003, s. 4). Riksrevisjonsrapporten fra 2005, nevner ikke dette tiltaket spesifikt som et av de tiltak som ikke har blitt ferdigstilt. Dog kan det være

interessant å se at KIS i mai 2006 tar opp dette igjen og etablerer Samarbeidsgruppen for regelverk og informasjonssikkerhet (SARI). Sluttleveransen til dette prosjektet kommer i 2007 og konkluderer med at det kan virke som at gjeldende regelverk ikke er konsekvent i sin språkbruk. Noe som skader en enhetlig tolkning, som igjen da ikke vil danne grunnlag for en felles forståelse på tvers av sektorene (Eriksen, 2007, s. 26). Riksrevisjonens egen oppfølging av forvaltningsrevisjonene, fra 2009-2010. Viser at en av årsakene bak den manglende fremdriften i arbeidet med it-sikkerhet var manglende samordning av regelverket (Riksrevisjonen, 2009a). Riksrevisjonsrapporten kritiserer også NORSIS for at de ikke har nådd vesentlig mål for sin virksomhet (Riksrevisjonen, 2005, s. 9).

Et tankekors knyttet til FADs ansvar for å initiere tiltak av tverrsektoriell karakter, er at FAD ikke hadde en mer markert rolle i den overordende evalueringen av Øvelse SNØ og Øvelse IKT-08 (DSB, 2009, s. 5). Dersom FAD skal kunne utøve sitt arbeid med å adressere tverrsektorielle tiltak, så mener jeg det er helt nødvendig at de er en aktiv part i denne formen for arbeid.

FADs sektorielle interesser knytter seg hovedsaklig til ansvarsdefinisjonen til DSS som blant annet er å beskytte informasjon som PST i gjennom hele 2000 tallet har advart om at det drives ulovlig etterretningsvirksomhet i mot. *”Etterretningsvirksomheten er rettet mot både statlige og private aktører involvert i politiske beslutningsprosesser, og aktører som behandler spørsmål relatert til blant annet norsk økonomi-, ressurs- og sikkerhetspolitikk” (PST, 2007, s. 3).*

Tidligere er det vist til hendelser i den senere tid som har aktualisert PSTs trusselvurderinger (Johansen, 2010c; Johansen & Overn, 2010). Og den seneste årsrapporten fra NSM bekrefter også at spionasjeangrepene mot departementene var en av de alvorligste IKT-hendelsene (NSM, 2011b). Riksrevisjonen gjorde dog i sin årlige revisjon i 2009 en revisjon av arbeidet med informasjonssikkerhet i FAD og DSS. Her får både FAD og DSS kritikk for at det ikke er gjort en systematisk vurdering av kritisk IKT-infrastruktur for hele sektoren. Dette til tross for at ansvarsprinsippet skulle være gjeldende og at alle sektorer og fagdepartement skulle gjøre dette i henhold til retningslinjene for å styrke informasjonssikkerheten 2007-2010. Dog ble Depnett/U i DSS vurdert som kritisk for den operative evnen i regjeringskvartalet, selv om departementets vurdering ikke er dokumentert (Riksrevisjonen, 2010, s. 118).

Delkonklusjoner FAD inkl. KIS, DSS og NORSIS

FAD har i utgangspunktet en helhetlig tilnærming i sitt daglige arbeid med blant annet IKT-politikk for myndighetene og koordineringsansvaret for informasjonssikkerhetsarbeidet. Dette kan ha medført at forholdet til det å arbeide med helhetlige tilnærminger er annerledes en for eksempel JDs samordningsansvar, ikke helt ulikt den type ansvar FAD har hatt siden etablering. FAD ser ut til på den ene siden å styres i større grad til en helhetlig tilnærming på politisk og strategisk nivå. Mens de på den annen side styres av ansvarsprinsippet i den praktiske gjennomføringen av politikken. I FAD eller i KIS ligger det ikke et mandat sterkt nok til å overstyre ansvarsprinsippet i dag, noe som igjen tilsier at tiltakene står og faller med den prioritering som den blir gitt innen sin sektor.

Samferdselsdepartementet og Post og Teletilsynet

SD er et fag- og sektor departement, og de har ingen helhetlige eller samordnende roller utenfor sin egen sektor. Det kan derfor virke urimelig å skulle vurdere deres forhold til helhetlig tilnærming og ansvarsprinsipp. SD som sektordepartement måles etter sektorspesifikke oppgaver og en kan ikke forvente annet et at ansvarsprinsippet i større grad en helhetlige tilnærminger vil være styrende for SD. Det er også grunn til å tro at SDs forhold til ansvarsprinsippet er preget av at deres sektor har vært i gjennom store endringer knyttet til deres rammebetingelser. Sett i forhold til de andre aktørene nevnt i denne drøftingen, så er telekommunikasjonsbransjen i stor grad privatisert.

Gjennom å fokusere på utarbeidelser av krav, samt administrative og økonomisk virkemidler overfor til de private aktørene vil SD, kunne vise at de har et aktivt forhold til sitt strategiske ansvar. Et aktivt forhold til ansvarsprinsippet vil derimot kreve at myndighetene evner å følge opp de private aktørenes ansvar og plikter. Alle disse oppgavene er for øvrig lagt til PT, men prioriteringen av hva som vektlegges av organisasjonen (St.meld., nr. 47 (2000-2001), s. 32).

På grunn av sektorens fagretning har SD en plass i KIS sammen med FAD, JD og FD. Her er de en sentral del av myndighetens helhetlige tilnærming til informasjonssikkerhet. Gjennom deres rolle i KIS er de også medansvarlig til utarbeidelsen av de nasjonale retningslinjene for styrking av informasjonssikkerheten (FAD, 2007). Før dette, i 2003 ble også Nasjonal strategi for informasjonssikkerhet initiert og laget av Nærings- og handelsdepartementet men det ferske PT, underlagt SD, ble satt som gjennomføringsansvarlig på flere tiltak (NHD, et al., 2003). Dersom en går enda lenger tilbake vil en også se i St.meld. nr. 47 om ”Telesikkerhet

og -beredskap i et telemarked med fri konkurranse", at det er skissert flere sektorielle tiltak for å redusere den tverrsektorielle sårbarheten som avhengigheten til telenettene har skapt (St.meld., nr. 47 (2000-2001), s. 3).

En noe annen måte å se helhetlig tilnærming på er å vurdere deres tilnærming i forhold til de endrede rammebetingelsene sektoren har sett de senere år som for eksempel i det økte private eierskapet til ressursene i telekommunikasjonssektoren (St.meld., nr. 47 (2000-2001), s. 3). I 1999 etablerte SD, med PT som ansvarlig, prosjektet Teleberedskap i fritt konkurransemarked (TIFKOM). Prosjektet innhentet informasjon om telesikkerhet- og beredskap for å utvikle løsninger som kunne fungere i Norge. Funnene i dette prosjektet samsvarer med funnene, om behov for å styrke robustheten i de norske telenettene, i FFIs BAS-2 prosjekt om sårbarhet i offentlig telekommunikasjon. Videre omhandler TIFKOM rapporten krav som må stilles til de nye private markedsaktørene (St.meld., nr. 47 (2000-2001), s. 84). SD og PT står her ansvarlig for et sektororientert forskningsoppdrag hvor konklusjonene samsvarer med tidligere funn fra FFIs forskningsprogram "Beskyttelse av samfunnet", som sannsynligvis i større grad kan hevde å ha en mer helhetlig tilnærming i sitt arbeid.

Under riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur, kom kritikken både mot SD og PT. Undersøkelsen viste dessverre at kun et fåtall av tiltakene som var foreslått i stortingsmeldingen "Telesikkerhet og -beredskap i et telemarked med fri konkurranse" fra 2001, var gjennomført og at resten var under utredning (St.meld., nr. 47 (2000-2001)). Videre viste den også at SD ikke hadde revidert sine styringssignaler til Post- og teletilsynet. Eller at det har vært utviklet plan- og styringsdokumenter angående tiltakene som var foreslått i stortingsmeldingen. Ikke bare viser undersøkelsen til Riksrevisjonen at finansieringen til de respektive tiltakene ikke er avklart. Men det ser også ut til å være en uenighet mellom SD og PT, om hvor viktige de finansielle vs tekniske og kapasitetsmessige ressursene har vært for implementering av tiltakene fra stortingsmeldingen (Riksrevisjonen, 2005, ss. 14 & 73-74). PT hadde heller ikke utarbeidet planer for de foreslåtte tiltakene (Riksrevisjonen, 2005, s. 11). I tillegg til dette kom det, i forbindelse med den politiske gjennomgangen av riksrevisjonens funn også kritikk fra Kontroll og konstitusjonskomiteen.

> *At bare et fåtall av de vedtatte tiltak i St.meld. nr. 47 (2000-2001) Telesikkerhet og -beredskap i et telemarked med fri konkurranse er satt ut i livet, er etter komiteens syn sterkt å beklage og avdekker en* ***manglende respekt for Stortingets vedtak***[26]***.***
>
> *(Kontroll- og konstitusjonskomiteen, Innst. S. nr. 85 (2005-2006), s. 11)*

Det pekes på i Innst. S. nr. 9 (2002–2003) at koordinering og ansvarsklargjøring vil være helt nødvendig innenfor IT-sikkerhetsarbeidet. I forbindelse med arbeidet om å koordinere og klarlegge ansvarer for internett, kritiserte også riksrevisjonen dette arbeidet (Riksrevisjonen, 2005, s. 8).

> *"For å oppnå nødvendig robusthet og sikkerhet i tele og IT-systemene, må det* ***iverksettes effektive tiltak*** *for å forebygge, begrense eller håndtere kriser og andre uønskede hendelser så vel i fredstid som i en beredskaps- eller krisesituasjon. Det må med andre ord* ***etableres både planer og gjennomføres faktiske tiltak*** *som er gode nok til å kunne møte forhold som innebærer* ***ekstraordinær risiko****, for eksempel påkjenninger i forbindelse med sikkerhetspolitiske kriser og krig. Det er slike tiltak som inkluderes i begrepet teleberedskap*[27]*" (Samferdselsskomiteen, Innst. S. nr. 329 (2000-2001), s. 2).*

En forklarende faktor til PTs utfordringer og som kanskje også ligger bak deres prioriteringsvalg som har resultert i kritikk fra riksrevisjonen er omorganiseringen i PT i 2001. Omorganiseringen kom etter stortingsmeldingen om telesikkerhet, og medførte at det ble etablert en egen seksjon for telesikkerhet- og beredskap (St.meld., nr. 47 (2000-2001)). Relokaliseringen av PT som ble vedtatt i 2003 og iverksatt fra 2007 har påvirket ressurssituasjonen. FAD gjennom Asplan Viak fikk gjennomført en evaluering av denne relokaliseringen i 2009. PT har i tillegg til relokaliseringen også vært i gjennom noen interne omorganiseringer og også fått tilført noen flere oppgaver (Haaland Eriksen, 2009, s. 19). Antall ansatte har i perioden 2001-2009 gått i bølger og daler. På det meste har de vært 158-9 mens det i 2009 var nede i 130. Tendensen viser en nedadgående kurve i antall ansatte (Haaland Eriksen, 2009, s. 26). Undersøkelsen viser også at bransjen opplever at PT mangler erfaring på en del områder, men at kunnskapsnivået i 2009 igjen er på vei opp. I denne nesten ti år lange perioden har avskallingen av personell ført til at ved årskiftet 2008/2009 er det igjen kun 15 % av personalet fra årskiftet 2001-2002.

---

[26] Uthevelsene er forfatterens egne.

[27] Uthevelsene er forfatterens egne.

Undersøkelsen konkluderer med at store utskiftninger som PT har opplevd i perioden har gitt en stor ekstrabelastning for organisasjonen og deres medarbeidere (Haaland Eriksen, 2009, s. 28). Et slikt internt fokus for organisasjonen kan også være årsaken bak noe av den kritikken som Riksrevisjonen kommer med. Dette mener jeg også kan føre til at PTs ansvar i den nasjonale koordineringen av varsling, rådgivning og assistanse for informasjonssikkerhet ikke blir ivaretatt (DSB, 2009, s. 8; Riksrevisjonen, 2009a, s. 34).

Avslutningsvis kan det være interessant å se på PTs høringsuttalelse til cybersikkerhetsstrategiens tiltak nr. 15 om etablering av sektorvise CSIRT'er. Denne uttalelsen sier noe om den operative kapasiteten i sektoren til å sikre IT-infrastrukturen. Og sier også noe om ressursbruken, for PT vs NorCERT og evt de private eierne i telekommunikasjonsbransjen.

> *"For sektormyndigheter som ikke eier egen infrastruktur, bør det utredes nærmere hvilken nytte det har å opprette en CSIRT for sektoren og hvordan slike CSIRTer eventuelt bør organisere. En CSIRT for ekomsektoren vil etter PTs vurdering representere en betydelig andel av det ansvarsområdet NorCERT dekker i dag" (PT, 2010, s. 5).*

Delkonklusjoner Samferdselsdepartementet

Riksrevisjonen kritiserer SD for deres tilnærming til og gjennomføring av tiltak som skulle ivareta overordnede tverrsektorielle behov både, som "ansvarsavklaring rundt internett". SD kritiseres også i forhold til de sektorspesifikke målsetninger, og den manglende fremdriften på disse. Dette får meg til å konkludere med at riksrevisjonen legger til grunn at SD i liten grad har tilnærmet seg de helhetlige eller sektorspesifikke utfordringene må en strategisk eller løsningsorientert måte. Noe som tilsier at en ikke kan gjøre en enhetlig konkludering om hvorvidt SD føler seg mer bundet av helhetlige eller sektorielle krav eller utfordringer.

Forsvarssektoren: Nasjonal sikkerhetsmyndighet (NSM) inkl VDI & NorCERT

På samme måte som JD, er FD et sikkerhetsdepartement. Og på samme måte som SD har FD sektorielle virkemidler for å løse sitt ansvar. Når JD har et samordningsansvar for samfunnssikkerhet og beredskap i fredstid, er FDs ledende arbeid med sektorovergripende sikkerhetsutfordringer først et tema i en krigssituasjon. Denne oppgaven er avgrenset til fredstid og ser dermed på FD, og deres rolle i fredstid.

NSM har en sektorspesifikk rolle i det forebyggende arbeidet med å sikre nasjonal kritisk IKT-infrastruktur, sikkerhetsgraderte objekter og informasjon gjennom å være regelverksforvalter, godkjennings- og tilsynsmyndighet. I tillegg har NSM også en viktig rolle i myndighetens helhetlige tilnærming til cybersikkerhet gjennom deltakelsen i og sekreteriatsfunksjonen i KIS. I tillegg utøves det en helhetlig tilnærming i gjennom det offentlig/private samarbeidet i VDI som er lagt til NorCERT.

FD og NSMs sektorspesifikke rolle og forholdet til ansvarsprinsippet

1) Som regelverksforvalter

Som regelverksforvalter sitter man i en unik situasjon hvor en har mulighet til å forme regelverk på en måte som kan virke både helhetlig samtidig som viktige prinsipp ivaretas. Til tross for den muligheten er en også avgrenset til å adressere kun en del av en større helhet, som sektormyndighet. Grensesnittet mot andre lovverk og prosessene frem til etablering av nye lovverk blir derfor sentrale.

FD sendte ut en pressemelding tidligere dette år om at Sikkerhetsloven skulle gjennomgå en helhetlig evaluering med representanter fra sikkerhetssektoren (JD og FD) for å vurdere om det er et behov for en revisjon av sikkerhetsloven (FD, 2011). Det er positivt at en slik helhetlig evaluering vil bli gjennomført, men det er et par interessante forhold i FDs tilnærming her som bør vurderes nærmere. Først er det bruken av begrepet helhetlig i en sikkerhetssektor avgrenset betydning. Norge har som vist tidligere to regimer for sikring av informasjon, sikkerhetsloven som definerer den ene delen forvaltes av NSM. Med avgrensningen til sikkerhetsloven mister NSM kontrollen med og oversikten over den informasjonen som ønskes beskyttet, men som faller utenfor sikkerhetslovens domene

I tillegg er det en av konsekvensene av en slik avgrensning. Departementet som er ansvarlig for koordineringen av informasjonssikkerhet er ikke representert, noe jeg mener er uheldig. Årsaken til det er at denne fremgangsmåten vil kunne medføre at en kun ser Sikkerhetsloven i et selvstendig perspektiv, og får en evaluering som i mindre grad ser Sikkerhetsloven som et av flere lovverk som bygger opp om hverandre i et mer helhetlig perspektiv. I en slik evaluering må en blant annet også gjøre en vurdering av straffelovene (både ny og gammel), siden den nye ennå ikke er satt i kraft (Straffeloven, 1902, 2005). Forholdet til Offentleglova og beskyttelsesinstruksen er relevante grensesnitt, spesielt etter hendelsene og funnene gjort i

ettertid av de digitale angrepene mot statsforvaltningens ugraderte nett (Johansen, 2010c; NSM, 2011b; Riksrevisjonen, 2010).

FD & NSM kritiseres også av riksrevisjonens ved at det på tidspunktet for riksrevisjonsapporten ikke var klart hva som skulle defineres som skjermingsverdige objekter i henhold til sikkerhetsloven (Riksrevisjonen, 2005, s. 9). Denne kritikken henspeiler blant annet på det langvarige fraværet av Forskrift om objektsikkerhet[28].

FD påpeker i sitt svar til riksrevisjonen at en ny forskrift om objektsikkerhet kun vil virke forebyggende for sektorene, og dermed ikke vil ha noen betydning for håndteringen av eventuelle kriser. Det er sektorlovgivningen som er den lovgivning som setter nærmere krav til beskyttelse av skjermingsverdige objekt. FD ser også at konsekvensen av manglende forskrifter også viser en mangelfull helhetlig tilnærming til forebyggende tiltak (Riksrevisjonen, 2005, s. 16).

Dersom vi ser nærmere på denne objektsikkerhetsforskriften og høringsuttalelser til denne så vil jeg hevde følgende. 1) Forskriften søker å konkretisere ansvarsprinsippet overfor sektormyndighetene og objekteier. 2) At den som en policy for hvordan NSM tolker og vil gjennomføre sitt forebyggende og sektorovergripende ansvar ser ut til i mindre grad å være forpliktende. Disse påstandene vil jeg begrunne med forskriftens fokus på a) å tidlig avklare forholdet til sektorlovgivningen og sektormyndighetene i §1-3, mens forholdet til det forebyggende sektorovergripende ansvar ikke avklares. b) Hvis en ser i § 4-3, andre ledd vil en også se at til tross for at det tidligere er sagt at sektormyndighetene og sektorlovgivningen vil være styrende. Så kan NSM som tilsynsmyndighet overprøve et slikt arbeid basert på en overordnet vurdering av om tiltakene er harmonisert på tvers av sektorene (Objektsikkerhetsforskriften, 2010).

Det er også noen andre grunnleggende utfordringer med en evt praktisering av ansvarsprinsippet og forskrift om objektsikkerhet. 1) Vil en konkurranseutsatt objekteier innen f.eks, telekommunikasjonsbransjen, anbefale endringer som medfører vesentlige større driftskostnader for sin organisasjon? 2) Og vil et sektordepartement gå inn å anbefale endringer for en eller flere aktører i en konkurranseutsatt næring? Dette er noen av NSRs og

[28] Sikkerhetsloven ble satt i kraft i 2001, men forskrift om objektsikkerhet ble ikke satt i kraft før i 2011.

PTs kommentarer i deres høringsuttalelser til den nye objektsikkerhetsforskriften (NSR, 2009; PT, 2009).

Til tross for fraværet av Forskrift for objektsikkerhet har mye arbeid utenfor NSM blitt lagt ned i å klargjøre problemstillinger og utfordringer. BAS-5 prosessen hos FFI gikk delvis parallelt med infrastrukturutvalgets prosess som var satt ned av JD. Men dette var igjen to prosesser som begge ble forsinket. BAS-5 fikk en forsinket oppstart grunnet manglende finansiering, mens Infrastrukturutvalget fikk forlenget sin frist (NOU, 2006:6, s. 30; Riksrevisjonen, 2005, s. 9). Noe som da selvsagt påvirker prosesser som er avhengige av deres resultater. Men etter ferdigstillelse av både BAS-5 og Infrastrukturutvalget har bl.a. FAD i gjennom Stortingsmelding nr 17 ”Eit informasjonssamfunn for alle” fra 2006-2007 presisert rollene og ansvaret til de forebyggende, tverrsektorielle og sektorvise aktørene (St.meld., nr. 17 (2006-2007), ss. 159-161). Samtidig som også de nasjonale retningslinjene for å styrke informasjonssikkerhetene, utarbeidet av KIS, har påpekt ansvarsprinsippet overfor sektormyndighetene og virksomhetseiere (FAD, 2007, s. 10).

2) Som godkjennings- og tilsynsmyndighet.

NSMs ansvar som både godkjennings- og tilsynsmyndighet er avgrenset i henhold til Sikkerhetslovens definisjon. En godkjenner både personell, systemer og installasjoner og gjennomfører tilsyn for å føre kontroll med de organisasjoner som er ansvarlige for personellet, systemene og installasjonene. Når det gjelder tilsynsvirksomheten er denne to delt. En har både det tilsynet som er hjemlet i forbindelse med Sikkerhetslovens avgrensning og det tilsynet som gjøres i et samarbeid med DSB og som er knyttet til JDs samordningsansvar for samfunnssikkerhet og beredskap. NSMs sektorspesifikke tilsyn knyttet til sikkerhetsloven og de sikkerhetsgraderte systemer, er i mindre grad relevante for denne oppgaven og vil ikke håndteres nærmere. Tilsynsansvaret som løses i et samarbeid med DSB, er håndtert tidligere i denne oppgaven og vil derfor heller ikke belyses videre.

Når det gjelder godkjenninger og sertifiseringer av systemer og IT-installasjoner gjøres dette av NSM selv, av Sertifiseringsmyndighetene for IT-sikkerhet (SERTIT) og i samarbeid med søkerne. Sertifiseringsordningen ble etablert i 2002, et par år senere viste evalueringen av ordningen en ung organisasjon med oppstartsvansker (Riksrevisjonen, 2005, s. 61). Undersøkelser gjort i forbindelse med riksrevisjonens egen gjennomgang av myndighetenes arbeid med å sikre IT-infrastruktur, bekrefter stort sett evalueringen fra 2004. Det pekes i

riksrevisjonsrapporten spesifikt på utfordringer knyttet til at sertifiseringsordningen er lite kjent i forvaltningen og for små og mellomstore bedrifter i næringslivet. NORSIS peker også på at å bruke ordningen ikke medfører noen markedsmessige fordeler, noe som vil påvirke bruken negativt i næringslivet (Riksrevisjonen, 2005, s. 63).

NSM, rolle i en helhetlig tilnærming

VDI & NorCERT

Fra å ha et tydelig avgrenset forhold til det forebyggende ansvaret, har implementeringen av flere tiltak medført at utøvelsen av et mer helhetlig ansvar har blitt mer sentralt for NSM. Spesielt kan overtakelsen av VDI ansvaret og etableringen av NorCERT nevnes. Det siste helhetlige bidraget fra NSM, cybersikkerhetsstrategien, vil håndteres nærmere under argument 3 og vil derfor ikke inngå i denne delen av drøftingen.

VDI er et teknologisk virkemiddel til å fange opp trusler fra internett mot samfunnsviktige datanettverk. I forbindelse med oppstarten av prosjektet og senere også den permanente implementeringen av VDI, ble prosessen fulgt opp av EOS-utvalget. Denne kontrollen har ikke påvist kritikkverdige forhold knyttet til for eksempel misbruk av de teknologiske mulighetene (EOS, 2005, s. 13). Riksrevisjonsrapporten fra 2005-2006 viser til at VDI på den ene siden har lyktes med å få tilgang til informasjon om logiske trusler via internett. Men at VDI ikke har klart å nå andre målsetninger som at informasjonen til allmennheten skulle være mest mulig tilgjengelig. Riksrevisjonen er derfor kritisk til FDs prioritering til å løse denne delen av det helhetlige ansvaret. I den politiske gjennomgangen av riksrevisjonens undersøkelse presiser også Kontroll- og konstitusjonskomiteen at FDs kommentarer til Riksrevisjonen, viser et forbedringspotensial for denne virksomheten (Kontroll- og konstitusjonskomiteen, Innst. S. nr. 85 (2005-2006), s. 11).

På dette tidspunktet var det også avklart at et CERT skulle etableres og som skulle inkl. VDI (Riksrevisjonen, 2005, s. 9). NorCERT, som enheten underlagt NSM nå heter er en nasjonal operativ varslings- og håndteringskapasitet for alvorlige angrep mot samfunnsviktig IKT-infrastruktur (NSM, 2011b). Informasjon tilknyttet NorCERT er ikke lett tilgjengelig, og etter organisasjonens oppstart i 2006 er det ikke tilgjengeliggjort evalueringer av denne virksomheten. Det er derfor relevant å inkludere avisartikkelen fra desember 2010 hvor Aftenposten refererte til at ”flere store virksomheter selskaper ønsker ikke å være med på samarbeidet”, (Johansen, 2010a). Noe som kan tyde på at medlemmene i samarbeidet kanskje

ikke er helt fornøyd med hva en får tilbake på investeringen de har med å være delaktige i det sensornettverket, som VDI er. Artikkelen peker også på et alvorlig dilemma som kan skade legitimiteten til NSM/NorCERTs offentlig/private samarbeid. VDI er på den ene siden basert på frivillighet og selvfinansiering blant medlemmene. På den andre siden så er NSM ikke bare mottaker av finansieringen fra medlemmene, NSM også deres tilsynsmyndighet (Johansen, 2010a). Dette setter NSM i et økonomisk avhengighetsforhold til de samme aktørene som de har tilsynsansvar for, en praksis som ikke er fri for etiske utfordringer.

Delkonklusjon Forsvarssektoren: NSM inkl VDI & NorCERT

NSMs praksis viser en organisasjon som har både en helhetlig og sektoriell tilnærming til sitt arbeid. Deres sektor er sikkerhetssektoren og ikke kun forsvarssektoren, til det er forholdet til JD for tett. Forholdet er på enkeltområder ikke avklart nok da NSM tar med seg sine begrensninger i ansvar inn i justissektoren og etter min mening skaper et vakuum som forblir uadressert, eller i beste fall nedprioritert. Her er det IKT-sikkerheten i JDs tilsynsansvar det er tenkt på. Når det gjelder NSMs helhetlige tilnærming, er den heller ikke så helhetlig. Dette tror jeg kan ha med FDs manglende myndighet i fredstid å gjøre. Myndigheten til å sette krav til sikkerhet i fredstid, er ikke i samme grad gitt FD som JD, og helhetlige samarbeid blir derfor bygd på frivillighet og selvfinansiering. I tillegg til at denne praksisen tilfører etiske utfordringer for FD og NSMs ansvar og praksis, stilles det også spørsmålstegn til deres legitimitet i forbindelse med forslag til samarbeid.

5.3.3 Oppsummering av delkonklusjoner til Argument 2

Basert på funnene i drøftingen av ansvar og myndighet ser de ut til at sektorspesifikt ansvar og myndighet samt det ansvar som er gitt de hemmelige tjenestene er både er godt hjemlet og tolket gjennom egne instrukser. Derimot er tverrsektorielt ansvar ikke så godt beskrevet av de ansvarlige, ei heller forstått av fagdepartementene. Dette tilsier at ansvarsprinsippet ser mer gjennomarbeidet ut en den helhetlige tilnærmingen når en ser på myndighetsdelen.

Når en skal se på ansvar, ressurser og prioritering, vil jeg anbefale å se i forlengelsen av delkonklusjon 1. For det kan virke som om jeg er i ferd med å beskrive en følgefeil, om en vil kalle det for det. Grunnen til dette er at manglende konkretisering, og myndighetsgiving til aktørene med tverrsektorielt ansvar vil medføre en mindre gjennomførbar helhetlig tilnærming. Derimot har økt klargjøring av sektorielt ansvar bidratt til at ansvarsprinsippet blir stadig mer rotfestet som krisehåndteringsprinsipp.

Det er ikke entydige spor som sier at helhetlig tilnærming eller ansvarsprinsipp er mest styrende i dagens arbeid, knyttet til cybersikkerhet. Tiltak kommer og går, noen er mer helhetlig orientert enn andre og noen tiltak er mer konkretisert enn andre, om en ser på hvordan de skal implementeres. Dersom en standpunkt skal tas vil nok det gå i favør av at ansvarsprinsippet fortsatt er mer styrende enn helhetlige tilnærminger fra myndighetenes side.

5.4 Argument 3): Ingen legitim helhetlig aktør

Tidligere har både FADs koordineringsansvar for informasjonssikkerhet og JDs samordningsansvar for samfunnssikkerhet og beredskap blitt behandlet nærmere. Utgangspunktet for dette argumentet er utfordringen med legitime helhetlige aktører når ansvarsprinsippet skal legges til grunn til tross for at myndighetene vil ha helhetlige tilnærminger.

Men hva kreves så for å bli en legitim aktør for en helhetlig tilnærming i dag? Under det første argumentet ble to akser vurdert og hvor konklusjonene viste at både sektoransvar og tverrsektorielt ansvar øker i innhold og omfang. Når det gjelder både klarlegging av myndighet og praktisering av myndighet gjennom ressurser og prioriteringer, har en store utfordringer knyttet til helhetlige tilnærminger. Dette skaper en utfordring når en skal se nærmere på om en aktør kan og bør ha en rolle som kan håndtere ikke bare dagens arbeid, men som også kan fungere i en situasjon med en større helhet.

Etableringene og utviklingen av DSB, NorSIS, KSE, NSMs fagrapporteringslinje til JD, NorCERT, JDs samordningsansvar og KRU, har alle vært tiltak for å øke koordineringen, samordningen av det forebyggende arbeidet og den tverrsektorielle håndteringen av kriser og utfordringer[29]. Men myndighetenes ansvar er både fragmentert og uoversiktlig, og knytningen til de private kunne være bedre. Det er status dersom en ser på argumentasjonen og tiltakene i den nye cybersikkerhetsstrategien (NSM, 2009a).

[29] KSE er JDs Krise Støtte Enhet, som er en ressurs som kan benyttes av valgt lederdepartement i forbindelse med håndteringen av kriser.

Hvordan kan således en aktør med et legitimt tverrsektorielt ansvar være? Jeg vil under dette argumentet vurdere det alternativ som myndighetene nå sist har foreslått som en del av Cybersikkerhetsstrategien.

Nasjonal strategi for cybersikkerhet (cybersikkerhetsstrategien)

Tiltak 22: Nasjonalt cybersenter

Cybersikkerhetsstrategien er ikke spesifikt blitt gjort rede for i denne oppgaven. Nasjonalt cybersenter som sådan er også kun 1 av 22 tiltak, og vil derfor heller ikke bli redegjort nærmere for. Kort fortalt er det en nasjonal strategi for cybersikkerhet hvor undertittelen presiserer at den adresserer forebygging og håndtering av IKT-hendelser med store samfunnsmessige skadefølger. Den er utarbeidet av NSM, og høringsutsendelsen er gjort av FD (NSM, 2009a). Det er derfor naturlig å se nærmere på det foreslåtte nasjonale cybersenteret som en mulig tverrdepartemental aktør. Et slikt cybersenter som foreslås reiser kanskje flere spørsmål enn det besvarer. Ett par av disse som er relevante under argument 2 er 1) at et forslag om helhetlig tilnærming, tiltak for tverrdepartemental samordning og sektorovergripende løsninger fremmes av ett direktorat og departement, og ikke et samlet KIS, eller et annet eksisterende tverrdepartementalt samarbeid. Og 2) at cybersikkerhetsstrategien ikke sier noen ting om departemental tilhørighet for et slikt cybersenter, til tross for at funksjonene som er foreslått inn i et slikt senter hører hjemme i forskjellige departementer.

1) Cybersikkerhetsstrategien peker tidlig på både den helhetlige tilnærmingen og behovet for samordning og sektorovergripende løsninger. Samtidig som den også peker på at krisehåndteringsprinsippene skal ligge til grunn (NSM, 2009a, s. 13).

Dette er i seg selv en vanskelig balansegang. Det er nettopp derfor jeg velger å vektlegge at når ett direktorat presenterer en slik strategi, så har den til en viss grad i utgangspunktet feilet i henhold til sine egne mål. For kan et direktorat under et departement bidra til å skape en helhetlig tilnærming? I høringsuttalelsene vil vi finne at FAD, som er ansvarlig for den nasjonale IKT-politikken og koordineringen av informasjonssikkerhet, bl.a. peker på de overlappende målsetningene strategiene har i forhold til retningslinjene for informasjonssikkerhet (FAD, 2010). PST kommenterte også NSMs strategi og rolle, men dette vil jeg komme tilbake til under pkt 2).

Til tross for noe kritikk i forholdet til FADs og KISs rolle, så har responsen på initiativet til en slik tilnærming som cybersikkerhetsstrategien stort sett vært positiv (Finanstilsynet, 2010; PST, 2010a). Det er også på sin plass å vise til en uttalelse som i større grad også var kritisk til NSMs tilnærming. DSS peker i sin høringsuttalelse på at fokuset rundt NSMs ansvar i strategien er for stort, sett i forhold til ansvaret til DSB (DSS, 2010). Dette peker på to områder.1) Et ønske fra DSS om at DSB under JD bør ha et større ansvar enn NSM under FD, og 2) Et ønske om å bevege seg fra et snevrere sikkerhetsbilde med fokus på målbevisste angrep til et videre sikkerhetsbilde som i større grad adresserer sårbarhetene. Det siste begrunnes med at trusselen for store IKT-angrep, som for eksempel det mot Estland i 2007 er mer usannsynlig enn uhell som brannen i kulverten ved Oslo S (DSS, 2010; Kirk, 2007; Nilsen, 2007; PT, 2010).

DSS sine kommentarer er interessante både fordi DSS er underlagt FAD, men kanskje mer fordi de er ansvarlige for sikringen av informasjonssystemene som ivaretar deler av den statssikkerheten som denne oppgaven har satt fingeren på. Det er et stort sprang fra store IKT-angrep til uforutsette hendelser som kan medføre brudd på kommunikasjon og tap av informasjon. Og langs denne linjen av trusler vil en finne bl.a. informasjonsspionasje, noe DSS ikke har adressert i sin høringsuttalelse, selv om dette har vært et aktuelt problem i deres drift av statsforvaltningens datasystem (Johansen & Overn, 2010). Som underlagt enhet til FAD, så er også DSS knyttet til tilsyn fra DSB, og gitt deres datasystemers gradering, er heller ikke NSM deres tilsynsmyndighet på IT siden. Dette kan være med på å forklare noe av deres forhold til organisasjonene og synet på hva som skal være dimensjonerende i arbeidet, trusler eller risikovurdering.

Dersom vi legger fokuset på hvem som har tatt initiativet til side, kan vi fokusere på produktet i stedet for å se nærmere på hva som er lagt i begrepene helhetlig tilnærming, samordning og sektorovergripende løsninger. Et eksempel på hva cybersikkerhetsstrategien mener finner vi under tiltak 1, som omhandler det å kartlegge og verdivurdere kritiske IKT-systemer i alle sektorer. Cybersikkerhetsstrategien vektlegger her at dette må gjøres i en samordnet prosess, basert på eksisterende prosessmekanismer og kunnskap. I dette arbeidet må samtlige sektormyndigheter med sikkerhetsansvar delta. Det kan her være hensiktsmessig å peke på at det er JD som har et overordnet samordningsansvar for samfunnssikkerhet. Cybersikkerhetsstrategien peker både på eksisterende prosesser hos DSB og PT, uten å presisere hvem som evt skal ta ansvaret for samordningen de i mellom (NSM, 2009a, s. 14).

Det å kartlegge og verdivurdere kritiske IKT systemer i alle sektorer, har også blitt påpekt ved flere anledninger tidligere. Allerede i Innstilling nr. 9 til Stortinget i perioden 2002-2003, ble behovet for kompetanse på og informasjon om kritisk IKT-infrastruktur adressert. Et av temaene som ble adressert var hvilke ringvirkninger et bortfall av kritisk infrastruktur, som telekommunikasjon, vil resultere i. Dette er viktig for å få mer kjennskap til samfunnets sårbarhet (Forsvars- og Justiskomiteen, Innst. S. nr. 9 (2002-2003), s. 7). Riksrevisjonen kritiserer også at a) den nasjonale strategien for informasjonssikkerhet fra 2003, og 2) prosjektet BAS-5 ikke ble prioritert høyt nok i perioden. Noe som førte til at det verken ble planlagt noen aktiviteter for dette i departementene, eller at økonomiske midler ble stilt til rådighet to år senere enn planlagt[30] (Riksrevisjonen, 2005, s. 9).

Senere har infrastrukturutvalget, påpekt behovet for at JD tydeliggjør sin koordinerende rolle og ansvar knyttet til kritisk infrastruktur på tvers av sektoren (NOU, 2006:6, s. 56). Til tross for denne utredningens anbefaling fant Riksrevisjonens undersøkelse av JDs samordningsansvar for samfunnssikkerhet, at flere departement så på JDs samordningsansvar som uklart (Riksrevisjonen, (2007-2008), s. 11). Dette synet blir noe mer nyansert i den overordende evalueringen etter gjennomføringen av Nasjonal Øvelse 2008/IKT øvelse-08 hvor JDs operative samordningsrolle i en krisesituasjon ble oppfattet som uklar. Til tross for en økt interesse rundt tverrsektorielle løsninger vil vi også finne bekreftelser på at krisehåndteringsprinsippene fortsatt skal gjelde. Et slikt eksempel er den nye objektsikkerhetsforskriften, som igjen peker tilbake på departementene og deres ansvar (Objektsikkerhetsforskriften, 2010).

2) Cybersikkerhetsstrategien har flere tiltak som tilsier økt samordning eller tverrsektorielle løsninger, men tiltakene sier dog ikke alltid noe om hvordan eller igjennom hvem dette skal samordnes eller løses. Jeg vil her se nærmere på Tiltak 22 som omhandler etableringen av et nasjonalt cybersenter. Tiltaket beskriver det nasjonale cybersenteret som en operativ funksjon, som skal håndtere og respondere på alvorlige IKT-hendelser og situasjoner. Med tanke på at krisehåndteringsprinsippene skal ligge fast, kan det stilles spørsmål til hva som menes med at cybersenteret skal håndtere og respondere på alvorlige IKT-hendelser og situasjoner. Uttalelsen bør sees i sammenheng med tiltak 15 i samme strategi, som anbefaler en etablering

[30] Se tiltak nr. 1 i den nasjonale strategien for informasjonssikkerhet fra 2003 og i hovedtemaet for forskningsarbeidet til BAS-5. (Fridheim & Hagen, 2007; NHD, et al., 2003)

av sektorvise Computer Security Incident Response Team (CSIRT) miljøer. Dersom dette blir etablert vil man ha et distribuert nettverk på sektor- og virksomhetsnivå med ansvar for, og kompetanse til IKT-krisehåndtering. I tillegg vil da funksjonen NorCERT kunne ha en mer overordnet rolle med også et internasjonalt ansvar. Her er det viktig å påpeke at med et overordnet ansvar, ser det ikke ut til at NSM vil bevege et nasjonalt cybersenter vekk fra et operativt ansvar. Årsaken bak denne antagelsen er å finne i tiltak 19 og 20 som peker på behovet for å avdekke og identifisere trusler og trusselaktører samt og etablere offensive kapasiteter til å respondere på IKT-angrep. Disse to tiltakene viser hvorfor kulepunkt 3 i tiltak 22 ser ut som det gjør.

> *"Tverrfaglige analysefunksjoner i et samarbeid mellom de 3 EOS-tjenestene, og eventuelt andre ved behov, for å sikre en helhetlig analyse og vurdering av IKT risikobildet. Dette er i praksis en videreutvikling og operasjonalisering av Koordineringsgruppen for IKT-trusselbildet" (NSM, 2009a, ss. 22-23).*

Det nasjonale cybersenteret vil med disse funksjonene ha knyttet sammen enheter underlagt både JD og FD, og ved behov også andre departementer, som det henvises til under kulepunkt 3.

PST peker på noen viktige utfordringer knyttet til et evt nasjonalt cybersenter rolle, gitt at det skal inneha de funksjonene som angitt.

> *"… forslaget til strategi legger til grunn at "**juridiske forutsetninger og spørsmål knyttet til formelt ansvar må avklares nærmere, og detaljerte prosessbeskrivelser utarbeides."**, jf forslaget side 23. …Dette synes spesielt viktig dersom cybersenteret også skal være et viktig virkemiddel for å styrke evnen til å etterforske og bekjempe IKT-hendelser, oppgaver som i dag ikke tilligger NSM[31]" (PST, 2010a, s. 3).*

En operativ funksjon som et slikt nasjonalt cybersenter er tenkt å være, i henhold til kulepunkt 3, står i kontrast til etterretningssjefens kommentar i Teknisk Ukeblad i forbindelse med artikkelen om Forsvarets og Generalinspektøren for Forsvarets Informasjonsinfrastruktur ønske om å samle cyber-Norge. Her advarer sjef Etterretningstjenesten mot store organisatoriske endringer i iveren etter å styrke cyber-samarbeidet[32] (Grandhagen, 2011b).

[31] Uthevelsen er gjort for å vise i denne delen av teksten i PST høringsuttalelse ble vektlagt, da igjennom kursivering.

[32] Etterretningstjenesten leverte ikke noen offentliggjort høringsuttalelse på cybersikkerhetsstrategien, noe som gjør generalløytnant Grandhagens kommentar i Teknisk Ukeblad relevant i denne sammenheng.

Denne skepsisen til samordning fra både etterretningstjenesten og PST, bygger også godt under de funn som EOS-utvalget har gjort om eksisterende utfordringer i samarbeidsoperasjoner mellom PST og etterretningstjenesten. Utvalget gav i møte med PST også uttrykk for at denne situasjonen ikke var tilfredsstillende (EOS, 2007, s. 14). Dette rapporteres det om fra EOS-utvalget ett år etter samarbeidsinstruksen mellom etterretningstjenesten og Politiets sikkerhetstjeneste ble etablert. Etter denne kritikken fra EOS-utvalget har EOS-tjenestene etablert et samarbeid, KRU, for spesifikt å adressere IKT-trusselbildet. Og etter å ha sett kommentarene fra både PST og Etterretningstjenesten etter etableringen av cybersikkerhetsstrategien, vil jeg peke på følgende. 1) PST ser ut til å være villige til å se nærmere på hva som må legges til rette før en kan etablere et cybersenter. 2) Etterretningstjenesten ser ikke ut til å være villig til å formalisere det samarbeid som allerede er etablert i KRU. Basert på disse observasjonene, vil jeg hevde at et nasjonalt cybersenter slik det er skissert i cybersikkerhetsstrategien, vil ikke ha legitimitet en gang blant de aktørene som er tenkt skal være en integrert del av dette cybersenteret.

Det å samle disse funksjonene reiser også andre spørsmål. Forhold rundt til et slikt senters departementale tilhørighet, rapporteringsplikt, tilsynsansvar og EOS-utvalget er noen. Dette er viktige spørsmål fordi EOS-utvalget har påpekt flere utfordringer med arbeidet opp i mot EOS-tjenestene.

- Utviklingen innenfor informasjons- og kommunikasjonsteknologien, gjør arbeidet til EOS-utvalget vanskelig og tidkrevende, noe som også øker kravene til kompetanse og kanskje også metode i deres arbeid (EOS, 2002). Dette igjen vil generere økt behov for ressurser til EOS-utvalget og således også øke kostnadsbildet rundt den politiske styringen av EOS-tjenestene.

- Samarbeidet mellom EOS-tjenestene påvirkes mye av det endrede trusselbildet, og tjenestene må gå i gjennom store endringer for å tilpasse samarbeidet (EOS, 2003).

- For å sikre en politisk kontroll med tjenestene og deres samarbeidsløsninger har EOS-utvalget behov for aksept for sin tilsynsrolle. Prosessen frem til en slik aksept er ikke alltid problemfri (EOS, 2005).

Et slikt cybersenter som er forespeilet, har også et behov for en legitimitet i det politiske miljøet som har det overordnede styringsansvaret. EOS tjenestenes grensesnitt mot viktige rettsstatsprinsipper som personvern og rettssikkerhet vil arves, og må derfor også være under

politisk kontroll og styring. Datatilsynet er også usikker på NSMs rolle, og setter dette opp mot et mer sivilt alternativ, som DSB, i en slik setting som cybersikkerhetsstrategien skisserer. Videre peker også Datatilsynet på tiltak 17, 18 og 19 om datalagring, etterforskning og identifisering av trusselaktører som bekymringsverdig i forhold til personvernet (Datatilsynet, 2010).

Dersom en tar med seg Datatilsynets bekymringer og ser nærmere på de uønskede konsekvensene av økt press mot personvernet i favør av statlige institusjoner, vil jeg henvise til Kap. 3 i boken Overvåking i en rettsstat av Dag Wiese Schartum, som omhandler personvern, rettssikkerhet og vern mot alvorlig kriminalitet.

> *"Dersom det offentliges kunnskap om borgernes privatliv øker, for eksempel ved at statens mulighet til å overvåke borgerne utvides, vil mulighetene til maktmisbruk øke. Dette vil kunne påvirke borgernes tillit til de offentlige myndigheter, noe som vil kunne forstyrre maktbalansen mellom borgerne og myndighetene, som igjen vil kunne virke ødeleggende for demokratiet" (Bruce & Sunde Haugland, 2010, s. 65).*

Jeg mener dette på en god måte viser nødvendigheten av legitimitet i det politiske miljøet. I tillegg til hvilke uforutsette og langsiktige virkninger som forhastede organisasjonsetableringer kan føre til. Legitimitet må derfor vurderes også i et slikt strategiarbeid, og i utviklingen av tiltak, slik som i cybersikkerhetsstrategien.

Avslutningsvis vil jeg i tillegg peke på kommentaren i kulepunkt 3, som tilsier at andre aktører utover EOS tjenestene kun vil delta ved behov. Med andre aktører menes både andre myndigheter med tverrsektorielle funksjoner og private aktører. Jeg tar her utgangspunkt i at sektorspesifikke aktører vil være i dialog med et slikt cybersenter gjennom sine CSIRT, som ønskes etablert under tiltak 15. Grensesnittet ut mot private vil også være et grensesnitt som vil være avhenging av at et offentlig cybersenter også har legitimitet blant de private aktørene. Finansnæringens Fellesorganisasjon (FNO) peker på noen utfordringer som må løses før cybersikkerhetsstrategien kan implementeres. Blant annet må formålet med en evt ny organisasjon, som cybersenteret, vurderes i sammenheng med eksisterende aktører innen eksisterende analyse-, sikrings- og beredskapsarbeid (FNO, 2010). Om et nytt cybersenter vil bli en kompletterende eller konkurrerende aktør i markedet, vil også avgjøre dens legitimitet blant de private aktørene.

5.4.1 Oppsummering av delkonklusjoner til Argument 3):

Denne fremstillingen er gjort for å vise tiltakene som cybersikkerhetsstrategien har for å 1) løse utfordringene med å få kartlagt og verdivurdert den kritiske IKT-infrastrukturen og 2) JDs samordningsansvar. Dessverre sier ikke strategien noen om implementeringen av de respektive tiltakene, og det er ikke satt noen tidsperspektiver eller delmål på veien til måloppnåelse. Jeg ønsker derfor her å vise en av PSTs kommentarer fra deres høringsuttalelse. For å skissere et bedre ambisjonsnivå for hvor en er i dag.

> *"PST finner at forslaget til strategi for cybersikkerhet vil være et godt utgangspunkt for en videre prosess knyttet til arbeidet med å sikre samfunnskritisk infrastruktur. … Som en av de sentrale aktørene på dette feltet, vil PST gjerne delta i den videre prosessen knyttet til disse spørsmålene" (PST, 2010a).*

Denne uttalelsen bekrefter langt på vei at strategien, som strategi ikke fungerer bl.a. på grunn av at den manglende helhetlige tilnærmingen i prosessen rundt utarbeidelsen av strategien. Når dokumentet kan brukes i et videre arbeid, mener jeg dette viser det til at tilnærmingen dokumentet har til målrettede tiltak, er både relevant og ønsket.

Myndighetene har ikke foreslått en tverrsektoriell aktør med nødvendig legitimitet i cybersikkerhetsstrategien. Faktisk er legitimitet ikke tatt hensyn til verken i prosessen med å utvikle strategien, eller i vurderingene rundt forutsetningene til eller konsekvensene av tiltakene. Kritikken og reservasjonene fra PST og etterretningstjenesten er eksempler på dette. Datatilsynets bekymringer knyttet til utfordringer med ivaretakelse av personvern og rettssikkerhet er et annet eksempel. Noe som jeg mener også støttes av funnene til EOS-utvalget i de senere år. Til slutt viser også private aktører at legitimitet ikke er noe myndighetene kan organisere seg frem til, uten å måtte se dette i sammenheng med allerede eksisterende aktører og funksjoner i markedet. Noe som i følge FNO ikke er gjort i stor nok grad.

6. Oppsummering, konklusjon og implikasjon

Hensikten med dette kapitelet er å kort oppsummere drøftingen, konkludere i forhold til oppgavens problemstilling og utlede kort om noen alternative implikasjoner av funnene fra arbeidet med denne Masteroppgaven. Drøftingen i denne oppgaven baserte seg på tre argumenter som tar tak i kjente utfordringer knyttet til forholdet i mellom en helhetlig tilnærming og at ansvarsprinsippet i krisehåndteringen fortsatt skal ligge til grunn.

6.1 Oppsummering av drøftingen

Det inntrykket som sitter igjen etter å ha sett nærmere på funnene fra drøftingen i argument 1 er at både sektorielle aktører og aktører med tverrdepartementalt ansvar utvider sin tolkning av både ansvar og oppgaver. Utviklingen skjer i takt med økt kritisk blikk både på deres ansvar og den teknologiske utviklingen. To trender som funnene understøtter er 1) at hva som definerer en helhetlig tilnærming ikke adresseres. Både FADs rolle knyttet til IKT-politikken og den koordinerende rollen for informasjonssikkerhet bør klarlegges nærmere. I tillegg til at JD også bør klarlegge samordningsansvaret overfor de forskjellige virkemidlene de har i sin verktøykasse. 2) Den andre trenden er at avstanden i mellom myndighetene og de private forsterkes ved at ansvarsprinsipp og sektoransvar er mer konkretisert og håndgripelig en den helhetlige forebyggende satsingen.

I grensesnittet i mellom å ha helhetlig ansvar og sektoransvar viser drøftingen av argument 2 at sektorielt ansvar stadig blir bedre hjemlet og forstått. Når det gjelder ansvar for helhetlig tilnærming konkretiseres ikke dette på den samme måten. Utfordringene knyttet til et slik ansvar er både kjent og blir gjentatt stadig hyppigere, gjennom både utredninger og revisjoner. Sett utenfra ser derfor ansvarsprinsippet ut som en mer gjennomarbeidet og forstått praksis ut fra den helhetlige tilnærmingen, både i forhold til myndighetsdelen og i utøvelsen av ansvaret gjennom ressurser og prioritering.

Det er dog interessant å se at til tross for en satsning på en helhetlig tilnærming ser det ut til at det er på det sektorielle ansvaret at oppgavene, ansvaret og behovet for ressurser/prioritering det er mest utvikling. Drøftingen viser at ansvarsprinsippet fortsatt er mer styrende enn helhetlige tilnærminger fra myndighetenes side.

Etter å har drøftet på FADs forebyggende koordineringsansvar for informasjonssikkerhet og JDs samordningsansvar for samfunnssikkerhet og beredskap, ville jeg i argument 3 se

nærmere på det nyeste forslaget som ligger på bordet i dag angående tverrsektorielle aktører. Cybebersikkerhetsstrategien skisserer der i tiltak 22, et nasjonalt cybersenter. Funnene fra drøftingen viser at ordet legitim, som brukt i argumentet er et sentralt begrep.

Myndighetene har ikke vektlagt legitimitet nok, verken i planleggingen av, utarbeidelsen eller i det endelige resultatet av cybersikkerhetsstrategien. En helhetlig tilnærming krever en bred offentlig/privat deltakelse, inkludering av flere hensyn, en reell diskusjon om alternativer og konsekvenser. Kritikken og reservasjonene fra PST, etterretningstjenesten, datatilsynet og FNO er eksempler på dette.

Til tross for den manglende helhetlige tilnærmingen i prosessen rundt utarbeidelsen av strategien kan dokumentet brukes i et videre og mer helhetlig arbeid, fordi tilnærmingen dokumentet har til målrettede tiltak, er både relevant og ønsket av de fleste høringsinstansene.

6.2 Svar på problemstilling

Denne oppgavens problemstilling er som følger: Vil det være mulig å ha en helhetlig tilnærming til cybersikkerhet i Norge, når ansvarsprinsippet skal ligge til grunn?

Basert på de funnene denne oppgaven har gjort vil det kanskje være fristende å si nei, det ville vært enklest. Grunnen til dette er at når en bruker begrepet helhetlig tilnærming, og så ser på dette opp i mot FADs koordineringsansvar for informasjonssikkerhet og JDs samordningsansvar for samfunnssikkerhet, er kritikken til måten oppgaven er løst ganske stor. Mangelen på gjennomføringskapasitet i FAD og KIS ligger her som kanskje det sentrale ankepunktet. Det er behov for at arbeidet med cybersikkerhet ledes av noen med mer enn et rent koordinerende ansvar. 14 års erfaringer med koordinerende roller på dette i USA har ikke virket, slik Walter Gary Sharp, Sr. ser dette[33] (Sharp, 2010, s. 20).

Hvis en i tillegg ser litt prinsipielt på en av JDs store utfordringer, mener jeg også at mangelen på konkretisering av tverrdepartementalt ansvar og instruksverk for utøvelse av et slikt ansvar også bidrar til at helhetlig tilnærming vil være mindre styrende enn ansvarsprinsippet for

[33] Walter Gary Sharp, Sr. Senior Associate Deputy General Counsel for Intelligence, Office of the General Counsel, U.S. Department of Defense; Adjunct Professor of Law, Georgetown University (Sharp, 2010) Law Center; and Judge Advocate, U.S. Marine Corps (Retired).

sektorene. Avslutningsvis vil også manglende legitimitet til tverrdepartementale samarbeidsformer hindre en mer helhetlig tilnærming.

Dersom en så får konkretisert roller og oppgaver for tverrdepartementalt ansvar, og virkemidler gjøres tilgjenglig slik at gjennomføringskapasiteten øker. Har en også økt sannsynligheten for økt legitimitet til en aktør som kan agere helhetlig på strategisk nivå. En legitimitet som er vesentlig om en også ønsker en helhetlig tilnærming også på utøvende nivå senere. Helhetlig tilnærming kan bare bygges ovenfra og ned.

6.3 Implikasjoner av forskningen

I innledningskapitelet har jeg vist til noen prosesser som er i gang og av interesse for denne oppgaven. FAD og KIS skal i løpet av året revidere de nasjonale retningslinjene for styrking av informasjonssikkerhet, og i den sammenheng må de sektorielle bidragene sees i sammenheng med dette. Cybersikkerhetsstrategien må det arbeides nærmere med og en kan ikke komme utenom en vurdering av disse to dokumentene opp i mot hverandre. Basert på dette får en vurdere hvorvidt helhetlig tilnærming eller fortsatt prioritering av ansvarsprinsippet er riktig veg å gå. Velger enn å prioritere helhetlig tilnærming må det også fokuseres nærmere på hvordan en mer konkretisert tverrdepartemental myndighetsutøvelse kan implementeres.

FD proklamerte tidligere i år et behov for å evaluere sikkerhetsloven, dette kan være hensiktsmessig basert på de utfordringer forsvarssektoren står overfor. FAD, JD og SMK burde i denne sammenhengen også inkluderes i et slikt arbeid for å evaluere hvorvidt det er behov for et mer helhetlig lovverk knyttet til informasjon som bør beskyttes, uansett om det er av sikkerhetshensyn, politiske eller økonomiske hensyn. En slik tilnærming vil måtte adressere både unntaksreglene i Offentleglova, bruken av beskyttelsesinstruksen og vurderingen om ett sikkerhetsregime kontra to.

Avslutningsvis vil jeg også påpeke at alle de overnevnte prosessene, ikke må gjennomføres på bekostning av å fa satt i kraft den nye straffeloven. Dette fordi denne loven vil bidra både på det forebyggende området, men også på det operative i forbindelse med straffeforfølging.

Litteraturliste

Akerhaug, L., & Johansen, P. A. (2010). Nytt dataangrep mot regjeringen. Hentet fra http://www.aftenposten.no/nyheter/iriks/article3921285.ece

Beskyttelsesinstruksen. (1972). *Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter* Oslo: Statsministerens kontor (SMK).

Bistandsinstruksen. (2003). *Instruks om Forsvarets bistand til politiet* Oslo: Forsvarsdepartementet.

Bruce, I., & Sunde Haugland, G. (2010). Personvern, rettssikkerhet og vern mot alvorlig kriminalitet. I D. W. Schartum (Red.), *Overvåking i en rettsstat*: Fagbokforlaget.

Cavelty, M. D. (2007). Cyber-Terror– Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics, 4(1) 2007*. doi: 10.1300/J516v04n01_03

Creswell, J. W. (2009). *Research design: qualitative, quantitative, and mixed methods approaches*. Los Angeles: SAGE.

Datatilsynet. (2010). *Høring — forslag til strategi for cybersikkerhet* (Vol. 10/00839-2/AAR). Oslo: Datatilsynet.

Difi. (2011). *Digitalt førstevalg - en kartlegging av hindringer og muligheter* (Vol. 2011:3). Oslo Direktorat for forvaltning og IKT.

Dragnes, K. (2011, Publisert: 13.02.11 kl. 11:21). Midtøstens fred og ufred, *Aftenposten*. Hentet fra http://www.aftenposten.no/meninger/kommentatorer/dragnes/article4027965.ece

DSB. (2005). Nasjonal sårbarhets- og beredskapsrapport for 2005. Tønsberg: Direktoratet for Samfunnssikkerhet og Beredskap.

DSB. (2009). Sivil nasjonal øvelse (SNØ) 2008 Øvelse IKT-08. Tønsberg: Direktoratet for Samfunnssikkerhet og Beredskap.

DSS. (2010). *Høring — forslag til strategi for cybersikkerhet*. Oslo: Departementenes Servicesenter.

DSS. (2011, 02.07.2009). Avdelingar. Hentet 31. mars, 2011, fra http://dss.dep.no/Om-oss/Avdelinger/

Ekomloven. (2003). *Lov om elektronisk kommunikasjon*. Oslo: Samferdselsdepartementet.

EOS. (2002). *Dokument nr. 16 Årsmelding for 2002* (Vol. (2002-2003)). Oslo: Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste.

EOS. (2003). *Dokument nr. 16 Årsmelding for 2003* (Vol. (2003-2004)). Oslo: Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste.

EOS. (2005). *Dokument nr. 20 Årsmelding til Stortinget* (Vol. (2005-2006)). Oslo: Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste.

EOS. (2007). *Dokument nr. 9 Årsmelding* (Vol. (2007-2008)). Oslo: Stortingets kontrollutval for etterretnings-, overvakings- og tryggingsteneste.

Eriksen, A. (2007, 29.05.2007). Rettslig plikt til å ha system for informasjonssikkerhet? Hentet 05.09., 2011, fra https://www.nsm.stat.no/Documents/KIS/Publikasjoner/Systemplikter%20informasjonssikkerhetsregelverk.pdf

Facebook. (2011). Facebook principles. Hentet 25 Februar, 2011, fra http://www.facebook.com/profile.php?id=540180909#!/principles.php

FAD. (2007). *Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010*. Oslo: Fornyings- Administrasjons- og Kirkedepartementet.

FAD. (2010). *Høring - forslag til strategi for cybersikkerhet* (Vol. 201001472-/NZM): Fornyings-, administrasjons- og kirkedepartementet.
FAD. (2011). Informasjonssikkerhet. Hentet 31. mars, 2011, fra http://www.regjeringen.no/nb/dep/fad/tema/ikt-politikk/informasjonssikkerhet.html?id=623457
FD. (2003). *Fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet.* (Vol.): Forsvarsdepartementet.
FD. (2009). *Evne til innsats - Strategisk konsept for Forsvaret*. Oslo: Forsvarsdepartementet.
FD. (2011). Økt IKT-trussel: Sikkerhetsloven evalueres. Pressemelding 2/2011 Hentet 19. mai, 2011, fra http://www.regjeringen.no/nb/dep/fd/pressesenter/pressemeldinger/2011/okt-ikt-trussel-sikkerhetsloven-evaluere.html?id=633659
Finanstilsynet. (2010). *Forslag til strategi for cybersikkerhet - høringsuttalelse* (Vol. 10/7002). Oslo: Finanstilsynet.
FNO. (2010). *Høringsuttalelse — Forslag til strategi for cybersikkerhet* (Vol. 10-320-EV): Finansnæringens Fellesorganisasjon.
Forsvars- og Justiskomiteen. (Innst. S. nr. 9 (2002-2003)). *Veien til et mindre sårbart samfunn*: Forsvars- og Justiskomiteen,.
Fridheim, H., & Hagen, J. M. (2007). *Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer: sluttrapport* (Vol. 2007/01204). Kjeller: FFI.
FSA Instruks. (2010). *Instruks om sikkerhetstjeneste i Forsvaret, Fastsatt 29. april 2010 av Forsvarsdepartementet i medhold av instruksjonsmyndighet.* Oslo: Forsvarsdepartementet.
FSJ. (2011). Forsvarets årsrapport 2010. Hentet 23. mai,, 2011, fra http://forsvaret.no/arsrapport2010/Documents/forsvarets-arsapport-2010.pdf
galrahn. (2011). Google Declares War on the Egyptian Government. Hentet 3. februar, 2011, fra http://blog.usni.org/2011/02/01/google-declares-war-on-the-egyptian-government/
Gilje, N., & Grimen, H. (1993). *Samfunnsvitenskapenes forutsetninger: innføring i samfunnsvitenskapenes vitenskapsfilosofi*. Oslo: Universitetsforlaget.
Google. (2011). Vår filosofi_Ti ting vi vet. Hentet 22. mars, 2011, fra http://www.google.no/intl/no/corporate/tenthings.html
Grandhagen, K. (2011a). Etterretningstjenesten mellom hemmelighold og åpenhet. Hentet 23 Mai, 2011, fra http://www.oslomilsamfund.no/oms_arkiv/2011/2011-02-28-Grandhagen.html
Grandhagen, K. (2011b). Har utenlandsansvaret. Hentet 22. mai 2011, fra http://www.tu.no/it/article276944.ece
Hagen, T. (2006). E-tjenesten i en omskiftelig verden. Manuskript til foredrag i Oslo Militære Samfunn.Hentet 23. mai, 2011, fra http://www.oslomilsamfund.no/oms_arkiv/2006/2006-11-20-Hagen.html
Henriksen, S., Sørli, K., & Bogen, L. (2007). *Metode for identifisering og rangering av kritiske samfunnsfunksjoner* (Vol. 2007/00874). Kjeller: FFI.
Hokstad, S. A. (2010). *Helhetlig tilnærming - et verdibegrep: en sammenligning mellom den politiske styringens og den militære profesjonens bruk av begrepet helhetlig tilnærming.* Masteroppgave Forsvarets høgskole, Oslo.
Haaland Eriksen, L. (2009). Evaluering av utflytting av statlig virksomhet Post- og teletilsynet (s. 52). Bærum: Asplan Viak.
IKTSoS. (2004, Februar 2004). IKT sikkerhet og sårbarhet - Programbeskrivelse. Hentet 22.05, 2011, fra http://www.forskningsradet.no/servlet/Satellite?c=Page&pagename=iktsos%2FHovedsidemal&cid=1228296117212

IKTSoS. (2008). IKT sikkerhet: Det kontinuerlige kappløpet - Sluttrapport. Hentet 22.05, 2011, fra http://www.forskningsradet.no/servlet/Satellite?c=Page&pagename=iktsos%2FHovedsidemal&cid=1228296117212

Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser?: innføring i samfunnsvitenskapelig metode*. Kristiansand: Høyskoleforl.

JD. (2002). *Instruks for Koordinerings- og rådgivningsutvalget for etterretnings- og sikkerhetstjenestene.* . Oslo: Justis- og politidepartementet.

JD. (2008). *St.prp. nr. 1 (2008–2009) For budsjettåret 2009, Utgiftskapitler: 61, 400–480, Inntektskapitler: 3061, 3400–3474 og 5630,* . Oslo: Departementenes servicesenter.

Johansen, P. A. (2010a, 1 Desember). Dataforsvaret er blitt kraftig svekket, *Aftenposten*, s. 4-5.

Johansen, P. A. (2010b, 10 November). Hackere prøvde å ta seg inn på Nobel-direktørens PC, *Aftenposten*. Hentet fra http://www.aftenposten.no/nyheter/iriks/article3898053.ece

Johansen, P. A. (2010c, 19 Oktober). Regjeringen tappet for store mengder data, *Aftenposten*. Hentet fra http://www.aftenposten.no/nyheter/iriks/article3862920.ece

Johansen, P. A., & Foss, A. B. (2011, 4 Januar). Fransk spionasje verre enn russisk og kinesisk, *Aftenposten*. Hentet fra http://www.aftenposten.no/nyheter/uriks/wikileaks/article3971575.ece

Johansen, P. A., & Overn, K. (2010, 21 Oktober, 2010). Eksstatsråd skjulte dårlig datasikkerhet, *Aftenposten*. Hentet fra http://www.aftenposten.no/nyheter/iriks/article3862920.ece

Kirk, J. (2007, 17 Mai). Estonia recovers from massive DDoS attack - Denial-of-service onslaught may have Russian origins, *Computerworld*. Hentet fra http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

Kontroll- og konstitusjonskomiteen. (Innst. S. nr. 85 (2005-2006)). *Innstilling om Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur*. Oslo: Kontroll- og konstitusjonskomiteen,.

KRIPOS. (2006). *Strategi 2006-2010*. Oslo: KRIPOS.

Lewis, J. A. (2011, 03.01.2011). Significant Cyber Incidents Since 2006. Hentet 24 Januar, 2011, fra http://csis.org/files/publication/110118_Significant_Cyber_Incidents_Since_2006.pdf

NATO. (2010a). *Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation*. Lisboa: NATO.

NATO. (2010b). AAP-6 NATO Glossary of terms and definitions. Brussels: NATO Standardization agency.

NHD, FD, & JD. (2003). *e-Norge- Nasjonal strategi for informasjonssikkerhet, Utfordringer, prioriteringer og tiltak* (K-0668 B). Hentet fra https://www.nsm.stat.no/Documents/KIS/Publikasjoner/Nasjonal_strategi_for_informasjonssikkerhet.pdf.

Nilsen, J. (2007). Politiet 2006: – Strømbrudd lite sannsynlig. Hentet 22.05., 2011, fra http://www.tu.no/iphone/article125391.ece

NorCERT. (2011). VDI. Hentet 28 mars, 2011, fra https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/VDI/

NOU. (1998:4). *Politiets overvåkingstjeneste* (Vol. NOU 1998:4). Oslo: Statens forvaltningstjeneste.

NOU. (2000:24). *Et Sårbart samfunn: utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet* (Vol. 2000: 24). Oslo: Departementenes servicesenter, Informasjonsforvaltning.
NOU. (2003:18). *Rikets sikkerhet* (Vol. NOU 2003: 18). Oslo: Statens forvaltningstjeneste. Informasjonsforvaltning.
NOU. (2006:6). *Når sikkerheten er viktigst: beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner* (Vol. NOU 2006: 6). Oslo: Statens forvaltningstjeneste. Informasjonsforvaltning.
NSM. (2003). *Risikovurdering*. Oslo: Nasjonal sikkerhetsmyndighet Hentet fra https://www.nsm.stat.no/Publikasjoner/risikovurderinger/.
NSM. (2006). *Risikovurdering*. Oslo: Nasjonal sikkerhetsmyndighet Hentet fra https://www.nsm.stat.no/Publikasjoner/risikovurderinger/.
NSM. (2009a). *Nasjonal strategi for cybersikkerhet*. Oslo: Forsvarsdepartementet Hentet fra http://www.regjeringen.no/nb/dep/fd/dok/hoeringer/hoeringsdok/2010/forslag-til-strategi-for-cybersikkerhet/Horingsnotat.html?id=599898.
NSM. (2009b). *Veiledning i verdivurdering*. Oslo: Nasjonal Sikkerhetsmyndighet Hentet fra https://www.nsm.stat.no/Documents/Veiledninger/Veiledning%20i%20verdivurdering%20200903.pdf.
NSM. (2010, 29 August 2010). Sikkerhetsvarsel fra NSM. Informasjon om skadevaren Stuxnet. Hentet 22.05., 2011, fra https://www.nsm.stat.no/upload/Sikkerhetsvarsel/Sikkerhetsvarsel%20Stuxnet.pdf
NSM. (2011a, Udatert). Gradert informasjonssystemsikkerhet. Hentet 19.04., 2011, fra https://www.nsm.stat.no/Arbeidsomrader/Informasjonssystemsikkerhet/
NSM. (2011b, April 2011). Årsmelding 2010. Hentet 09.05., 2011, fra https://www.nsm.stat.no/Documents/Brosjyrer/Årsmelding_NSM2010web.pdf
NSM, PST, & Etterretningstjenesten. (2010). *Bakgrunnsnotat Cybersikkerhet* (2010/00719/430 utg.): Forsvarsdepartementet.
NSR. (2009, 07.12.2009). AD: Høring — Forskrift om objektsikkerhet. Hentet 10.05., 2011, fra http://www.regjeringen.no/nb/dep/fd/dok/hoeringer/hoeringsdok/2009/forskrift-om-objektsikkerhet/horingsuttalelser.html?id=583748
NSR. (2011a, 31 mars 2011). Om NSR. Hentet 19.04., 2011, fra http://www.nsr-org.no/Hvem.htm
NSR. (2011b, 30 mars 2011). Samfunnets datasårbarhet må ikke bli et militært anliggende Hentet 22.05., 2011, fra http://www.nsr-org.no/artikler/cyberforsvar.htm
NTB. (2011, 16.01.11 - 13:04). USA og Israel samarbeidet om dataangrep mot Iran, *Verdens Gang*. Hentet fra http://www.vg.no/nyheter/utenriks/artikkel.php?artid=10021090
Objektsikkerhetsforskriften. (2010). *Forskrift om objektsikkerhet* Oslo: Forsvarsdepartementet.
Offentleglova. (2006). *Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova).* Oslo: Justis- og politidepartementet
Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and Implications. Cooperative Cyber Defence Centre of Excellence Hentet 23 Mai, 2011, fra http://www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf
PDMT. (2011, 01.09.2009 14:17). Virksomhetsinformasjon. Hentet 25 mars, 2011, fra https://www.politi.no/pdmt/avdelinger/ikt/
Politiloven. (1995). *Lov om politiet*. Oslo: Justis- og politidepartementet.
PST. (2004). Politiets sikkerhetstjenestes trusselvurdering 2004. Hentet 22.05., 2011, fra http://www.pst.politiet.no/PST/Templates/Article____872.aspx
PST. (2006). Ugradert Trusselvurdering 2006. Hentet 05.22., 2011, fra http://www.pst.politiet.no/PST/Templates/Article____872.aspx

PST. (2007). Ugradert Trusselvurdering 2007. Hentet 05.22., 2011, fra http://www.pst.politiet.no/PST/Templates/Article____872.aspx
PST. (2010a, 22 Juni 2010). Høring - Forslag til strategi for cybersikkerhet. Hentet 05.22., 2011, fra http://www.regjeringen.no/pages/2534053/Cybersikkerhet_svar-med-merknader_PST.pdf
PST. (2010b). Åpen Trusselvurdering. Hentet 05.22., 2011, fra http://www.pst.politiet.no/PST/Templates/Article____872.aspx
PST. (2011a). Ingen tittel. Hentet 05.22, 2011, fra http://www.pst.politiet.no/
PST. (2011b). Åpen Trusselvurdering. Hentet 05.22., 2011, fra http://www.pst.politiet.no/PST/Templates/Article____872.aspx
PST Instruks. (2005). *Instruks for Politiets sikkerhetstjeneste* (Vol.). Oslo: Justis- og politidepartementet.
PT. (2009, 04.12.2009). Høyringssvar - forskrift om objektsikkerheit. Hentet 05.10., 2011, fra http://www.regjeringen.no/nb/dep/fd/dok/hoeringer/hoeringsdok/2009/forskrift-om-objektsikkerhet/horingsuttalelser.html?id=583748
PT. (2010, 25 Juni 2010). Høring - forslag til strategi for cybersikkerhet. Hentet 05.22., 2011, fra http://www.regjeringen.no/pages/2534053/Cybersikkerhet_svar-med-merknader_Post-og-teletilsynet.pdf
Reuterdal, A.-C., Kolberg, M., & Randen, A. (2010, 29.11.2010). Wikileaks-avsløringene svekker diplomatiet. Hentet 24 Januar, 2011, fra http://www.nrk.no/nyheter/verden/1.7402062
Riksrevisjonen. (2005). *Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur* (Vol. Dokument nr. 3:4). Oslo: Riksrevisjonen.
Riksrevisjonen. (2008). *Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2007* (Riksrevisjonen, Trans. Vol. Dokument nr. 1). Oslo: Departementenes servicesenter.
Riksrevisjonen. (2009a). *Riksrevisjonens oppfølging av forvaltningsrevisjoner som er behandlet av Stortinget* (Riksrevisjonen, Trans. Vol. Dokument nr. 3:1). Oslo: Departementenes servicesenter.
Riksrevisjonen. (2009b). *Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2008* (Riksrevisjonen, Trans. Vol. Dokument nr. 1). Oslo: Departementenes servicesenter.
Riksrevisjonen. (2010). *Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2009* (Riksrevisjonen, Trans. Vol. Dokument nr. 1). Oslo: Departementenes servicesenter.
Riksrevisjonen. ((2007-2008)). *Riksrevisjonens undersøkelse av Justisdepartementets samordningsansvar for samfunnssikkerhet* (Riksrevisjonen, Trans. Vol. Dokument nr. 3:4). Oslo: Departementenes servicesenter.
Rutledal, F., Hagen, J., Nystuen, K. O., & Østby, E. (2000). *Kraftmarkedets føringer for sårbarheten i norsk kraftforsyning* (Vol. 2000/03451). Kjeller: FFI.
Samarbeidsinstruksen. (2006). *Instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste.* Oslo: Forsvarsdepartementet.
Samferdselsskomiteen. (Innst. S. nr. 329 (2000-2001)). *Innstilling fra samferdselskomiteen om telesikkerhet og -beredskap i et telemarked med fri konkurranse*. Oslo: Samferdselsskomiteen.
SAMRISK. (2006). Samfunnssikkerhet og risikoforskning - Programplan. Hentet 23. februar, 2011, fra http://www.forskningsradet.no/servlet/Satellite?c=Page&cid=1228296552890&pagename=samrisk%2FHovedsidemal
Scholte, J. A. (2000). *Globalization: a critical introduction*. Basingstoke: Macmillan.

SD. (2009, 10 Desember 2009). Forskrift om objektsikkerhet - Høringsuttalelse. Hentet 23.mai, 2011, fra http://www.regjeringen.no/nb/dep/fd/dok/hoeringer/hoeringsdok/2009/forskrift-om-objektsikkerhet/horingsuttalelser.html?id=583748

Sharp, W. G. S. (2010). The Past, Present, and Future of Cybersecurity. *Journal of national security law & policy, 4*(1).

Sikkerhetsloven. (1998). *Lov om forebyggende sikkerhetstjeneste* Oslo: Forsvarsdepartementet.

Sommer, P., & Brown, I. (2011). Reducing Systemic Cybersecurity Risk. Future Global Shocks Hentet 01.05., 2011, fra http://www.oecd.org/dataoecd/57/44/46889922.pdf

St.meld. (nr. 17 (2006-2007)). *Eit informasjonssamfunn for alle*. Oslo: Fornyings- og administrasjonsdepartementet

St.meld. (nr. 22 (2000-2001)). *Politireform 2000 Et tryggere samfunn*. Oslo: Justis- og politidepartementet.

St.meld. (nr. 22 (2007-2008)). *Samfunnssikkerhet- Samvirke og samordning*. Oslo: Justis- og politidepartementet.

St.meld. (nr. 42 (2004-2005)). *Politiets rolle og oppgaver*. Oslo: Justis- og politidepartementet.

St.meld. (nr. 47 (2000-2001)). *Telesikkerhet og -beredskap i et telemarked med fri konkurranse*. Oslo: Samferdselsdepartementet.

St.prp. (nr. 42 (2003-2004)). *Den videre moderniseringen av Forsvareti perioden 2005–2008*. Oslo: Forsvarsdepartementet.

St.prp. (nr. 48 (2007-2008)). *Et forsvar til vern om Norges sikkerhet, interesser og verdier*. Oslo: Forsvarsdepartementet.

Straffeloven. (1902). *Almindelig borgerlig Straffelov*. Oslo: Justis- og politidepartementet.

Straffeloven. (2005). *Lov om straff (straffeloven).* . Oslo: Justis- og politidepartementet.

Sælør, M. C. (2010). PST: Skjult tjeneste i et åpent samfunn. I D. W. Schartum (Red.), *Overvåking i en rettsstat* (s. 282-296): Fagbokforlaget.

Sørli, K., Henriksen, S., Bogen, L., & Mørkestøl, K. (2007). *Bakgrunnsstudie til metode for identifisering og rangering av kritiske samfunnsfunksjoner* (Vol. FFI-rapport 2007/00875). Kjeller: FFI.

Torgersen, H. H., Ege, R. T., Johnsrud, I., & Johnsen, A. B. (2011). Tror nordmenn var med på cyberangrepet. Hentet 21 Mai, 2011, fra http://www.vg.no/nyheter/innenriks/artikkel.php?artid=10093946

U.S. Naval Institute. (2008). About the U.S. Naval Institute. Hentet 21 Mai, 2011, fra http://blog.usni.org/about/

US Army CAC. (2008). *NSPD-54/HSPD23*. Hentet fra http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=9140.

Vassnes, B. (2011). Naiv cyberoptimisme. *Klassekampen*.

Zachariassen, E. (2011). Hun må være sjefen. *Teknisk Ukeblad, 2011*(17/11). Hentet fra http://www.tu.no/it/article286203.ece