Forsvarets høgskole

våren 2014

Masteroppgave

Sivil-militært samarbeid i en cyberkrise

En studie av Cyberforsvarets rolle dersom sivil elektronisk kommunikasjonsinfrastruktur rammes av et cyberangrep

Ingunn Harildstad Gustavsen

Forord

Masteroppgaven har vært en fin anledning til å kunne fordype meg i et tema jeg hadde lite kjennskap til fra før. Det har vært lærerikt og utfordrende. God støtte fra erfarne kolleger med stor fagkunnskap har medvirket til at jeg kom i mål, - til slutt.

Det er mange som fortjener ros for gode innspill, men jeg vil fremheve de velvillige intervjuobjektene: Bjarte Malmedal, Stig Rune Heen, Rune Dyrlie, Storm Jarl Landaasen, Torbjørn Braastad Tynning, Roger Johnsen, Torgeir Magnussen og Hans Christian Pretorius. De har bidratt med innsikt, gode vurderinger og mye inspirasjon.

En annen som fortjener en stor takk er Torgeir Broen i Cybermakt-prosjektet ved FFI. Torgeir har lagt ned en betydelig innsats for å hjelpe. Han ga meg god drahjelp i starten og har fulgt opp med faglig støtte, konstruktiv kritikk og stort engasjement under veis.

Jeg har lært mye gjennom arbeidet med denne oppgaven, men å omsette læringsutbyttet til en samfunnsvitenskapelig tekst har vært svært krevende. Det har vært mange lange dager og mye frustrasjon. Tusen takk til hovedveileder Gert Lage Dyndal for engasjement og kyndig veiledning.

Eventuelle feil og mangelfulle vurderinger tar jeg ansvar for.

To års studie går nå mot slutten. Jeg er veldig glad for at arbeidsgiver ga meg muligheten til å gjennomføre dette studiet, det har vært spennende og lærerikt. Særdeles god tilrettelegging og støtte fra skolen, kunnskapsrike lærerkrefter og fantastiske medstudenter har gjort dette til en svært fin tid, men nå gleder jeg meg til å komme tilbake til FLO/IKT.

Det har vært utfordrende å kombinere rollene student, kone og mamma. Både for meg og familien. Jeg har til tider vært selvsentrert og mentalt fraværende. Lars Ivar, Vilde og Ingrid fortjener all ros for å ha holdt ut med meg.

Lommedalen 22.mai 2014

Ingunn Harildstad Gustavsen

Sammendrag

Temaet for denne studien er sivil-militært samarbeid i en cyberkrise og oppgaven har fokusert på Cyberforsvarets rolle dersom sivil elektronisk kommunikasjonsinfrastruktur (ekom-infrastruktur) rammes av et cyberangrep[1], herunder *når* Cyberforsvaret kan bistå og *hva* de kan bistå med?

Utgangspunktet er at nasjonal krisehåndtering og regulering av sivil-militært samarbeid er uavhengig av domenet krisen oppstår i. Det etablerte systemet utgjør slik det teoretiske grunnlaget for å kunne drøfte Cyberforsvarets rolle i en cyberkrise. Oppgaven er løst som en kvalitativ studie, en kombinasjon av innholdsanalyse, casestudie og intervju.

Cyberangrep er vanskelig å definere og kan ligge i en gråsone mellom kriminell virksomhet og krigshandlinger, mellom politi og Forsvar sine ansvarsområder. Hovedregelen er likevel at cyberangrep mot sivil infrastruktur ledes av sivile myndigheter inntil Regjeringen beslutter noe annet. Studien viser imidlertid at politiet har begrenset med kompetanse og ressurser til å kunne håndtere pågående cyberangrep og vil kunne få behov for bistand fra Forsvaret. Videre viste studien at Cyberforsvarets ansvar er knyttet til Forsvarets egen kommunikasjonsinfrastruktur og understøttelse av Forsvarets operasjoner hjemme og ute. Cyberforsvaret vil ha en bistands rolle dersom sivil ekom-infrastruktur rammes av et cyberangrep som setter samfunnssikkerheten i fare. Bistand er imidlertid ikke en dimensjonerende oppgave for Cyberforsvaret, og det må eventuelt skje innenfor rammene av bistandsinstruksen. Cyberforsvaret har erfaring fra drift og overvåkning av egen landsdekkende infrastruktur. De har kompetanse på analyse av sårbarheter og ondsinnet kode, besitter mobile kapasiteter og har erfaring med bruk av dem i nettverk de har lite kjennskap til fra før. Cyberforsvaret vil kunne bistå med all tilgjengelig kompetanse og ressurser dersom det besluttes at Forsvaret kan avgi disse cyberressursene.

[1] I denne oppgaven skal cyberangrep forstås som målrettede angrep med ulike formål, herunder både spionasje og sabotasje, se kapittel 1.2. Begrepsbruken er imidlertid stadig under utvikling, oppgaven kommer nærmere inn på dette i kapittel 4.4

Abstract

The theme of this study is civil-military cooperation in cyber-crisis. In Norway, the military authority is responsible for defending the nation against external threats meanwhile the police shall uphold the law against domestic threats. The military assistance to the police is regulated in national law.

The general rule is that cyber-attacks against civilian infrastructure are handled by civil authorities. This thesis analyzes the Norwegian Cyber Force possibilities, both in regards to time and resources, to support the civilian authorities if Norwegian civilian telecommunications infrastructure is attacked via a cyber-attack.

The thesis shows that the Norwegian police may have neither sufficient resources nor competence necessary if a national cyber-crisis appears. Another conclusion presented is, that the Norwegian Cyber Force has technology, expertise and experience from operating, monitoring and defending its own nationwide infrastructure.

If civil telecommunications infrastructure is targeted by a cyber-attack that puts important social interests, life or health in danger, the Norwegian Cyber Force will be able to assist the police as well as other civilian authorities with all from advisors to units with special competence.

Innhold

Figurliste

Forkortelser

BKI	Avdeling for beskyttelse av kritisk infrastruktur
CNA	Computer Network Attack
CIS TG	Communication Information System Task Group
CKG	Cyberkoordineringsgruppen
CND	Computer Network Defence
CNE	Computer Network Exploration
CNO	Computer Network Operations - Datanettverksoperasjoner
DSB	Direktoratet for samfunnssikkerhet og beredskap
EKOM	Elektronisk kommunikasjon
E-tjenesten	Forsvarets Etterretningstjeneste
FD	Forsvarsdepartementet
FFI	Forsvarets forskningsinstitutt
FFOD	Forsvarets fellesoperative doktrine
FKI	Forsvarets kommunikasjonsinfrastruktur
FOH	Forsvarets operative hovedkvarter
FO/S	Forsvarets overkommando/Sikkerhetsstaben
FSA	Forsvarssjefens sikkerhetsavdeling
FST	Forsvarsstaben
IKT	Informasjons- og kommunikasjonsteknologi
INI OPS	INI operasjoner (nå CYFOR CTO)
JD	Justis- og beredskapsdepartementet
KSE	Krisestøtteenheten
NorCERT	Norwegian Computer Emergency Response Team
NOU	Norges offentlige utredninger
NSM	Nasjonal sikkerhetsmyndighet

PBS1	Politiets beredskapssystem del 1
POD	Politidirektoratet
PST	Politiets sikkerhetstjeneste
PT	Post- og teletilsynet
SD	Samferdselsdepartementet
VDI	Varslingssystem for digital infrastruktur

1 Innledning

Spørsmålet er ikke lengre *om* vi vil rammes av en cyberkrise men *når* krisen inntreffer. Det er inntrykket man sitter igjen med etter å ha fulgt med på Dagbladets artikkelserie *Null CTRL* i fjor. I løpet av serien, som omhandlet IKT-sikkerhet i Norge, avslørte Dagbladet at over 2500 styringssystemer var koblet til internett, med minimal eller ingen sikkerhet (Karlsen, 2013). 500 av disse systemene kontrollerte industriell eller samfunnskritisk infrastruktur. I forbindelse med artikkelserien ble daværende sjef for Cyberforsvaret, generalmajor Roar Sundseth intervjuet. Sundseth uttalte at angrep mot norsk infrastruktur ikke kan utelukkes. Han påpekte at verken Norge eller særlig mange andre land har sett omfattende angrep enda, men at muligheten er der. «Trusselen er stor, og den er økende» sa Sundseth (Hillestad & Sandli, 2013). Sundseths vurdering samsvarer godt med rapporter fra Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets Etterretningstjeneste (E-tjenesten). NSM rapporterer om økende antall detekterte forsøk på dataangrep og datainnbrudd i kritisk infrastruktur. I 2013 håndterte de 50 alvorlige digitale infiltrasjonsforsøk. (NSM, 2014b, s. 4). E-tjenesten beskriver trusler i det digitale rom som «særlig relevant» for norsk sikkerhet og nasjonale interesser: «Digitale operasjoner kan rettes mot infrastruktur eller styringssystemer og forårsake forstyrrelser, fysisk skade eller ødeleggelse» (Etterretningstjenesten, 2014, s. 59).

IKT utgjør grunnmuren for samhandling nasjonalt og internasjonalt. Det moderne velferdssamfunnet vårt avhenger av elektronisk kommunikasjonsinfrastruktur (ekom-infrastruktur) for å fungere. Erkjennelsen av samfunnets teknologiske avhengighet, og begrepet *et sårbart samfunn,* ble etablert med utgivelsen av sårbarhetsutvalgets rapport i 2000 (NOU 2000: 24, 2000). Utfordringene knyttet til et *sårbart samfunn* kan være like aktuelle i dag som i 2000. *Sårbarhetsutvalget* ble oppnevnt av Bondevik-regjeringen og ledet av Kåre Willoch. Utvalget slo fast at kritiske samfunnsfunksjoner vil bryte sammen uten elektronisk kommunikasjon. En av disse kritiske samfunnsfunksjonene er informasjons- og ledelsesapparatet som trer i kraft ved kriser. Kriseapparatets behov for ekom-tjenester ble særlig bekreftet av to hendelser i 2011. I juni 2011 førte en logisk feil i en server til at Telenors mobilnett falt ut i hele landet[2], samtidig som Østlandet var rammet av storflom. I romjulen samme år førte stormen Dagmar til at omkring 20 000 husstander ble uten fasttelefon og 7500 uten internett/bredbånd.

Konsekvensene av utfallene var i hovedsak de samme i begge situasjonene: bortfall av mobil- og fasttelefonnettet gjorde kommunikasjon mellom viktige beredskapsaktører og mellom myndigheter og befolkning svært vanskelig. Fylkesmannen hadde store utfordringer med å få oversikt over situasjonen i fylket og få kontakt med kommunene. Den kommunale kriseledelsen hadde problemer med å kommunisere med nødetater og Statens vegvesen. I tillegg til å gi kriseledelsen store utfordringer hadde frafallet av ekom-tjenester negativ påvirkning på befolkningens trygghetsfølelse.

Brannen i Lærdal i januar i år og et strømutfall på Nord-Vestlandet i mars har vist at nettene fortsatt er sårbare. Under storbrannen i Lærdal gikk en av Telenor sine sentraler tapt. Sentralen var knutepunkt for både mobil, fasttelefon og bredbånd, og tapet av denne medførte at kommunikasjonen kollapset i Lærdal sentrum (Senel & Hattrem, 2014). To måneder senere ble 132 basestasjoner i Møre og Romsdal og 30 i Sogn og Fjordane satt ut av drift på grunn av et strømutfall. Kapasiteten i mobilnettet var sterkt redusert, og bredbånd og fasttelefoni var helt ute av funksjon. Konsekvensene var at trygghetsalarmer ble satt ut av funksjon, ingen av telefonene til politiet i Sunnmøre fungerte, samt at 110 og 113 fungerte bare delvis og for noen kunder. I tillegg sluttet bankterminalene å virke og folk fikk utfordringer med å utføre sin daglige virksomhet (Dagbladet, 2014; Korsnes, Roaldseth, & Berg, 2014; Rosbach & Utne, 2014). Vi er litt overrasket over at vi er så sårbare som vi er, sa politiet i Ålesund og erkjente det hadde vært en krevende situasjon (Korsnes et al., 2014).

Ingen av de nevnte hendelsene var tilsiktet. Men dagens trusselbilde tilsier altså at det finnes aktører som vil kunne ramme kritisk infrastruktur digitalt. Cyberangrep i form av spionasje eller sabotasje via nett. Det er kriminelle aktører som står bak de fleste illegale aktivitetene på nett i dag, men Forsvaret hevder det er nasjonalstater som utgjør den største trusselen (Etterretningstjenesten, 2014; Hillestad & Sandli, 2013). Statene driver etterretningsaktivitet for å ivareta egen nasjonal sikkerhet men samtidig foregår det også spionasje for å fremme kommersielle mål. Denne typen spionasje skiller seg fra øvrig kriminalitet i cyberdomenet ved å være både mer målrettet og langt mer avansert (S. T. Johnsen & Kveberg, 2014, s. 36). Et eksempel i denne sammenheng er den britiske etterretningstjenesten. En artikkel i *Der Speiegel* i september 2013 indikerer[3] at det britiske etterretningsbyrået Government Communications

[2] Utfallet varte i 18 timer
[3] Basert på dokumenter lekket fra NSA-varsleren Edward Snowden

Headquarters (GCHQ) skal stå bak et omfattende hacker-angrep[4] mot Belgacom. Belgacom er Belgias svar på Telenor: landets største telekommunikasjonsselskap og delvis statlig eid (Knudsen, 2013). Ansatte ble lurt til et nettsted hvor de fikk installert ondsinnet programvare på datamaskinene sine. Datamaskinene ble så brukt som utgangspunkt for videre spionasje mot de delene av infrastrukturen de hadde tilgang til. Målet har tilsynelatende vært en sentral nettverkskomponent som håndterer internasjonal trafikk. GCHQ skal ha vært ute etter å kartlegge Belgacom sin infrastruktur og legge til rette for avansert utnyttelse av mobiltelefonbrukere (Spiegel Online International, 2013). Kveberg og Johnsen, stiller i rapporten *Cyberdomenet, cybermakt og norske interesser* spørsmål om stater risikerer å påvirke stabiliteten i andre staters infrastruktur ved slike etterretningsoperasjoner (Kveberg & Johnsen, 2013, s. 26). Hvem vil ha ansvar, myndighet og virkemiddel til å håndtere situasjonen dersom digitale operasjoner rettes mot norsk kommunikasjonsinfrastruktur og forårsaker forstyrrelser?

1.1 Valg av problemstilling

Samfunnet vårt er tilsynelatende helt avhengig av tilgang til ekom for å fungere. Systemene har imidlertid vist seg å være sårbare og trusselen mot dem fremstår som høy. Norge utsettes jevnlig for cyberangrep, operasjoner som kan forårsake forstyrrelser, og i verste fall ødeleggelse av infrastruktur og styringssystemer. Det kan være et spørsmål om tid før krisen inntreffer. Er Norge beredt til å håndtere en cyberkrise dersom den skulle inntreffe?

Nasjonal beredskap- og krisehåndtering har fått stor fokus etter 22/7. *Aldri mer 22/7* er nærmest blitt et mantra. Utfordringen relatert til *ressursene som ikke fant hverandre* var knyttet til det fysiske domenet i juli 2011(NOU 2012: 14, 2012). Ville ressursene ha funnet hverandre dersom krisen oppstod i det digitale domenet, - i dag? Ivaretar dagens regulering av det sivil-militære samarbeidet cybertrusselen? Gjennom *Nasjonal strategi for informasjonssikkerhet* ga regjeringen, i 2012, sin beskrivelse av sikkerhetsutfordringene og hvilke områder de ville vektlegge. I dokumentet påpekes det at dagens utfordringer krever en helhetlig tilnærming og grenseoverskridende tiltak. Den nye Regjeringen støtter dette og sier de ønsker å stille Forsvarets ressurser til disposisjon for nasjonal krisehåndtering, - og «koble Cyberforsvaret inn i sivil cybersikkerhet hvor dette er hensiktsmessig» (Høyre-Frp-Regjeringen, 2013, s. 40). Men hva ligger det egentlig i å *koble inn* Cyberforsvaret og når vil det kunne være hensiktsmessig? Spørsmålene leder meg frem til følgende problemstilling:

[4] Å *hacke* vil si å bryte seg inn på datasystemer og -nettverk som vedkommende ikke har lovlig tilgang til

Hva er Cyberforsvarets rolle dersom sivil elektronisk kommunikasjonsinfrastruktur rammes av et cyberangrep? Når kan Cyberforsvaret bistå og hva kan de bistå med?

For å kunne besvare denne problemstillingen er det nødvendig å ha kunnskap om hvordan kriser prinsipielt håndteres i Norge og hva som regulerer bruken av militære ressurser i fredstid. Utgangspunktet er at nasjonal krisehåndtering og regulering av sivil-militært samarbeid er uavhengig av domenet krisen oppstår i. Blant de bestemmelser som regulerer sivilt-militært samarbeid, står *bistandsinstruksen*[5] særlig sentralt. Det er ikke gitt at dette systemet er tilpasset cyberhendelser men håndteringen av cyberhendelsene må likevel forholde seg til etablerte prinsipper og gjeldende bestemmelser. Forståelse for dette systemet er viktig, det utgjør det teoretiske grunnlaget for å kunne drøfte Cyberforsvarets rolle i en cyberkrise og vil derfor vies relativt stor plass i oppgaven.

Selve undersøkelsen vil jeg gjennomføre i tre deler, hvor den første delen skal bidra med økt kunnskap om ekom-infrastruktur og cyberdomenet. Jeg vil se på hva ekom-infrastruktur *er* og hvorfor forstyrrelser i, eller ødeleggelse av, sivil ekom-infrastruktur *kan* forårsake en nasjonal krise – en cyberkrise. Videre vil jeg se nærmere på hva et cyberangrep innebærer og de utfordringer en vil stå overfor i håndteringen av alvorlige cyberangrep. For å kunne drøfte Cyberforsvarets rolle er det viktig å ha kjennskap til hvilke andre aktører som innehar roller. Derfor vil jeg i del to kartlegge aktører og diskutere ansvar, oppgaver og myndighet knyttet til ekom-infrastruktur og håndtering av cyberangrep. De sivile aktørenes kapasitet vil indikere om de vil få behov for bistand fra Forsvaret eller ei. På samme måte vil Cyberforsvarets oppdrag og kapasiteter gi en god indikasjon på hva de vil kunne bistå med. I tredje og siste del vil jeg studere to caser som innebar cyberangrep mot sivil infrastruktur, analysere hvordan ble disse håndtert og hvilken støtte det viste seg å være behov for. Caseanalysen vil ha fokus på de oppgavene som er vektlagt i *Nasjonal strategi for informasjonssikkerhet*, herunder oppdage, analysere, koordinere og håndtere. De oppgaver hvor det viste seg å være behov for støtte vil så drøftes fortløpende. Har Cyberforsvaret kunnskap og verktøy til å kunne støtte og kan Cyberforsvaret bistå gitt dagens prinsipper for krisehåndtering og regulering av Forsvarets bistand til det sivile samfunn?

[5] *Instruks om Forsvarets bistand til politiet* regulerer det operative samarbeidet mellom Forsvaret og politiet. «Det er oppgåva til politiet å hindre allmenn kriminalitet, her under terrorhandlingar. For Forsvarsdepartementet (FD) er det viktig at det er og skal vera eit skarpt skilje mellom sivile og militære oppgåver. Når det er sagt, finst det årsakar

Målsettingen er å bidra til økt forståelse for de muligheter og utfordringer som er knyttet til bruk av Cyberforsvarets ressurser ved håndtering av cyberhendelser i sivil infrastruktur, i fredstid

1.2 Definisjoner

Oppgaven tar for seg en del begreper som det vil være nyttig å definere. Jeg vil forklare hva jeg legger i det enkelte begrep.

Cyberdomenet, også kalt det digitale rom, skal forstås som fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data. *Cyber* er et prefiks som indikerer at en aktivitet foregår i cyberdomenet. *Cyberangrep*[6] skal i denne oppgaven forstås som målrettede angrep med ulike formål, herunder både spionasje og sabotasje. Cyberangrep som rammer samfunnskritisk infrastruktur, samfunnskritisk informasjon eller samfunnskritiske funksjoner på en slik måte at det får betydning for samfunnets og befolkningens trygghet defineres som *alvorlige cyberhendelser*. Begrepsbruken er under stadig utvikling, jeg har valgt å basere meg på FD sine definisjoner, gitt i *FDs cyberretningslinjer*. Mer om dette i Kapittel 4.4.

Begrepene *elektronisk kommunikasjon* (ekom) og *telekommunikasjon* brukes om hverandre. Telekommunikasjon oppfattes likevel som et snevrere begrep, opphengt i tidligere systemer og tjenester[7]. Ekom-nett defineres i Ekomloven til å være: «system for signaltransport som muliggjør overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel der radioutstyr, svitsjer, annet koplings- og dirigeringsutstyr, tilhørende utstyr eller funksjoner inngår, herunder nettverkselementer som ikke er aktive» (Ekomloven, 2003: §1-5).

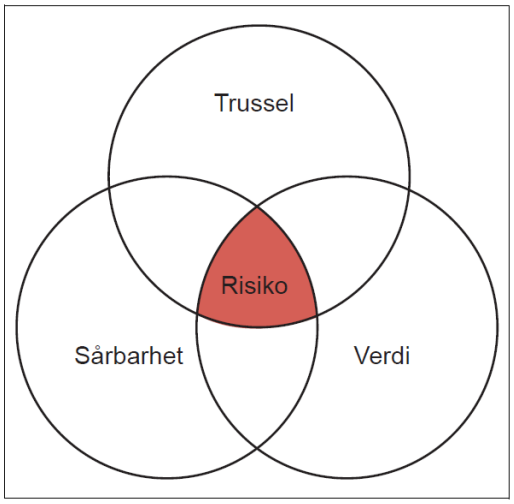
---

til at Forsvaret likevel i enkelte høve kan hjelpe politiet i dette arbeidet. Dette er regulert i den nemnde instruksen» (Regjeringen, 2013b)

[6] de handlinger i eller gjennom cyberdomenet som har til hensikt å skade eller påvirke personell, materiell eller konfidensialiteten , integriteten , tilgjengeligheten eller autentisiteten til et informasjonssystem (Forsvarsdepartementet, 2014, s. 5).

[7] EKOM er et begrep som først ble tatt i omfattende bruk i forbindelse med utarbeidelse av EKOM-loven, som erstattet den tidligere Teleloven. Telekommunikasjon er fremdeles et mye brukt begrep, men oppfattes ofte som snevrere og mer opphengt i tidligere systemer og tjenester. I en historisk beskrivelse er det imidlertid mest korrekt å benytte begrepet tele/telekommunikasjon (Nystuen & Fridheim, 2007, s. 9).

Trussel, sårbarhet, verdi og risiko: *Trussel* er sannsynligheten for å bli utsatt for et angrep. Sannsynligheten for å bli utsatt for en tilsiktet uønsket handling kan ikke vurderes på samme måte som sannsynligheten for naturhendelser og ulykker da sannsynligheten for et cyberangrep vil avhenge av de til enhver tid aktive trusselaktører, deres intensjoner og kapasitet som antas å foreligge for å gjennomføre uønskede handlinger og oppnå bestemte mål. Trusselnivået er ingen statisk størrelse, men kan endres fra dag til dag (DSB, 2013a, s. 7). Trusselaktørene er globale og spenner fra statlige etterretnings- og sikkerhetstjenester, via tradisjonelle militære motstandere, globale næringsbedrifter, terrorist- og ekstremistgrupper til organiserte hackergrupper og enkeltpersoner (E-tjenesten, NSM, & PST, 2013, s. 9).



Figur 1: Samspillet mellom trussel, sårbarhet og verdi (NOU 2012: 14, 2012, s. 68)

Sårbarhet defineres som manglende evne til å motstå en uønsket hendelse eller å opprette en ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning (E-tjenesten et al., 2013, s. 12).

Verdi er det vi av ulike hensyn ønsker å beskytte, det kan være alt fra liv og helse til fysiske objekter og infrastruktur, eller også abstrakte verdier som omdømme og operativ evne. De fleste sektorer er avhengige av kraft og telekommunikasjon, derfor har noen samfunnskritiske virksomheter verdier som er viktige for hele samfunnet og bortfall av verdiene vil ha konsekvenser for hele samfunnet, direkte eller indirekte.

Risiko er uttrykk for forholdet mellom trusselen mot en verdi og verdiens sårbarhet overfor denne spesifiserte trusselen. Reduseres ett eller flere av komponentene, reduseres også risikoen.

1.3 Tidligere og pågående forskning

Forsvarets Forskningsinstitutt (FFI) har gjennom prosjektene *Beskyttelse av samfunnet* (BAS) tatt for seg utfordringer knyttet til sårbarheter i kritisk infrastruktur. BAS prosjektene har vært gjennomført i samarbeid med Justis- og beredskapsdepartementet (JD), Direktoratet for samfunnssikkerhet og beredskap (DSB) og andre aktører innenfor sivil beredskap og samfunnssikkerhet.

I forbindelse med BAS5, gjennomførte fire forskere ved FFI en grundig analyse og beskrivelse av sårbarhetene i internettinfrastrukturen i 2007. I rapporten, *Sårbarheter i Internett*, deles sårbarhetene inn i fire kategorier: fysiske[8], logiske og sosiale[9] sårbarheter samt avhengigheter[10] (Windvik et al., 2007, s. 23). Forskerne påpeker at et angrep vil kunne utnytte og ha effekter i flere av disse dimensjonene. Logiske sårbarheter omfatter sårbarheter realisert i programvare, herunder protokoller og tjenester samt logisk redundans. Angrepsmidler mot logiske sårbarheter kan være «alt fra utnyttelse og bruk av allmenn tilgjengelig infrastruktur og kode som publiserte nettverksverktøy på Internett, til angrepskode og mer spesialskrevne verktøy» (Windvik et al., 2007, s. 23). Det presiseres at alle komponenter som kjører programvare, og alle systemer som helt eller delvis styres via programvare kan være sårbare. Det er angrepsmidler mot logiske sårbarheter som har fokus i denne oppgaven.

I tilknytning til det samme BAS-prosjektet forsket Lene Borgen og Kristin Mørkestøl på hvilke aktører som kan bli involvert i en IKT-krise på nasjonalt nivå i Norge, samt hvilke ansvar, myndighet og virkemidler de forskjellige aktørene har (Bogen & Mørkestøl, 2005). Bogen og Mørkestøl erfarte at selv om konsekvensene på mange måter er de samme om hendelsen skyldes

[8] Fysiske sårbarheter: Denne kategorien omfatter i første rekke sårbarheter grunnet feil på materiell, sabotasje og manglende fysisk redundans. Virkemidler som fysisk maktbruk og elektronisk krigføring retter seg direkte mot denne type sårbarheter. (Windvik, Thuv, Nystuen, & Sivertsen, 2007, s. 23).

[9] Sosiale sårbarheter. Denne kategorien dekker den menneskelige kontakten og innflytelsen på et datasystems utvikling, drift og vedlikehold, styring og bruk. Herunder faller krav til menneskelig kompetanse, håndtering av konfigurasjonsendringer, oppdateringer, uvøren bruk og organisatoriske aspekter. "Social engineering" er en type angrep som utnytter det menneskelige elementet direkte.

[10] Avhengigheter. Denne kategorien dekker sårbarheter som oppstår grunnet avhengigheter mellom systemet og andre systemer, eller avhengigheter innad i systemet. Dette kan være avhengigheter til helt andre infrastrukturer (strøm, vann), en tjenestes avhengighet av en annen tjeneste eller indre avhengigheter av spesielle noder i systemet grunnet arkitektur og design.

ekstremvær eller angrep vil årsaken til krisen kunne påvirke hvilke virkemidler som tas i bruk og Forsvarets rolle i håndteringen (Bogen & Mørkestøl, 2005, s. 11). Etter deres vurdering var det høy terskel for å sette inn Forsvaret i krisehåndteringen. Det nærmer seg 10 år siden dette arbeidet ble utført, siden da har avhengigheten til IKT økt. Maskinvare og programvare er blitt mer avansert, mer tilgjengelig og i større grad integrert i folks dagligliv. Terskelen for å bruke Forsvarets ressurser i krisehåndtering kan ha endret seg, og tillegg har Cyberforsvaret blitt etablert. Forsvaret vil derfor kunne få en annen rolle dersom nasjonen rammes av en IKT-krise[11] i dag. Denne oppgaven vil drøfte Cyberforsvarets rolle dersom sivil infrastruktur skulle bli utsatt for et cyberangrep i dag.

I sluttrapporten fra BAS5 påpekes det at privatiseringen av IKT-baserte tjenester og infrastrukturer har økt antallet aktører på feltet og gitt utfordringer i forhold til aktørers roller og ansvar (Fridheim & Hagen, 2007, s. 9-16). Denne oppgaven vil kartlegge de mest sentrale aktørene og diskutere deres ansvar og oppgaver i dag.

I 2010 gjennomførte Fridheim, Grunnan og Hagen en studie av nasjonal kriseledelse og sivil-militært samarbeid. Forskerne påpekte utfordringer knyttet til ansvar og roller i kriseledelsen og at Norge manglet en god strategi for hvordan vi skal håndtere et omfattende IKT-angrep (Hagen, Fridheim, & Grunnan, 2010). Regjeringen har i ettertid gitt ut *Nasjonal strategi for informasjonssikkerhet*. Denne oppgaven vil se om strategien har bidratt til å avklare hvordan et alvorlig cyberangrep mot sivil ekom-infrastruktur skal håndteres.
Det er ellers lite offentlig tilgjengelig forskningsmateriale som sier noe om oppgavens tema, men det er flere interessante forskningsprosjekter i gang som vil berøre samme problemstilling.

Parallelt med BAS-prosjektene har Forskningsrådet kjørt et program for samfunnssikkerhet og risiko – SAMRISK. SAMRISK ble sluttført i juni 2011, men Forskningsrådet sier terrorangrepene 22.juli er med på å anskueliggjøre at det er behov for ny forskning. Det påpekes at den fremtidige forskningen på samfunnssikkerhet ikke må ha for stor fokus på forrige krise: «Neste gang en krise rammer kan det være på et helt annet område som krever en helt annen type kunnskap, andre reaksjoner eller tiltak» (Forskningsrådet, 2013). Cybertrusler er et av

[11] Forskerne baserte seg på *Sårbarhetsutvalgets* definisjon av krise: «en hendelse som har potensial til å true viktige verdier og svekke en organisasjons evne til å utføre viktige funksjoner» og beskrev IKT-krise som en naturlig utvidelse av krisebegrepet: «en situasjon der informasjons- og kommunikasjonssystemer blir satt ut i en grad som gjør at de ikke kan håndteres med "vanlig" bemanning og normale rutiner» (Bogen & Mørkestøl, 2005, s. 10).

Forskningsrådets nye prioriterte forskningstema: «Det er behov for mer kunnskap om aktører, operasjonsmodus, konsekvenser, scenarier og muligheter for forebygging gjennom beskyttelse, avverging og andre former for bekjempelse» (Bjørgo et al., 2013).

FFI etablerte i 2012 prosjektet *Cybermakt***.** Prosjektet er en studie av cyberdomenets egenskaper og mulig evne som et nytt krigføringsdomene. Studien er bestilt av Cyberforsvaret og har som mål å komme opp med en anbefaling vedrørende hvilke kapabiliteter Norge og Forsvaret bør ha i cyberdomenet og hvordan cyberdomenet skal forsvares og utnyttes i fred, krise, væpnet konflikt og krig. Prosjektet skal etter planen ferdigstilles i 2014.

1.4 Avgrensning og presisering

Det er flere avdelinger i Forsvaret som vil kunne få en rolle i krisehåndteringen dersom samfunnskritisk ekom-infrastruktur rammes av et cyberangrep. Jeg har valgt å fokusere på Cyberforsvaret siden de ble nevnt spesifikt i regjeringserklæringen. Samtidig er kjernen i denne oppgaven håndtering av selve cyberangrepet, herunder å oppdage, varsle, analysere, koordinere og håndtere, og relatert til disse oppgavene er Cyberforsvaret en av de mest relevante avdelingene i Forsvaret.

Et cyberangrep mot sivil ekom-infrastruktur vil i første rekke kunne true samfunnssikkerheten ved at kritiske funksjoner settes ut av spill, men avhengig av angrepets omfang og mål kan det også true statssikkerheten (Prop. 73 S (2011-2012), s. 24). Denne oppgaven avgrenses til kriser som eies og ledes av sivile myndigheter, fordi Cyberforsvarets rolle er mye tydeligere dersom angrepet er av en slik art at Forsvaret leder håndteringen. Oppgaven vil derfor i veldig liten grad[12] berøre juridiske betraktninger om hva som skal til for at angrepet passerer grensen for *angrep på Norge* [13].

[12] Kommer litt inn på det i kapittel 4.5

[13] Det er regjeringen som må beslutte om situasjon er et «væpnet angrep på Norge», vurderingen som vil omfatte en rekke faktorer, herunder hvem som står bak terroranslaget, omfang og kompleksitet, betydningen for rikets sikkerhet og folkerettslige rammer. «Når et væpnet angrep først er konstatert, vil en nærmere vurdering av den konkrete situasjonen være avgjørende for hvilke deler av krigens folkerett som får anvendelse» (Meld. St. nr. 29 (2011-2012), 2012, s. 98).

1.5 Oppbygging

Dette kapittelet har presentert bakgrunnen for oppgaven og valg av problemstilling: *Hva er Cyberforsvarets rolle dersom sivil elektronisk kommunikasjonsinfrastruktur rammes av et cyberangrep? Når kan Cyberforsvaret bistå og hva kan de bistå med?* I tillegg har det blitt gitt en kort presentasjon av tidligere forskning som har bidratt til å sette rammen for denne oppgaven. Figur 2 viser en skisse av oppgavens oppbygging. Neste kapittel vil gjøre rede for valgt metode og kilder.

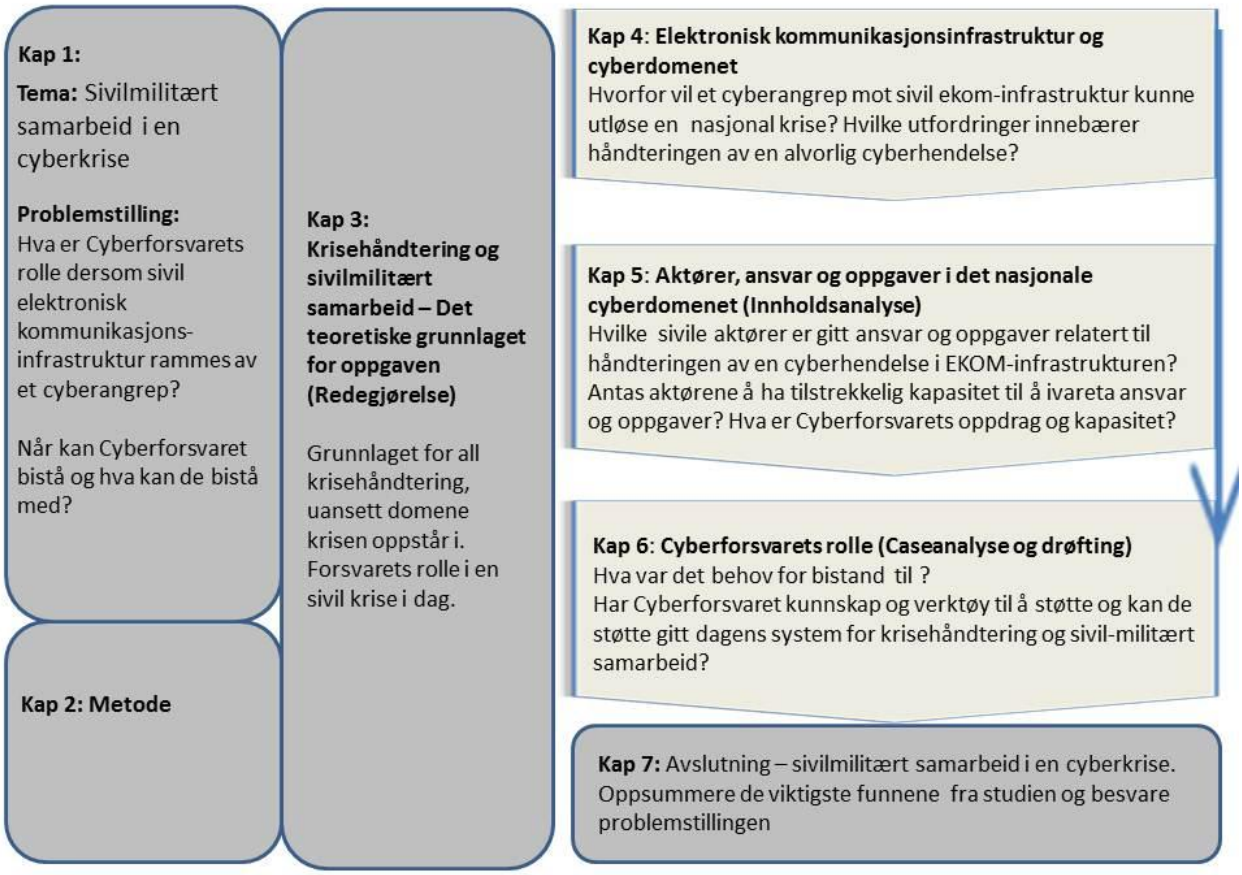
Kapittel tre skal etablere det teoretiske grunnlaget for oppgavens problemstilling. Utgangspunktet er at nasjonal krisehåndtering og regulering av sivil-militært samarbeid er uavhengig av domenet krisen oppstår i. Håndteringen av et cyberangrep mot ekom-infrastrukturen og en eventuell cyberkrise må forholde seg til det etablerte systemet.

Kapittel fire vil sette søkelyset på ekom-infrastruktur og cyberdomenet. Hensikten er å bidra til økt forståelse for hva ekom-infrastruktur *er* og hvorfor forstyrrelser i eller ødeleggelse av sivil ekom-infrastruktur kan forårsake en nasjonal krise – en cyberkrise. Og samtidig hva et cyberangrep innebærer og hvilke utfordringer en vil stå overfor i håndteringen av alvorlige cyberangrep.

Kapittel fem vil ta utgangspunkt i *Nasjonal strategi for informasjonssikkerhet* og kartlegge sentrale aktører og diskutere deres ansvar og oppgaver knyttet til ekom-infrastruktur og håndtering av cyberangrep. Hensikten er å indikere bistandsbehovet i sivil sektor samt hva Cyberforsvaret vil kunne bistå med.

Kapittel seks vil analysere to caser som innebar cyberangrep mot sivil infrastruktur. Caseanalysen vil ha fokus på de aktørene og oppgavene som ble kartlagt og diskutert i innholdsanalysen. Hvordan disse oppgavene ble håndtert og om ansvarlig aktør hadde behov for støtte. De oppgaver hvor det viser seg å være behov for støtte vil så drøftes fortløpende. Har Cyberforsvaret kunnskap og verktøy til å kunne støtte og kan Cyberforsvaret bistå gitt dagens prinsipper for krisehåndtering og regulering av det sivil-militære samarbeidet?

Kapittel sju vil oppsummere oppgaven og svare på hva som er Cyberforsvarets rolle dersom sivil elektronisk kommunikasjonsinfrastruktur rammes av et cyberangrep, herunder *når* de skal bistå og *hva* de kan bistå med?



Figur 2: Oppgaveskisse

2 Metode og kilder

2.1 Valg av metode

Den ene forskningsmetoden er ikke bedre enn den andre, - men de egner seg til å belyse ulike typer problemstillinger, sier Dag Ingvar Jacobsen, førsteamanuensis ved Høgskolen i Agder (Jacobsen, 2005, s. 87). Kunsten er å finne det undersøkelsesopplegget som er best egnet til å besvare den spesifikke problemstillingen.

Problemstillingen i denne oppgaven er *uklar*, - uklar på den måten at vi har lite forhåndskunnskaper om det som skal undersøkes. Det er mindre enn ett år siden Sundseth, daværende sjef Cyberforsvaret, selv etterlyste nærmere avklaringer om Cyberforsvarets samfunnsrolle (Kirknes, 2013). Som Sundseth påpekte eksisterer det ikke noen nasjonal cyberstrategi, og bistand fra Forsvaret til det sivile samfunn i forbindelse med cyberhendelser er så langt uprøvd. Problemstillingen blir dermed det som kalles *utforskende*, eller *eksplorerende* (Jacobsen, 2005, s. 67-84). Jacobsen skriver at eksplorerende problemstillinger krever en metode som får frem nyanserte data, går i dybden og er åpen for kontekstuelle forhold. Jeg valgte en kvalitativ metode, en kombinasjon av innholdsanalyse, casestudie og intervju.

Innholdsanalyse er en systematisk analyse av dokumenter og tekster (Ringdal, 2013). En teknikk hvor data deles inn i tema eller kategorier og deretter forsøker å finne sammenhengen mellom kategoriene (Jacobsen, 2005, s. 187). Denne studien fokuserer på håndtering av selve cyberhendelsen, herunder oppgavene å oppdage, varsle, analysere, koordinere og håndtere. *Nasjonal strategi for informasjonssikkerhet* viser ansvarsdelingen på et overordnet nivå. Ved å se dette dokumentet opp mot andre dokumenter og tekster kunne jeg kartlegge og diskutere hvilke aktører som er gitt ansvar, oppgaver og myndighet knyttet til ekom-infrastruktur og håndtering av cyberangrep og samtidig belyse aktørenes antatte kapasitet.

Dokumentene gir ikke klare svar, det var derfor hensiktsmessig å kombinere innholdsanalysen med en casestudie. En casestudie er en form for studie hvor selve studieobjektet er avgrenset i tid og rom (Cresswell, 2013; Jacobsen, 2005; Ringdal, 2013). Ringdal sier en case er en analyseenhet som er gjenstand for intensiv undersøkelse, og at en casestudie derfor gjerne bare

omfatter en eller noen få caser (Ringdal, 2013, s. 170). Etter Ringdal sin forståelse av casestudier kan casen være så mangt, eksempelvis individer, bedrifter, organisasjoner, hendelser og beslutninger. Han skriver videre at dataene kan samles inn på ulike måter, hvor samtaleintervju nevnes som en av flere. Jacobsen sin tolkning av casestudier er ikke så ulik Ringdal sin forståelse. Jacobsen sier en case kan være en spesiell situasjon, noe spesielt som har skjedd (Jacobsen, 2005, s. 87-101). Jeg valgte å se på to caser. Kriteriene for valg av caser var at de mest sentrale aktørene skulle være involvert i begge casene, casene måtte være av nyere dato og omhandle håndtering av et cyberangrep mot sivil infrastruktur. Samtidig ønsket jeg at Cyberforsvaret skulle ha ulik rolle i de to hendelsene. Det har vært mange reelle cyberhendelser de senere år, imidlertid er få av disse tilgjengelig for forskning da de fleste virksomhetene ønsker å holde informasjon om hendelsene for seg selv. Valget falt på den reelle cyberhendelsen hos Telenor i 2013 og øvelse CyberDawn i 2013. Bakgrunnen for valget av disse to er at Telenor gikk til media og informerte om angrepet de hadde vært utsatt for (heretter kalt *Industrispionasjesaken*), og gjorde det slik sett tilgjengelig for forskning, og *CyberDawn* er den eneste kjente norske cyberøvelsen hvor Forsvaret har hatt en aktiv rolle og støttet en sivil virksomhet gjennom bistand til politiet.

Intervjuene ble gjennomført som samtale intervjuer med basis i en intervjuguide (Ringdal 200 s 102-103). Intervjuguiden ble tilpasset det enkelte intervju og sendt respondenten i forkant. Spørsmålene varierte fra informant til informant. Ringdal sier denne typen intervju skal være velegnet for kvalitative studier fordi man oppnår fleksibilitet i intervjuet, samtidig som en åpen dialog mellom forsker og informant gjør at man kan få informasjon om tema eller opplysninger som ellers ikke ville ha kommet frem. Det er også min erfaring. Jeg gjennomførte 8 intervjuer. Oversikt over respondentene finnes i vedlegg 1. I oversikten finner man også dato for når intervjuet ble gjennomført samt lengde på intervjuet. Prosjektet er innrapportert til Personvernombudet for forskning og godkjent. Respondentene fikk tilsendt et informasjonsskriv i forkant (vedlegg 2). Informasjonsskrivet innehold opplysninger om studiens tema, hensikt samt hvordan intervjuet skulle gjennomføres. Respondentene ble bedt om å bekrefte at de hadde lest og forstått informasjonen og samtykket til å delta. Intervjuene ble tatt opp digitalt og lagret som lydfiler. Alle intervjuene er transkribert i ettertid.

2.2 Kilder

I boken *Mellom fred og krig, Norsk militær krisehåndtering* (Bjerga & Håkenstad, 2012b) drøftes Forsvarets rolle i nasjonal krisehåndtering i ulike perspektiver. Cyberforsvaret, cyberdomenet og cyberkriser er ikke omtalt, men boken bidrar med nyttig kunnskap om kriser og krisehåndtering i de andre domenene. Boken inneholder bidrag fra flere forfattere, deriblant Kjell Inge Bjerga, Magnus Håkenstad, Anders Kjølberg og Tormod Heier. Nasjonal krisehåndtering er også i søkelyset i boken *Strategisk ledelse i krise og krig* (Dyndal, 2010). Heller ikke i denne boken er cyber noe tema men Gjert Lage Dyndal og Bjørn Olav Heieraas bidrar med kunnskap om utfordringer knyttet til sivil-militært samarbeid både før og nå.

Generalmajor Sundseth, tidligere sjef i Cyberforsvaret (Sundseth, 2013), Kristin Bergtora Sandvik (Sandvik, 2013) og Morten Irgens (Irgens, 2013) bidrar med kunnskap direkte relatert til problemstillingen, henholdsvis til cybertrusler, juridiske utfordringer og cybersikkerhet.

Flere forskere ved FFI har bidratt med forskning på kritiske infrastrukturer og ekom. Disse rapportene er omtalt i kapittel 1.4 *Tidligere og pågående forskning*, og har primært blitt brukt til å etablere en kunnskapsplattform og til å definere og avgrense oppgaven.

Flere utredninger har synliggjort samfunnets avhengighet av kritisk infrastruktur og sårbarhet overfor svikt i disse. To nasjonale offentlige utredninger (NOU) som er verdt å utheve i denne sammenheng er *Sårbarhetsutvalget* (NOU 2000:24) og *Infrastrukturutvalget* (NOU 2006:6). Sårbarhetsutvalget bidrar med vurderinger knyttet til felles sivil-militær ressursbruk og utvikling av forholdet mellom politi og forsvar, og Infrastrukturutvalget gjør rede for kritisk infrastruktur og kritiske samfunnsfunksjoner. En tredje NOU som er relevant for oppgaven er *Rapport fra 22. juli-kommisjonen* (NOU 2012: 14, 2012). Utredningen omhandler hendelsen den 22. juli 2011 og fokuserer på trusler i det fysiske domenet, men utredningen bidrar med informasjon om viktige sider ved beredskapen og nasjonens evne til å beskytte seg mot angrep. Ved siden av disse tre nasjonale offentlige utredningene har DSB og Post- og teletilsynet (PT) gjennomført flere utredninger som gir viktig kunnskap om infrastrukturens sårbarhet, samfunnets sårbarhet overfor brudd i offentlige ekom-nett, og kunnskap om dagens ekom-marked.

Stortinget har siden Sårbarhetsutvalgets rapport, *Et sårbart samfunn,* behandlet flere stortingsmeldinger om samfunnssikkerhet og beredskap. De mest relevante for denne oppgaven er:

- St.meld. nr. 17 (2001 – 2002) *Samfunnssikkerhet – veien til et mindre sårbart samfunn* beskriver hva som ligger i begrepet samfunnssikkerhet. Forsøksprosjektet *Varslingssystem for digital infrastruktur* (VDI) er omtalt og robusthet i teleinfrastrukturen og beredskap er nevnt i meldingen.
- St.meld. nr. 39 (2003 – 2004) *Samfunnssikkerhet og sivilt-militært samarbeid* omtaler det nye totalforsvaret og det sivil-militære samarbeidet.
- St.meld. nr. 22 (2007 – 2008) *Samfunnssikkerhet – samvirke og samordning* fokuserer på betydningen av samvirke og samarbeid både nasjonalt og internasjonalt i møte med fremtidens risiko, trussel- og sårbarhetsbilde.
- Meld. St. nr. 29 (2011-2012) *Samfunnssikkerhet* gjennomgår samfunnets beredskap, læringspunkter og tiltak etter 22/7, samt flom kombinert med svikt i telenettene, ekstremvær og andre alvorlige utfordringer de siste årene. Samvirkeprinsippet introduseres og ansvarsforholdene rundt kritisk infrastruktur presiseres.
- Meld. St. nr. 21 (2012-2013) *Terrorberedskap* presenterer en overordnet strategi for å forebygge og håndtere terror i Norge. Meldingen har fokus på å videreutvikle de områder hvor Forsvarets ressurser kan supplere og komplementere sivil beredskap- og krisehåndtering.

Ved siden av disse stortingsmeldingene er det også brukt andre offentlige dokumenter, herunder lover, instrukser, proposisjoner, strategidokumenter og doktriner. De mest sentrale for studien er Nasjonal strategi for informasjonssikkerhet, FDs cyberretningslinjer og bistandsinstruksen, disse tre presenteres senere i oppgaven.

Industrispionasjesaken fikk mye omtale i media. Rune Dyrlie i Telenor informerte om hendelsen og håndteringen av den på NSM sin sikkerhetskonferanse i 2013 (NSMs sikkerhetskonferanse, 2013)[14], og Norman Shark har skrevet en omfattende rapport om hendelsen, *Operation Hangover Unveiling an Indian Cyberattack Infrastructure* (Fagerland, Kråkvik, & Camp, 2013).

[14] Videoene fra NSM sin sikkerhetskonferanse 2013 er ikke lengre tilgjengelig på den nettadressen som ligger i kildelisten, men antar de kan fremskaffes ved å kontakte NSM.

CyberDawn fikk mye medieomtale, både før, under og etter øvelsen. Det er laget en film basert på videopptak fra øvelsen, reggisert av Storm Jarl Landaasen og Kristin V. Tønnesen. Landaasen har gitt meg en kopi av filmen. Kortversjonen av filmen, *Cyberkriser må koordineres på tvers*, ligger tilgjengelig på internett (Tønnesen & Landaasen, 2013b). Etter øvelsen forfattet Rune Dyrlie og Storm Jarl Landaasen en sluttrapport med bidrag fra alle deltagerne, rapporten er ikke offentlig tilgjengelig men jeg har fått en kopi fra Telenor (Dyrlie & Landaasen, 2013).

Jeg har gjennomført 8 intervjuer. Respondentene er valgt ut fra sin stilling og kunnskap. Alle har tilknytning til virksomheter som vil inneha sentrale roller dersom problemstillingen skulle bli et faktum, herunder Telenor, NSM, Politidirektoratet (POD) og FD, FOH og Cyberforsvaret. De utvalgte respondentene er representanter for en kunnskap som få besitter og dermed sentrale for oppgaven[15].

2.3 Vurdering av metoden

Problemstillingen er uklar og eksplorerende. Jeg har søkt å kombinere flere metoder for å samle tilstrekkelig empiri til å kunne drøfte Cyberforsvarets rolle dersom sivil ekom-infrastruktur skulle bli rammet et av cyberangrep. Jacobsen påpeker at den ene kilden ikke er bedre enn den andre men at de gir ulik informasjon. Jeg har brukt et bredt utvalg av kilder, herunder faglitteratur, utredninger, stortingsproposisjoner, stortingsmeldinger, strategier, høringsnotat, lover, instrukser, interne dokumenter, rapporter, medieoppslag og intervjuer, for å styrke oppgaven. Utvelgelse av tekster samt begrenset forståelse og erfaring med kildekritikk og kontekstuelle forhold er likevel en fallgruve, men utstrakt bruk av referanser, og kildelisten, skal gjøre det mulig å etterprøve arbeidet.

Ringdal beskriver antall egnede caser som en utfordring ved casestudier. Det var tilfellet også i denne studien, men *industrispionasjesaken* og *CyberDawn* viste seg å være to veldig relevante caser. At den ene casen var en øvelse på initiativ av en privat aktør[16], kunne ha svekket studien. For eksempel deltok ikke Forsvares operative hovedkvarter (FOH), FD og JD på øvelsen, dette er aktører som alle ville hatt svært sentrale roller dersom dette hadde vært en reell hendelse. Imidlertid er det håndteringen på taktisk nivå som er kjernen i denne oppgaven ikke strategisk

[15] Oversikt over respondentene finnes i vedlegg 1. I oversikten finner man også dato for når intervjuet ble gjennomført samt lengde på intervjuet
[16] Krisehåndteringsøvelse i Telenor

krisehåndtering, så det svekket ikke studien i betydelig grad. For å kompensere intervjuet jeg representanter fra FOH og JD som kjente til øvelsen og politiinspektør i POD som deltok på øvelsen.

En svakhet ved bruk av intervju som metode er at intervju av enkeltpersoner gir enkeltpersoners meninger. Det kan ikke utelukkes at andre respondenter ville gitt andre svar, men jeg har tatt høyde for dette ved å intervjuet så mange som jeg hadde kapasitet til, og intervjuene er i all hovedsak brukt til å forsterke og utdype det som andre kilder allerede har indikert. Andre kjente utfordringer ved intervju er at intervjuer ubevisst kan stille ledende spørsmål og påvirke respondenten, samt at intervjuer kan notere og analysere feil (Jacobsen, 2005; Ringdal, 2013). Jeg har hatt disse feilkildene i bakhodet både ved forberedelse og gjennomføring av intervju, og har tatt opptak av intervjuene for å unngå å notere feil.

Ved å kombinere disse metodene, ta høyde for svakhetene og sammenstille funnene fikk jeg et godt grunnlag for å kunne drøfte problemstillingen.

Målsettingen med denne oppgaven er å gi økt innsikt i og forståelse for de utfordringer og muligheter som ligger i bruk av Cyberforsvarets ressurser i sivil krisehåndtering. Studien har vært tett knyttet til Telenor sin infrastruktur og virksomhet. Studien utelukker likevel ikke på noen måte at også andre ekom-virksomheter kan besitte samfunnskritisk infrastruktur, men Telenor viste seg å være den dominerende leverandøren av ekom-nett og ekom-tjenester i Norge, og fikk derfor en sentral plass i oppgaven. En annen ekom-virksomhet og andre caser kunne ha gitt andre funn. Men Cyberforsvarets kapasiteter er uansett det Cyberforsvarets kapasiteter er og det samme gjelder nasjonal krisehåndtering og regulering av sivil-militært samarbeid. Likevel, kriser er unike og vurderes og håndteres hver for seg, det er ikke lett å generalisere. Som Ringdal sier er regelmessigheter i samfunnet prinsipielt forskjellige fra naturlover fordi de kan oppheves ved at vi bestemmer oss for å handle annerledes (Ringdal, 2013).

3 Kriser og sivilmilitært samarbeid

Det vil være delte oppfatninger om hvordan kriser bør bli eller burde ha blitt håndtert. Utredninger, rapporter og medieoppslag etter 22/7-hendelsen er et godt eksempel. Det nasjonale systemet for krisehåndtering, hvordan kriser prinsipielt håndteres i Norge, og bruken av militære ressurser i fredstid er uavhengig av hvilket domene krisen oppstår i. Det er ikke gitt at systemet har tatt høyde for eller passer til alle hendelser, men håndteringen av dem må likevel forholde seg til det etablerte systemet. For å kunne drøfte Cyberforsvarets rolle i en sivilt ledet krise, er det derfor en forutsetning å ha kjennskap til og forståelse for dette systemet.

3.1 Krisehåndtering

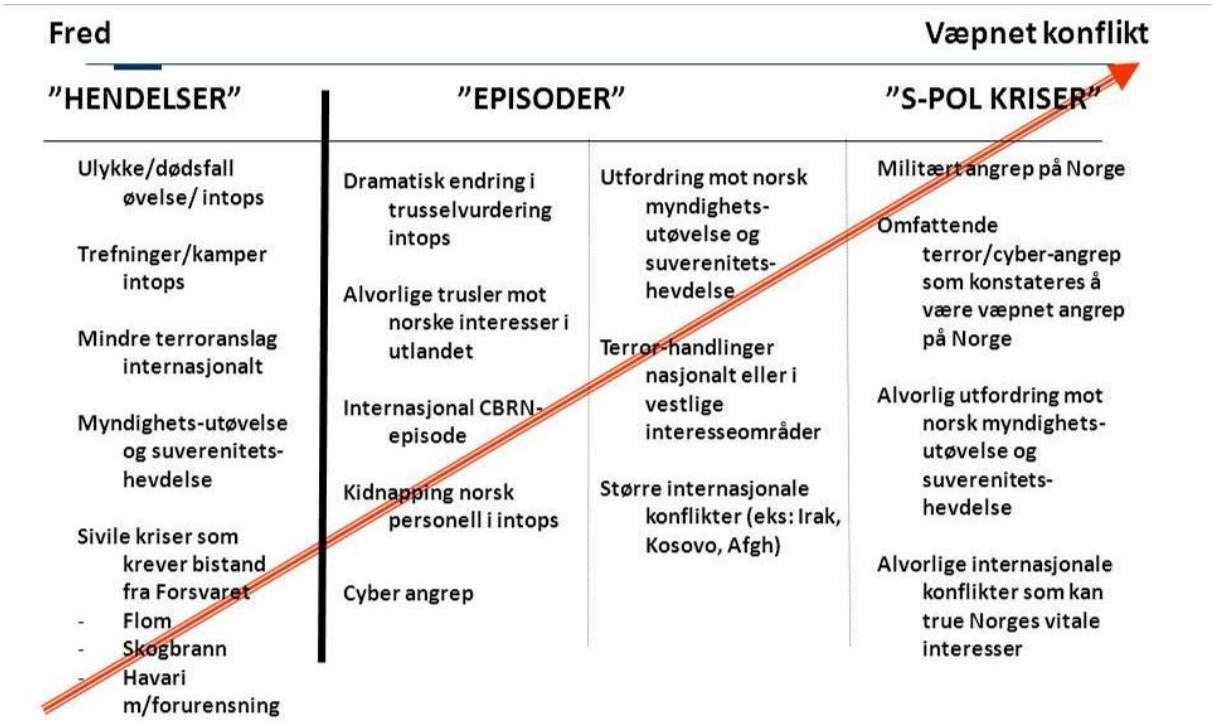
3.1.1 Hva definerer en krise?

Situasjoner som oppleves kritisk på taktisk nivå kan håndteres som en daglig operasjon på strategisk nivå – og motsatt. 27 % av norske virksomheter sier at de *opplever det kritisk* når IT-systemene er nede 1 time. Ytterligere 35 % av svarer at det er *kritisk for virksomheten* når viktige IT-systemer er nede 1 dag (Næringslivets sikkerhetsråd, 2012, s. 10). Men det er ikke nødvendigvis en nasjonal krise av den grunn.

Willoch-utvalget definerte en krise til å være «en hendelse som har potensiale til å true viktige verdier og svekke en organisasjons evne til å utføre viktige funksjoner» (NOU 2000: 24, 2000, s. 19). Politiet bruker Willoch-utvalgets definisjon av krisebegrepet og utdyper ved å si at krise er en «tilstand som kjennetegnes av at samfunnssikkerheten eller andre viktige verdier er truet, og at håndteringen utfordrer eller overskrider kapasiteten og/eller kompetansen til den aktøren som i utgangspunktet har ansvaret» (Politiet, 2011, s. 25). Politiets definisjon inneholder et annet begrep som også har manglet en tydelig definisjon, nemlig *samfunnssikkerhet*.
Samfunnssikkerhet ble i St. meld. nr. 17 (2001-2002) beskrevet som «den evne samfunnet som sådan har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger» (St. meld. nr. 17 (2001-2002), 2002, s. 4). Slik begrepet ble beskrevet i meldingen skulle det dekke et bredt spekter av utfordringer, fra begrensede, naturskapte hendelser, via større krisesituasjoner som representerer omfattende fare for liv, helse, miljø og materielle verdier, til sikkerhetsutfordringer som truer nasjonens selvstendighet eller eksistens. Begrepet ble senere avgrenset til «angrep og annen skade i

situasjoner der statens grunnleggende interesser ikke er truet» (St. meld nr. 37 (2004-2005), 2005, s. 50). Kort fortalt dreier samfunnssikkerhet seg om vern av samfunnet mot hendelser som truer og primæransvaret for samfunnssikkerhet ligger hos de sivile myndigheter. Det er JD som har hovedansvaret for å ivareta helheten i regjeringens politikk for samfunnssikkerhet, men Forsvaret kan bistå. Samarbeidet mellom sivile og militære myndigheter for å støtte opp under samfunnssikkerheten omtales som *sivil-militært samarbeid*. Forsvaret sier i siste langtidsplan at de vil gjøre sitt ytterste for å kunne bistå når det anmodes om det (Prop. 73 S (2011-2012)).

I sin tolkning av krise vektlegger Forsvaret tilgangen på ressurser og sier en «krise kan føre til at én myndighet eller etat alene ikke har ressurser til å håndtere krisen. I stedet vil det være nødvendig å konsentrere deler eller samtlige av statens tilgjengelige ressurser» (Forsvarsstaben, 2014: pkt 03026). Forsvarets bistand vil eventuelt være et supplement til sivile myndigheters krisehåndtering, og støtten skal primært være innenfor områder der etaten har kompetanse eller ressurser som andre ikke har. Forsvaret plasserer situasjoner ut i fra intensitet, geografiske omfang og varighet på en *konfliktskala* som vist i figur 3.



Figur 3: Konfliktskalaen (Forsvarsstaben, 2014: Figur 3.3)

Konfliktskalaen dekker alle situasjoner fra fred til krig. Imidlertid er ikke begrepene absolutte. Dyndal skriver at det er «flytende overganger mellom hendelser og episoder, kriser og sikkerhetspolitiske kriser og til sist krig». «Situasjoner som oppstår, oppleves ulikt av de forskjellige aktørene, og begrepene blir brukt forskjellig» (Dyndal, 2010, s. 13). Andre kjennetegn som er nevnt ved kriser er at «de kommer uventet og utvikler seg raskt og uforutsigbart» (NOU 2012: 14, 2012, s. 209). Aktørene vil kunne oppleve at det haster å få kontroll over situasjonen, samtidig som den vanlige beslutningsprosessen oppleves som uhensiktsmessig eller ikke-fungerende. Selv om det ikke finnes noen absolutt definisjon på hva en krise *er*, gir disse sitatene oss et bilde av at en krise *kan være.*

3.1.2 Sentrale prinsipper for beredskap og krisehåndtering

Dagens modell for beredskap og krisehåndtering er tuftet på fire prinsipper: ansvar, likhet, nærhet og samvirke. De tre første prinsippene ble introdusert i St.meld. nr. 17 (2001-2002) *Samfunnssikkerhet – veien til et mindre sårbart samfunn*, mens det siste prinsippet ble lagt frem i Meld. St 29 (2011-2012) *Samfunnssikkerhet.*

Ansvarsprinsippet innebærer at den virksomhet, myndighet eller etat som har ansvar for et fagområde til daglig også har ansvar for å håndtere ekstraordinære hendelser på området (Meld. St. nr. 29 (2011-2012), 2012, s. 39). Kritisk infrastruktur er ikke noe unntak: ”Ansvar for beskyttelse av kritisk infrastruktur ligger til eier eller operatør av infrastrukturen og følger sektoransvaret” (St. meld nr. 22 (2007-2008), 2008, s. 40). I praksis innebærer ansvarsprinsippet at eier av infrastrukturen må sørge for de nødvendige beredskapsforberedelser, herunder å planlegge hvordan funksjoner innenfor eget ansvarsområde skal kunne opprettholdes og videreføres dersom det inntreffer en ekstraordinær hendelse, - eksempelvis et cyberangrep. For å ivareta sitt ansvar må virksomheten sørge for å ha tilstrekkelige avtaler med sine underleverandører og andre for å sikre seg hjelp i tilfelle kriser (Brattekås, Hagen, & Sandrup, 2011, s. 43). Det er ministeren som sitter med det overordnede ansvaret for sin sektor. Det overordnede ansvaret innebærer å peke ut og sikre kritisk infrastruktur i egen sektor, iverksette nødvendige forebyggende tiltak, forberede beredskapstiltak og krisehåndtering samt føre tilsyn med informasjonssikkerheten i egne underliggende etater (Meld. St. nr. 29 (2011-2012), 2012). En krise som oppstår på bakgrunn av et cyberangrep mot en teleoperatør vil innledningsvis høre inn under samferdselsministeren sitt ansvarsområde. Dersom angrepet i stedet rammet prosesskontrollsystemet i et oljeselskap ville krisen ha sortert under Olje og Energidepartementet

(Brattekås et al., 2011, s. 19). Dersom ansvarlig minister ikke har nødvendig kompetanse eller ressurser i sin sektor for å håndtere situasjonen vil det være nødvendig å koordinere med andre departementer og etater, men det konstitusjonelle ansvaret for å løse oppgavene i sin sektor ligger like fullt hos den enkelte fagstatsråd (NOU 2006: 6, 2006, s. 150).

Likhetsprinsippet innebærer at den organisasjonen en opererer med under kriser skal være mest mulig lik den en opererer med i det daglige. Prinsippet henger tett sammen med ansvarsprinsippet og understreker at ansvarsforholdene internt i og mellom virksomheter ikke skal endres i forbindelse med krisehåndtering området (Meld. St. nr. 29 (2011-2012), 2012, s. 39). Slik vil personellet kunne forholde seg til kjente prosedyrer, regelverk og ansvarslinjer.

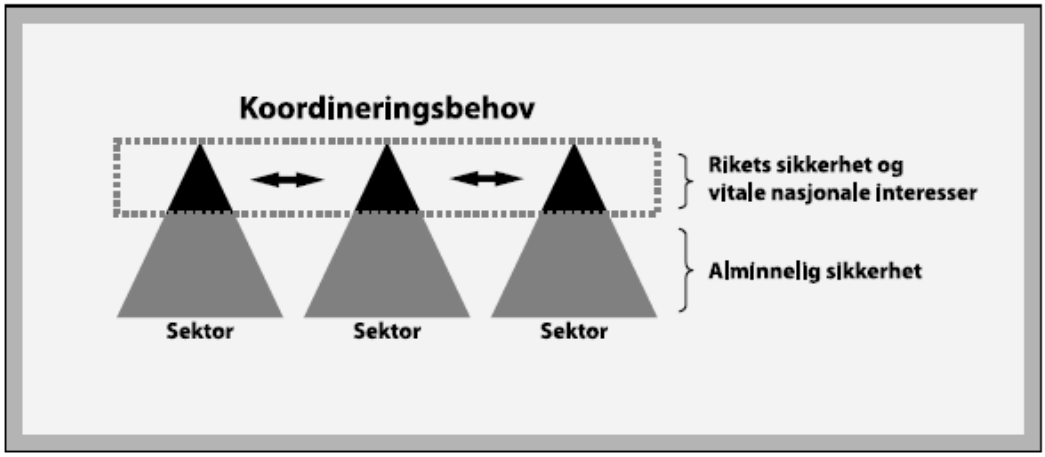
Nærhetsprinsippet innebærer at situasjonen skal håndteres på så lavt nivå som mulig. Også dette prinsippet er tett knyttet til ansvarsprinsippet, - en krise innenfor en virksomhets ansvarsområde er det virksomhetens ansvar å håndtere. «Departementenes hovedfunksjon i det daglige er å være sekretariat for den politiske ledelsen, og det er viktig at departementene i krisesituasjoner ikke overtar oppgaver som best kan utføres av de operative nivåene underlagt departementet» (St. meld nr. 37 (2004-2005), 2005, s. 32). De som står nærmest vil dessuten ha best kjennskap til de lokale forhold og normalt kunne yte den raskeste og mest målrettede assistansen (NOU 2006: 6, 2006, s. 150). Prinsippet innebærer at kriseledelse må kunne ivaretas like godt på lokalt nivå som på sentralt nivå. Det ideelle er at beslutninger fattes så lavt som mulig, men likevel på tilstrekkelig høyt nivå til at de overordnede nasjonale målsettinger blir ivaretatt. Jo større krisen er desto mer sentralisert krisehåndtering vil det være behov for. Av den grunn gjelder ikke nærhetsprinsippet ved sikkerhetspolitiske kriser (Meld. St. nr. 29 (2011-2012), 2012, s. 39).

Det siste prinsippet, *samvirkeprinsippet,* innebærer at alle myndigheter, virksomheter og etater har et selvstendig ansvar for å samvirke best mulig med relevante aktører og virksomheter i arbeid med forebygging, beredskap og krisehåndtering (NOU 2012: 14, 2012, s. 70). Prinsippet ble lagt frem i stortingsmeldingen *Samfunnssikkerhet* i juni 2012. Bakgrunnen var erfaringer fra hendelser som hadde illustrert et forsterket behov for samordning og samhandling mellom ulike aktører, herunder angrepene 22. juli 2011, samt ekstremvær og flom kombinert med svikt i telenettet samme år. Hensikten var å tydeliggjøre regjeringens samlede ansvar for samfunnssikkerhet og beredskap på tvers av sektorgrenser (Meld. St. nr. 29 (2011-2012), 2012).

Regjeringen sier ansvar og samvirke skal være overordnet og styrende, særlig ved større sektorovergripende kriser (Høyre-Frp-Regjeringen, 2013).

3.1.3 Det strategiske lederapparatet

Ikke alle kriser kan løses innenfor departementets myndighetsområde. Dersom krisen er så alvorlig eller kompleks at den ikke kan håndteres av sektoren alene vil det være behov for en sentral kriseledelse. «I slike situasjoner vil det være behov for informasjonsdeling og koordinering av planer og ressurser for krisehåndtering på tvers av ansvarslinjene» (NOU 2006: 6, 2006, s. 150). *Infrastrukturutvalget* skisserte denne koordineringen som vist i figur 4:



Figur 4: Koordinering på strategisk nivå (NOU 2006: 6, 2006, s. 56: Figur 5.1).

Stortinget besluttet i 2005, i kjølvannet av flodbølgekatastrofen i jula i 2004, å basere strategisk krisehåndtering på tre hovedelementer: lederdepartement, Kriserådet[17] og Krisestøtteenheten. Hvem som skal ha rollen som lederdepartement skulle besluttes ut fra faktorer som: krisens karakter, hvem som hadde mest informasjon og best tilgang til informasjon om krisen, samt hvem som hadde de riktige virkemidlene for å håndtere krisen (St. meld nr. 37 (2004-2005), 2005, s. 31). I ettertid har det imidlertid blitt besluttet at «Justis- og beredskapsdepartementet skal være fast lederdepartement for sivile nasjonale kriser med mindre noe annet er bestemt» (Meld. St. nr. 29 (2011-2012), 2012, s. 7). Det er lederdepartement som skal ivareta samordningen mellom departementene i mindre alvorlige kriser, mens Kriserådet skal sørge for samordningen i komplekse kriser. Kriserådet er det høyeste koordineringsorganet på

[17] Den gang kalt Regjeringens kriseråd. Regjeringen besluttet i 2012 å endre navn til Kriserådet for å unngå *«usikkerhet utad om når møtet finner sted på politisk nivå og om når møtet finner sted på administrativ nivå»* (Meld. St. nr. 29 (2011-2012), s. 69). Kriserådet har fem faste medlemmer: regjeringsråden ved Statsministerens kontor,

administrativt nivå. Alle departementsrådene kan kalle inn til og etablere Kriserådet. En av de viktigste oppgavene til dette rådet er å vurdere hvem som bør lede krisen. I tillegg har rådet ansvar for å koordinere tiltak i de ulike sektorene som er involvert i krisen, informasjon til publikum og media samt å ivareta regjeringens beslutningsunderlag. Det departementet som utpekes til lederdepartement i en krisesituasjon skal også lede Kriserådet. Krisestøtteenheten (KSE) er et permanent, dedikert sekretariat for sivil krisehåndtering. Enheten ligger organisatorisk under JD men skal bistå lederdepartement og Kriserådet i deres krisehåndtering. Verken lederdepartement, Kriseråd eller KSE rokker ved ansvarsprinsippet, det konstitusjonelle ansvaret ligger fortsatt hos statsrådene i hvert enkelt departement.

3.1.4 Hvem eier krisen, - sivile eller militære myndigheter?

Bjerga og Håkenstad skriver at det i de fleste tilfeller er det krisens årsak som definerer krisen. Hvem som *eier* krisen og således har ansvar for å lede håndteringen av den avhenger av hva slags krise vi står overfor. Avhengig av om det er en *militær* eller en *sivil krise* vi står overfor, skal den håndteres av henholdsvis militære eller sivile myndigheter. De militære krisene består av krig og sikkerhetspolitiske kriser for øvrig (Bjerga & Håkenstad, 2012a, s. 58). Krig innebærer et væpnet angrep på Norge mens sikkerhetspolitisk krise er en krise hvor Norges territorielle integritet, politiske suverenitet eller økonomiske livsgrunnlag utfordres av fremmed makt eller andre internasjonale aktører uten at det nødvendigvis dreier seg om et militært angrep i tradisjonell forstand (NOU 2012: 14, 2012, s. 209). Imidlertid vil det kunne være vanskelig å umiddelbart fastslå hvilken type krise man står overfor. I FFOD bemerkes det at Forsvaret har et selvstendig ansvar i, det de kaller, *nasjonale kaossituasjoner*, herunder omfattende cyberangrep, hvor det er uklart om Norge står overfor en krise eller væpnet konflikt (Forsvarsstaben, 2014: pkt 03032). I PBS1 eller den offentlige utredningen fra 2006, *Når sikkerheten er viktigst*, eksisterer ikke begrepet *kaossituasjoner*, men politiets ansvar for den operative håndteringen i terror og sabotasjesituasjoner fremheves: «Politiet skal lokalisere og pågripe gjerningsperson(er) som har iverksatt eller truer med å iverksette slike handlinger i fred, krise eller krig, såfremt det åpenbart ikke er stridshandlinger utført av militære stridskrefter tilhørende en fremmed makt» (NOU 2006: 6, 2006, s. 151). Stridshandlinger med opprinnelse utenfor Norges grenser er et grunnvilkår for å kunne konstatere et væpnet angrep på Norge. Bjerga og Håkenstad mener at det i lys av hendelsen den 22.juli og regjeringens umiddelbare beslutning om at det var en sivil krise er grunn til å stille spørsmål ved hva som skal til for at et anslag vurderes til å være en

---

utenriksråden i Utenriksdepartementet og departementsrådene i Helse- og omsorgsdepartementet, JD og FD. I

sikkerhetspolitisk krise. De sier at kanskje alle kriser i fremtiden «som ikke innebærer en eksplisitt fiendtlig, militær inntrengning på norsk territorium vil defineres som sivile kriser og håndteres der etter» (Bjerga & Håkenstad, 2012a, s. 74).

3.2 Sivil-militært samarbeid

Samfunnssikkerhet innebærer vern av samfunnet mot hendelser som truer befolkningens trygghetsfølelse samt viktige samfunnsinstitusjoner og infrastruktur. Det er de sivile myndigheter som har primæransvaret for å ivareta samfunnssikkerheten i Norge. Forsvaret på sin side har ansvar for statssikkerheten, som innebærer ivaretagelse av suverenitet, territoriell integritet og politisk handlefrihet. Politiet skal sørge for landets indre sikkerhet mens Forsvaret skal ivareta rikets sikkerhet i forhold til eksterne trusler. Sivilmilitært samarbeid omhandler samarbeidet mellom sivile og militære myndigheter for å støtte opp under samfunnssikkerheten og Forsvaret har i siste langtidsplan sagt at de vil gjøre sitt ytterste for å kunne bistå når det anmodes om det. Det er likevel ikke slik at dette er helt uproblematisk.

3.2.1 Et historisk tilbakeblikk på det sivil-militære samarbeidet

Bjørn Olav Heieraas hevder at uenighet rundt «hva militærmakt skal brukes til, og mot hvem den kan brukes» har gjort bruken av militære styrker til et følsomt tema, fra innføringen av allmenn verneplikt og frem til i dag (Heieraas, 2010, s. 104). I Menstadslaget i 1931 ble et gardekompani og fire marinefartøyer satt inn for å støtte politiet, mot demonstranter. Dyndal og Simonsen fremhever i sin beskrivelse av hendelsen at det aldri ble direkte konfrontasjon mellom soldater og demonstranter, men at hendelsen likevel skapte debatt og fikk betydning for folks syn på bruken av militære styrker. De mener hendelsen i for stor grad har påvirket tolkning og nyutvikling av lover og reguleringer i Norge i ettertid (Dyndal & Simonsen, 2013).

Det var erfaringer fra 1940 og faren for en ny storkrig som førte til etableringen av etterkrigstidens totalforsvar. 15.desember i 1950 trådde beredskapsloven i kraft (Beredskapsloven, 1950). Loven gir konge (regjering) og militære myndigheter vide fullmakter til å disponere samfunnets sivile ressurser i tilfelle krig. Totalforsvarskonseptet skulle sørge for at alle landets ressurser skulle kunne nyttes for å verne om nasjonale interesser, verdier, territorium, samfunn og befolkning. Heieraas mener muligheten for bruk av militær makt i

---

tillegg til disse faste medlemmene kan andre delta ved behov.

fredstid likevel var svært begrenset frem til etableringen av 200-milssonen i 1976. Men ved opprettelsen av Kystvakten i 1977, Forsvarets spesialkommando (FSK) i 1982 og Indre Kystvakt i 1996, ble Forsvaret gradvis en aktør på områder som tidligere hadde vært forbeholdt politiet. Heieraas beskriver den generelle utviklingen som økt bruk av militær støtte til løsning av sivile samfunnsoppgaver (Heieraas, 2010, s. 102). Faren for ny storkrig ble gradvis mindre, og etter at den kalde krigen tok slutt har beredskapsarbeidet dreid seg i retning av å kunne forebygge og håndtere kriser i fredssituasjoner. Imidlertid har planverket hatt stort fokus det siste året og det er for tidlig å si hvilke konsekvenser utfordringene i Ukraina vil få, kanskje tradisjonell sikkerhetspolitikk og krisehåndtering igjen blir mer sentralt?

3.2.2 Begrenset mulighet for bruk av militær ressurser i fredstid

Begrensningene for militær maktbruk mot egne borgere er beskrevet i Grunnloven, fra 1814. I §99 annet ledd står det: «Regjeringen er ikke berettiget til militær Magts Anvendelse mod Statens Medlemmer, uden efter de i Lovgivningen bestemte Former, medmindre nogen Forsamling maatte forstyrre den offentlige Rolighed og den ikke øieblikkelig adskilles, efterat de Artikler i Landsloven, som angaare Oprør, ere den trende Gange lydeligen forelæste af den civile Øvrighed» (Grunnloven, 1814).

Regjeringen har altså i utgangspunktet ikke anledning til å anvende militær makt mot statens borgere, med unntak om at maktbruken er hjemlet i formell lov, eller dersom en forsamling forstyrrer den offentlige ro og orden og ikke oppløser seg selv etter at straffelovens opprørsparagrafer er blitt opplest av politiet. Det innebærer at Forsvarets bistand til politiet, i utgangspunktet skal begrunnes i en lovhjemmel. Forsvarets bistand til politiet har imidlertid så langt vært regulert i kongelige resolusjoner, av henholdsvis 1965, 1998, 2003 og senest 22.juni 2012, men FD foreslo i 2013 å lovfeste Forsvarets bistand til politiet i en egen lov (Regjeringen, 2013a). I høringsnotatet *Om lov om Forsvarets ansvar for å avverge luftbårne terroranslag og Forsvarets bistand til politiet* skriver FD at «Det er imidlertid lang og fast praksis for at dagens former for bistand, slik disse er beskrevet i bistandsinstruksen - alminnelig bistand og håndhevelsesbistand, faller utenfor det alminnelige grunnslovforbudet. For dagens typer bistand er derfor lovforankring ikke ansett påkrevet» (Forsvarsdepartementet, 2013).

Om det er behov for lovforankring eller ikke, har imidlertid vært og er fortsatt svært omdiskutert. Jon Petter Rui, førsteamanuensis/post.doc. ved Det juridiske fakultet, Universitetet i Tromsø, skrev i 2011 artikkelen *Politiets behov for støtte i fra Forsvaret: Lovgivning er nødvendig*. Rui beskrev Forsvarets bistand i forbindelse med naturkatastrofer, større ulykker eller søk etter savnede personer som ukontroversielt. Forsvarets bistand til politiet med forebygging og bekjemping av straffbare forhold var derimot ikke like greit. «Det må anses som sikkert at Forsvaret uten hjemmel i formell lov ikke kan gi støtte til politiet, hvis formålet med operasjonen er at Forsvarets personell skal utøve fysisk makt overfor sivile borgere» (Rui, 2011, s. 445). Han avsluttet med å si at tiden er moden for at Stortinget tar stilling til om og eventuelt i hvilken utstrekning Forsvaret skal kunne bruke makt mot sivile borgere når det ytes støtte til politiet samt at klare prosedyrer for bistanden og ansvarsforhold lovfestes.

Lovforslaget har som nevnt vært på høring og «Forsvarsdepartementet tar sikte på å fremme en lovproposisjon så snart som mulig» (Regjeringen, 2013a).

3.2.3 Det nye totalforsvarskonseptet

Sårbarhetsutvalget, tok - under ledelse av Willoch - for seg problemstillinger knyttet til felles sivil-militær ressursbruk og utvikling av forholdet mellom politi og forsvar. Utvalget hevdet at rutinene for bistand til politiet var for byråkratiske, og kunne bidra til for lang beslutningsprosess. Samfunnet stod overfor en voksende og vanskelig definerbar risiko, som følge av bevisste handlinger i en gråsone mellom fred og krig. Utvalget argumenterte for at det var viktig å utvikle samarbeidet mellom politiet og Forsvaret, fordi politiet hadde begrenset kapasitet til å møte de nye utfordringene samfunnet stod overfor. Forsvaret skulle gi støtte til det sivile samfunn i fredstid, så fremt det var forenlig med Forsvarets primære oppgaver. Fare for anslag av omfattende skadevoldende karakter rettet mot vesentlige samfunnsinteresser ble oppgitt som en situasjon hvor det kunne være aktuelt med bistand fra Forsvaret (NOU 2000: 24, 2000, s. 55). Utvalget etterlyste en avklaring på hvordan samvirket mellom politi og militære styrker skulle kunne etableres i det som ble vurdert som særlig kritiske situasjoner uten at det krevde medvirkning fra vedkommende departementer. De fryktet at beslutningsprosessene skulle ta for lang tid, og at tapene derfor kunne blir større enn nødvendig. Fleksibel holdning til bruk av militære styrker ble vurdert som avgjørende for landets beredskapsmessige slagkraft, samtidig ble det poengtert at det ikke skulle bety en utvisking av skillet mellom sivilt og militært ansvar. Utvalget kunne ikke vise til klare eksempler på hvorfor det skulle være behov for å justere instruksverket på området, siden det ikke hadde vært noe omfattende tilfelle av slik terror, som

man ønsket sterkere beskyttelse mot. Utvalget anbefalte likevel gjennomgang av regelverk og prosedyrer (NOU 2000: 24, 2000, s. 54-59).

Terrorangrepene 11. september 2001 viste hvor sårbart det moderne samfunnet faktisk var blitt og at fredstidshendelser kan ha stort skadeomfang. Regjeringen hadde angrepene friskt i minne da stortingsmeldingen *Samfunnssikkerhet -Veien til et mindre sårbart* ble skrevet. Regjeringen erkjente at samfunnet kunne bli stilt overfor alvorlige trusler som ikke var knyttet til en trussel om invasjon. Situasjoner hvor samfunnet ville settes på prøve og det kunne bli nødvendig med ekstraordinær innsats. Erkjennelsen gjorde det nødvendig å vurdere prinsippene for samarbeid mellom Forsvaret og politiet (St. meld. nr. 17 (2001-2002), 2002, s. 7-10). Totalforsvaret skulle videreutvikles for å sikre at samfunnet hadde en gjennomgående sikkerhet og beredskap. For å styrke samordningen av samfunnssikkerhetsarbeidet fikk Justisdepartementet et tydeligere samordningsansvar. Dette innebærer blant annet ansvar for forebyggende sikkerhetstjeneste i sivil sektor.

I 2003 kom det ny instruks for Forsvarets bistand til politiet. I kgl.res. av 28. februar 2003 ble bistand delt i tre kategorier: administrativ bistand, operativ bistand og håndhevelsesbistand. Den militære innsatsen skulle fortrinnsvis konsentreres om vakthold, sikring og dekning. Stortingsmeldingen *Samfunnssikkerhet og sivilt-militært samarbeid* kom ut året etter og ga totalforsvarssamarbeidet et mer helhetlig innhold. Totalforsvarssamarbeidet skulle som før omfatte krig og sikkerhetspolitiske kriser, men det ble nå påpekt at kriser også skulle omfatte alvorlige og omfattende terrorhandlinger. *Det nye totalforsvarskonseptet* skulle bestå av «gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn om både forebygging, beredskapsplanlegging og operative forhold» (St. meld nr. 39 (2003-2004), 2004, s. 15). Samarbeidet mellom FD og JD om etatsstyringen av NSM ble presentert som et eksempel på sivilt-militært samarbeid innenfor det nye totalforsvarskonseptet (St. meld nr. 39 (2003-2004), 2004, s. 17). Forsvaret skulle kunne bidra til samfunnssikkerhet med tilgjengelige kapasiteter, kompetanse og ressurser og den videre moderniseringen av Forsvaret skulle legge til rette for at Forsvarets ressurser i større grad kunne tas i bruk til støtte for politiet og sivile myndigheter. Det ble imidlertid fastslått at bistand bare skulle gis under den forutsetning at politiets personell og materielle ressurser ikke strakk til, og den militære innsatsen skulle fortrinnsvis konsentreres om vakthold, sikring og dekning (St. meld nr. 39 (2003-2004), 2004, s. 23). Det ble gjort oppmerksom på at det var sterkt begrenset adgang for militært personell til å gi

håndhevelsesbistand. Bakgrunnen til denne restriktive holdningen var at håndhevelsesbistand kunne ha politiske implikasjoner, og spørsmålet om slik bistand skulle derfor behandles i Justisdepartementet i samråd med FD (St. meld nr. 39 (2003-2004), 2004, s. 23).

Infrastrukturutvalget forklarte hvordan endringer i samfunnets struktur og trusselbildet krevde større fokus på sivile enn militære utfordringer og at dette medførte større vekt på hva Forsvaret kan gjøre for å bistå det sivile samfunnet enn hva det sivile samfunnet kan gjøre for å forsvare landet mot en ekstern fiende. Telenettet ble brukt som et eksempel. Sikring av telenettet var ikke lengre begrunnet ut fra en totalforsvarstankegang, men ut fra det sivile samfunns avhengighet av tele-tjenester (NOU 2006: 6, 2006, s. 41). Utvalget mente det var vanskelig å «spesifisere de dimensjonerende scenariene for arbeidet med samfunnssikkerhet og sivil-militært samarbeid og ikke minst hvem som har ansvaret for å håndtere ulike trusler» (NOU 2006: 6, 2006, s. 189). Utvalget anbefalte å etablere møteplasser for offentlige og private virksomheter hvor de kunne treffes «for å drøfte hva det aktuelle trussel-, risiko- og sårbarhetsbilde har å si for deltakerne, hvilke handlingsalternativer som kan og bør iverksettes, samt oppfølgingen av iverksatte tiltak» (NOU 2006: 6, 2006, s. 20).

St.meld. nr. 22(2007–2008) *Samfunnssikkerhet - Samvirke og samordning* innledet med å fastslå at Regjeringens viktigste oppgave er å forebygge hendelser og kriser, men at dersom de likevel oppstår skal målet være å håndtere de raskt og effektivt ved bruk av samfunnets nasjonale ressurser. Det påpekes i meldingen at Forsvaret skal gi bistand til det sivile samfunn når viktige samfunnsinteresser og liv og helse står på spill, og at dette dreier seg om bistand både til politiet og til det øvrige sivile samfunn. NSM skulle bidra med kompetanse og tilsynsvirksomhet innenfor forebyggende sikkerhet, og da spesielt informasjonssikkerhet. NorCERT ble beskrevet som et viktig bidrag i å styrke den nasjonale beredskapen mot IT-angrep. NorCERT skulle utvikle et system for å ivareta koordinert respons og gjenoppretting dersom virksomheter med ansvar for samfunnskritiske funksjoner ble rammet av et angrep. Erkjennelsen av at disse utfordringene treffer på tvers av sektorer og etater gjorde at det ble etablert en koordineringsgruppe med representanter fra E-tjenesten og Politiets sikkerhetstjeneste (PST) for å sikre en helhetlig beskrivelse av IKT-trusselbildet.

Regjeringen påpekte at Forsvaret har et vidt spekter av ressurser som kan stilles til rådighet for det sivile samfunn i krisesituasjoner, men samtidig har Forsvaret færre mannskaps- og

materiellressurser til å yte bistand nå enn før. Utgangspunktet er at sivile kriser håndteres med sivile ressurser, og dersom det er behov for bistand må Forsvaret involveres tidlig i krisen «slik at relevante ressurser kan identifiseres og stilles til rådighet til rett tid» (St. meld nr. 22 (2007-2008), 2008, s. 71).

Rådighet over relevante ressurser var noe av det som manglet da samfunnet ble satt på prøve 22. juli 2011. Forsvarets fokus var fra første øyeblikk rettet mot å kunne bistå politiet med relevante støttekapasiteter. Forsvarsminister Faremo hadde gitt klar melding om å «støtte politiet med det de anmoder om» (NOU 2012: 14, 2012, s. 242). Forsvaret var derfor proaktiv, kalte inn mannskaper og startet å klargjøre materiell i påvente av bistandsanmodninger. Det kom i alt fem bistandsanmodninger hvorav samtlige omhandlet en eller annen form for håndhevelsesbistand (NOU 2012: 14, 2012, s. 243). *22. juli-kommisjonens* erfaring var at samarbeidet mellom etatene hadde fungert godt og at anmodningene hadde blitt ekspedert raskt (NOU 2012: 14, 2012, s. 160). Konklusjonen er at Forsvaret evnet å klargjøre de kapasiteter som ble etterspurt og løste sitt oppdrag på en tilfredsstillende måte. Oppdraget kunne imidlertid ha vært større. Kommisjonen indikerer at politiet burde ha tatt i bruk bistandsinstruksen tidligere og mer proaktivt (NOU 2012: 14, 2012, s. 245). Kommisjonen mente det var nødvendig å videreutvikle samhandlingen mellom politiet og Forsvaret (NOU 2012: 14, 2012, s. 146).

3.2.4 Økt fokus på Forsvarets bistand til politiet – ny bistandsinstruks

Etter terroranslaget 22.juli 2011 ble det et stort fokus på å forbedre ivaretagelse av samfunnssikkerheten i Norge – herunder det sivil-militære samarbeidet og Forsvarets bistand til politiet spesielt. Regjeringen redegjorde for viktigheten av dette arbeidet i stortingsproposisjon *Et forsvar for vår tid* (2011-2012) og stortingsmeldingen *Samfunnssikkerhet* (2011-2012).

I *Et forsvar for vår tid* påpekes det at angrep i det digitale rom er en av de raskest voksende truslene. Det forventes at truslene vil fortsette å øke og bli mer komplekse, og at det vil kunne skape utfordringer for kritisk infrastruktur, som telekommunikasjon. Selv om de fleste hendelsene så langt har vært spionasjeangrep kan utviklingen gå i retning av å sabotere kritisk infrastruktur. «Stans i kommunikasjonslinjene kan være en trussel både mot samfunns- og statssikkerheten» (Prop. 73 S (2011-2012), s. 22). Det bringes på det rene at Forsvaret kan bistå sivile myndigheter ved hendelser i cyberdomenet etter de samme prinsipper og regler som for

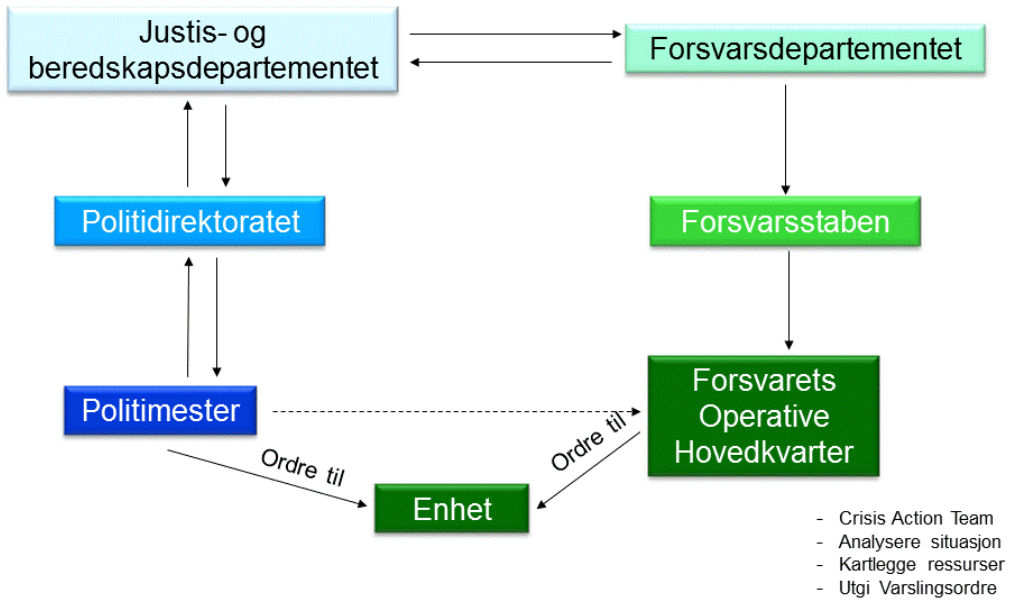
annen militær bistand til samfunnssikkerhet. Det påpekes i samme dokument at Forsvaret også yter bistand til andre sivile myndigheter enn politiet og at det allerede før 22. juli 2011 var igangsatt et arbeid med å utarbeide en egen instruks om Forsvarets bistand til andre sivile myndigheter enn politiet[18]. «I slike tilfeller er det viktig å unngå at Forsvaret påtar seg oppgaver som bør, kan eller skal ivaretas av sivile aktører» (Prop. 73 S (2011-2012), s. 54).

Terrorangrep utført i Norge av ikke-statlige aktører skal i utgangspunktet, slik det er beskrevet i stortingsmeldingen *Samfunnssikkerhet,* håndteres som alvorlig kriminalitet, og hører slik innunder ansvarsområdet til politiet og påtalemyndigheten. Regjeringens målsetting er imidlertid at «Forsvaret alltid skal være beredt til å bistå politiet med tilgjengelige og relevante kapasiteter i forbindelse med terror og annen alvorlig kriminalitet» (Meld. St. nr. 29 (2011-2012), 2012, s. 98). I den samme meldingen ble det uttalt at Forsvaret kanskje vil måtte bistå politiet med andre former for bistand enn det som var hjemlet i instruks og sedvanerett. Bistandsinstruksen skulle derfor gjennomgås på nytt, med fokus på anvendelsesområde, prosedyrer og kommandoforhold (Meld. St. nr. 29 (2011-2012), 2012).

22. juni 2012 ble den nye bistandsinstruksen vedtatt. Instruksen gjelder for Forsvarets bistand til politiet i fred, krise og krig. Med bistand menes all form for støtte, herunder både personell og materiell. Den nye instruksen slår sammen de tidligere tre bistandsformer til to: alminnelig bistand og håndhevelsesbistand. I § 5, som beskriver forutsetningen for bistand, er ordlyden endret til at politiets ressurser *normalt* skal være *uttømt eller funnet utilstrekkelig* for å løse oppdraget. Det kan se ut til at terskelen for å be om bistand er senket.

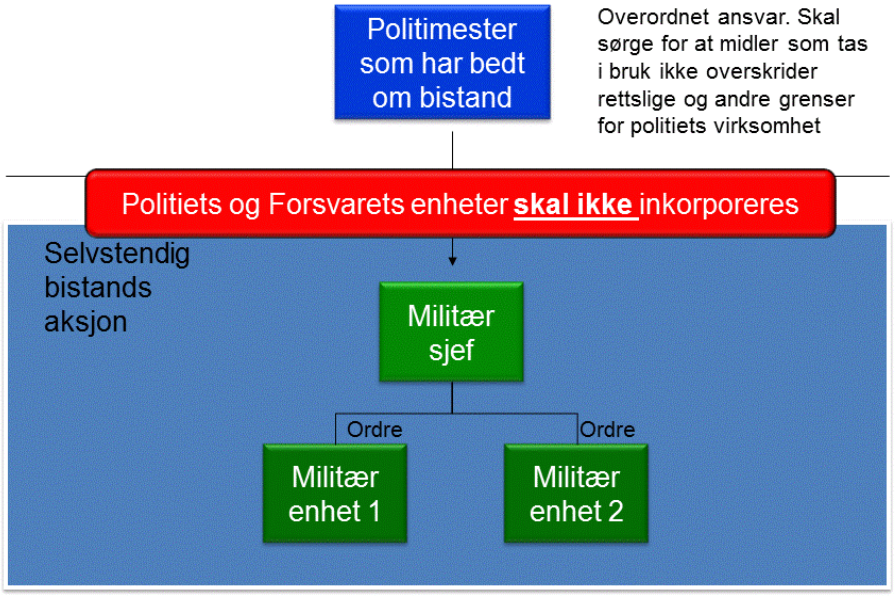
Ved behov for alminnelig bistand kan politimester ta direkte kontakt med FOH, mens anmodning om håndhevelsesbistand skal gå fra politimester, via POD og JD til FD, som vist i figur 5.

[18] Instruksen skulle ha vært ferdigstilt i 2013, men er ikke kommet ut foreløpig (mai 2014).



Figur 5: Anmodningsprosessen ved håndhevelsesbistand (Andersen, 2013, s. 39).

Bistandsanmodningen som sendes til POD skal samtidig sendes i kopi til FOH. FOH vil kunne begynne å kartlegge aktuelle ressurser og iverksette tiltak for å kutte ned på responstiden. Skal håndhevelsesbistand ytes gir FD nødvendige retningslinjer til JD og FOH. I hastesaker kan Forsvaret starte planlegging og forberedelser uten å avvente formell beslutning. Den politimester som anmoder om bistand har ansvar for overordnet ledelse av operasjonen, men Forsvarets bistand gjennomføres som en selvstendig bistandsoperasjon, med en egen militær sjef for den militære bistandsenhet, som illustrert i figur 6 (Bistandsinstruksen, 2012).



Figur 6: Ansvar og ledelse av bistandsoperasjon (Andersen, 2013, s. 41).

Bjerga skriver om grenseoppgangen mellom forsvar og politi i artikkelen *Tettere sivilmilitært samarbeid etter 22.juli*. Han sier det prinsipielt kan være «problematisk å gi de militære en rolle på egen jord i fredstid. Samtidig kan det være risikabelt å heve terskelen for å bruke Forsvaret» (Bjerga, 2012). Han mener terskelen for å be om bistand fra Forsvaret er blitt lavere med den nye bistandsinstruksen og at det er mye som taler for at Forsvaret vil få en større rolle i nasjonal beredskap i fremtiden. Bjerga sier det er vanskelig å se noen grunner til at politiet og Forsvaret ikke skal utfylle hverandre på beredskapsområdet og begrunner dette med at politiets ordinære oppgaver er potensielt ubegrensede og ressursene sjeldent tilstrekkelige, mens Forsvaret besitter et overskudd av ressurser som er relevant i nasjonal beredskap og krisehåndtering, også i fredstid.

3.3 Oppsummering

En krise omhandler situasjoner som kommer uventet, utvikler seg raskt og uforutsigbart og har potensiale til å true samfunnssikkerheten, samtidig som håndteringen utfordrer eller overskride kapasiteten og/eller kompetansen til den aktøren, myndighet, eller etat som i utgangspunktet har ansvaret. Dagens modell for beredskap og krisehåndtering er tuftet på fire prinsipper: ansvar,

likhet, nærhet og samvirke og Regjeringen sier ansvar og samvirke skal være overordnet og styrende ved større sektorovergripende kriser.

Sivile kriser skal håndteres av sivile myndigheter og JD er fast lederdepartement for nasjonale kriser med mindre noe annet blir bestemt. *Det nye totalforsvarskonseptet* innebærer gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn om både forebygging, beredskapsplanlegging og operative forhold. Forsvaret skal gi bistand til det sivile samfunn når viktige samfunnsinteresser og liv og helse står på spill. Dette dreier seg om bistand både til politiet og til det øvrige sivile samfunn. Forsvaret har et vidt spekter av ressurser som kan stilles til rådighet for det sivile samfunn i krisesituasjoner, men samtidig færre mannskaps- og materiellressurser til å yte bistand nå enn før. Utgangspunktet er at sivile kriser håndteres med sivile ressurser, men terskelen for å be om bistand fra Forsvaret skal ha blitt lavere med den nye bistandsinstruksen, og Forsvaret vil kunne få en større rolle i nasjonal beredskap i fremtiden. Prop. 73 S fastslår at Forsvaret kan bistå sivile myndigheter ved hendelser i cyberdomenet etter de samme prinsipper og regler som for annen militær bistand til samfunnssikkerhet.

Det nasjonale systemet for krisehåndtering og reguleringen av det sivil-militære samarbeidet definerer i stor grad *når* og med *hva* Cyberforsvaret[19] vil kunne bistå. Cyberforsvaret kan bistå sivile myndigheter ved et cyberangrep mot ekom-infrastrukturen dersom viktige samfunnsinteresser, liv og helse står på spill, - og under forutsetning av at politiets personell og materielle ressurser ikke strekker til. Cyberforsvaret vil i så fall kunne bistå med all tilgjengelig kompetanse og ressurser. For å besvare problemstillingen må derfor den videre studien vise hva som skal til for at et cyberangrep får konsekvenser for samfunnssikkerheten. Videre må studien se på hvilke cyberressurser politiet har, og hva som skal til for at deres personell og materiell eventuelt ikke strekker til. Og sist men ikke minst må studien gjøre rede for hvilken kompetanse og ressurser Cyberforsvaret besitter.

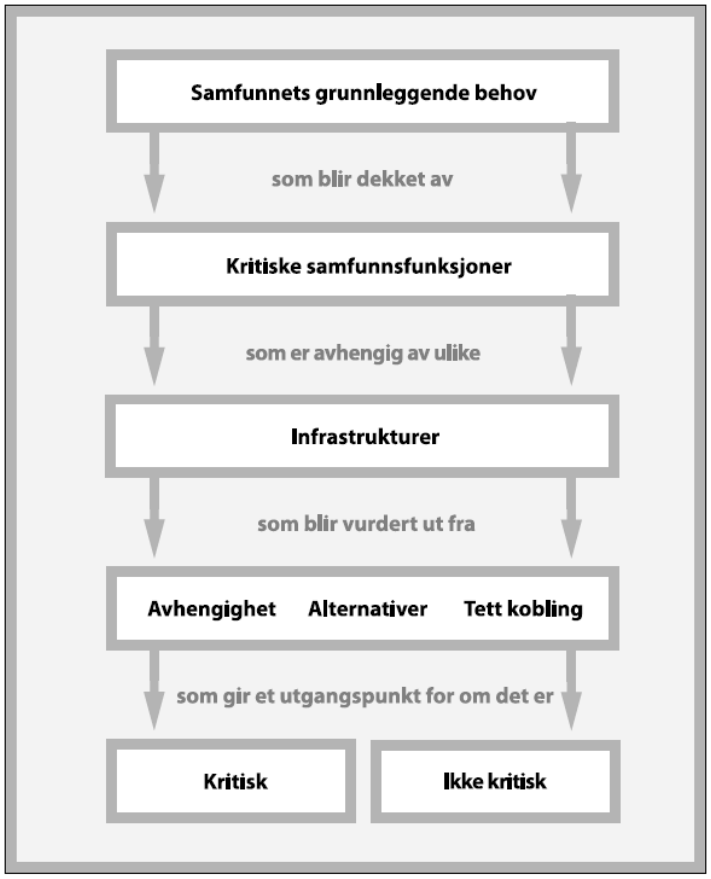
[19] Anmodning om bistand rettes til Forsvaret, beslutningen om å bistå tas enten ved FOH eller på strategisk nivå avhengig av hva slags bistand det er spurt om. Dersom det besluttes at Forsvaret skal bistå og Cyberforsvaret er den mest egnede ressursen i forhold til oppdraget vil disse ressursene kunne avgis.

4 Elektronisk kommunikasjonsinfrastruktur og cyberdomenet

Forsvaret skal gi bistand til det sivile samfunn når viktige samfunnsinteresser, liv og helse står på spill. NSM håndterte nært 4000 sikkerhetshendelser på internett i 2013, sentrale norske virksomheter som myndighetsorganer, forsvarsindustri og teknologibedrifter ble rammet, og 50 av angrepene ble kategorisert som alvorlige (NSM, 2014b). Det var likevel ikke behov for bistand fra Forsvaret i noen av disse hendelsene. Forståelse for at et cyberangrep rettet mot ekom-infrastrukturen kan forårsake en nasjonal krise hvor Forsvaret kan bli bedt om å bistå krever kjennskap til infrastrukturen. Dette kapitlet vil gjøre rede for hva ekom-infrastruktur *er*, og slik begrunne hvorfor cyberangrep mot denne infrastrukturen kan true samfunnssikkerheten og derfor kreve en annen håndtering enn de andre, daglige, sikkerhetshendelsene på internett.

4.1 Hva er kritisk infrastruktur?

Infrastrukturutvalget definerte kritisk infrastruktur til å være ”de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse” (NOU 2006: 6, 2006, s. 16). Utvalget fant tre generiske trekk - kriterier - for utvelgelse av kritisk infrastruktur: avhengighet, alternativer og tett kobling, som vist i figur 7. Det første kriteriet var kritisk *avhengighet* til infrastrukturen for å kunne opprettholde et tjenestetilbud. Bortfall av infrastrukturen vil få alvorlige konsekvenser dersom et stort antall mennesker er avhengige av den. Det andre kriteriet var *alternativer*, - få eller manglende alternativer som kan erstatte infrastrukturen indikerer at infrastrukturen er kritisk. Siste utvelgelseskriterium var *tett kobling*: «Dette kan gjelde mellom ulike komponenter innenfor ett og samme system slik at svikt i én komponent fører til at hele systemet svikter. En annen variant av tett kobling kan skyldes avhengighet mellom systemer slik at svikt i ett system, har negative virkninger for funksjonaliteten i andre systemer og at det dermed får sektorovergripende konsekvenser» (NOU 2006: 6, 2006, s. 21).



Figur 7: Kritisk infrastruktur og kritiske samfunnsfunksjoner (NOU 2006: 6, 2006, s. 33).

Prosesser som tidligere ble kontrollert innenfor lukkede systemer blir i økende grad koblet til internett. Fjernovervåking og fjernstyring av viktige samfunnsinnretninger, slik som navigasjonssystemer, oljeutvinning og vannkraftverk, medfører at alle infrastrukturene gradvis blir tettere koblet og mer avhengig av ekom-nett (NOU 2006: 6, 2006; NSM, 2014b). En alvorlige cyberhendelser i ekom-infrastrukturen vil slik ha potensiale til å indirekte ramme øvrig kritisk infrastruktur.

Infrastrukturutvalget definerte elektronisk kraft, vann og avløp, transport, olje og gass, satellittbasert infrastruktur og ekom som kritiske infrastrukturer.

4.2 Fra Televerkets monopol til et ekom-marked med fri konkurranse

Etter andre verdenskrig var beskyttelse av teletjenester en viktig del av totalforsvarskonseptet. Offentlige telekommunikasjonstjenester ble levert av en offentlig forvaltningsbedrift – Televerket. Til tross for at man hadde egne telenett med høye krav til robusthet innen jernbanen, Forsvaret og kraftforsyningen, var offentlige teletjenester likevel en svært viktig del av datidens totalforsvar (DSB, 2012). På slutten av 1980-tallet startet en gradvis omorganisering av sektoren. I 1988 ble Televerkets monopol på terminalutstyr opphevet, tre år etter ble det innført konkurranse innen mobiltelefoni og i 1995 ble Televerket omdannet til et statlig aksjeselskap, - Telenor. Da det norske telemarkedet ble åpnet for konkurranse 1. januar 1998 økte antall tilbydere innen ekom-tjenester hurtig. 10 år etter var det nært 200 aktører innenfor områdene fasttelefoni, mobiltelefoni, internett og leide linjer (Post- og teletilsynet, 2013). Et telemarked med fri konkurranse krevde et nytt konsept for telesikkerhet og – beredskap. Det nye konseptet ble beskrevet i St.meld. nr. 47 (2000-2001) *Telesikkerhet og -beredskap i et telemarked med fri konkurranse,* og innebar at alle teleoperatører, ikke bare Telenor, skulle pålegges en del beredskapsforpliktelser. PT skulle følge utviklingen og gjennom pålegg og ulike samarbeidstiltak sørge for økt robusthet (St. meld. nr. 17 (2001-2002), 2002, s. 44-45).

Bruksmønsteret har gradvis endret seg de siste 10 år. Innen telefoni har trenden vært nedgang i andelen fasttelefoni abonnement til fordel for mobiltelefonabonnement. Ved utgangen av første halvår 2013 var det 1,32 millioner fasttelefoni abonnement og om lag 5,9 millioner mobiltelefoni abonnement i Norge. Trafikken fra mobiltelefoner utgjorde nesten 75 prosent av den totale trafikken. Samtidig har internettbruken nærmest eksplodert. Ved utgangen av 2002 lå antallet abonnement for fast bredbånd på 200 000, mens man i 2013 nærmet seg 1,9 millioner. Mobilt bredbånd ble introdusert i 2006 og ved utgangen av første halvår 2013 nærmet man seg 812 000 abonnement, noe som tilsvarer om lag 43 prosent av antall abonnement for fast bredbånd (Post- og teletilsynet, 2013). Mobiltelefonen brukes stadig mer og dekker samtidig et større mangfold av behov. Endringer i bruksmønster er en medvirkende årsak til det pågående teknologiskiftet i Telenor. Telenor vil avvikle den linjesvitsjede telefoniplattformen og erstatte det med IP-teknologi og/eller mobile løsninger (DSB, 2013b, s. 5). DSB mener teknologiskiftet vil få betydning for samfunnets robusthet og sårbarhet: «Overgangen til en felles plattform for nesten all elektronisk kommunikasjon i Telenors nett medfører en endring i sårbarhetsbildet for

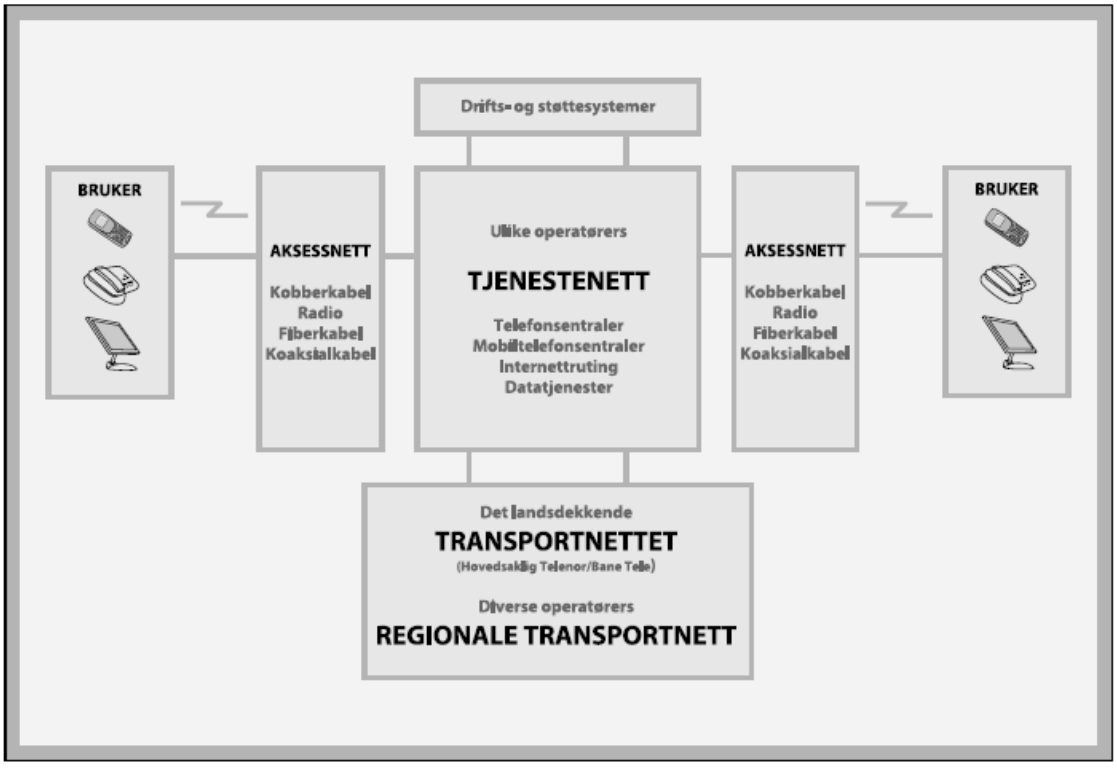
ekomnett og -tjenester. Redundansen vil bli redusert og ekomnettene vil i større grad enn før bli eksponert for cyberangrep av ulike slag» (DSB, 2013b, s. 6).

Telenor er den dominerende leverandør av teletjenester i Norge, både innenfor fasttelefoni, mobiltelefoni og internett (Post- og teletilsynet, 2013):

- Fasttelefoni: Telenor har, målt i omsetning, 68,1 % av markedsandelen.
- Mobiltelefoni Telenor har 49,6 % av markedsandelene.
- Datatrafikk (omfatter både ordinære abonnement for mobiltelefoni og dedikerte abonnement for mobilt bredbånd): Telenor har 43,8 %.
- Fast bredbånd: Telenor har 45,3 % av omsetningen i privatmarkedet og 27,3 % av omsetningen i bedriftsmarkedet.

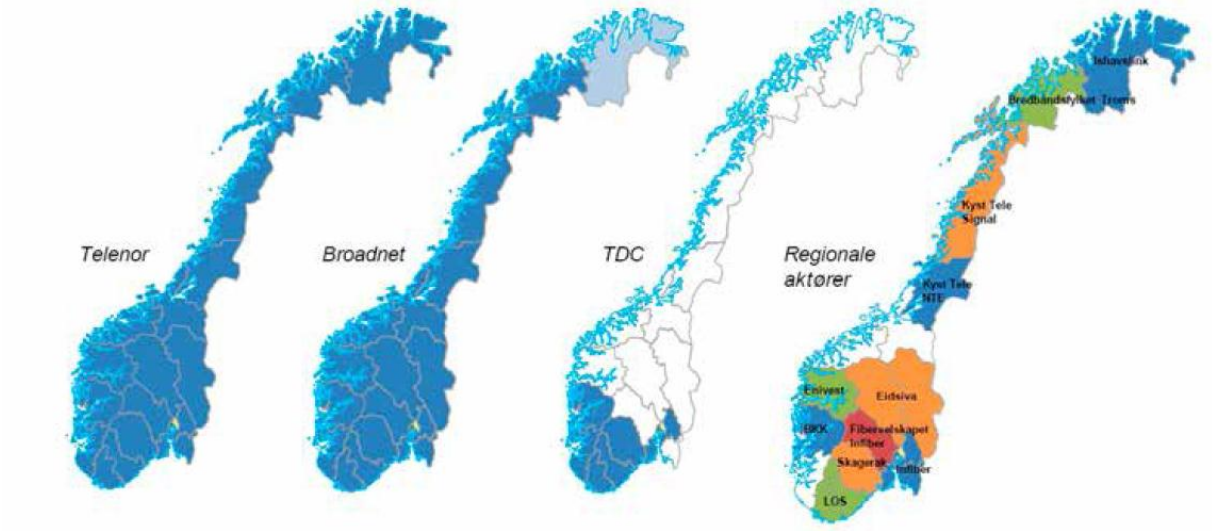
4.3 Elektronisk kommunikasjonsinfrastruktur - Oppbygning og status

Infrastrukturen består av stamnett, aksessnett, tjenestenett samt drift- og støttesystemer, som illustrert i figur 8.



Figur 8: Prinsippskisse ekom-infrastruktur (NOU 2006: 6, 2006, s. 100: Figur 10.1)

Stamnett, også kalt transportnett, er den landsdekkende motorveien for tele- og datakommunikasjon. Transportnettene består av overføringssystemer med stor kapasitet, fiberkabel og i noen tilfeller radiolinje. Det er flere virksomheter som eier fiberinfrastruktur som kan inngå i andre tilbyderes transportnett, men likevel er det få, om noen, aktører som ikke er avhengige av å leie kapasitet av Telenor for å sy sammen egne nett. Telenor og Broadnet[20] er, som illustrert i figur 9, de to eneste som tilbyr nasjonal transportkapasitet basert på fiberoptiske kabler. Telenor har i dag to landsdekkende og fysisk adskilte transportnett (Svendsen, 2014). Jernbaneverket har et digitalt nett som brukes til jernbaneformål, men det tilbys ikke andre. Statnett har også egen infrastruktur men kjøper fortrinnsvis overføringskapasitet fra andre aktører der hvor det er mulig (DSB, 2013b, s. 14).



Figur 9: Dekningsområdet for leverandører av overføringskapasitet (DSB, 2013b, s. 15)

Transportnettene er en del av det PT regner som kritisk infrastruktur (DSB, 2012, s. 15). Venstres stortingsrepresentanter, Breivik og Kjenseth, la nylig frem et krav om å etablere en nasjonal plan for utbygging av bredbåndsinfrastruktur. De mener dagens situasjon ikke er holdbar sett i fra et sårbarhets- og sikkerhetsperspektiv fordi: «Alle samfunnskritiske ekomtjenester, mobil- og nødnettstjenester hviler til syvende og sist på Telenors stamnett» (Breivik & Kjenseth, 2014).

[20] Ventelos virksomhet innen bredbånd og datakommunikasjon ble en del av Broadnet 1.7.2012. På sine nettsider skriver de at de har et landsdekkende fibernett, bestående av 32 000 km med fiber som knytter sammen over 90 norske byer fra nord til sør (Broadnet, 2014).

I tillegg til de sivile transportnettene har Forsvaret, siden midt på 1950-tallet driftet et eget landsdekkende ikke-kommersielt telenett. Nettet ble opprinnelig etablert for å gi samband til steder der det sivile telenettet ikke hadde tilstrekkelig dekning, samt sørge for sikring av informasjon og robusthet på sambandssiden. Forsvarets kommunikasjonsinfrastruktur (FKI) dekker i dag alle Forsvarets installasjoner over hele landet samt enkelte deler av offentlig forvaltning. FKI består av et stasjonært nett samt mobile og deployerbare enheter. (DSB, 2012, s. 15; Prop. 1 S (2007-2008), 2007, s. 125; Stenseth, 2003).

Transportnettet knytter sammen regionalnettene. Regionalnettene er riksveiene for tele- og datakommunikasjon. I regionalnettene står det flere sentraler som samler opp trafikk fra aksessnettene. Under brannen i Lærdal var det en slik sentral i regionalnettet som brant ned (Svendsen, 2014). *Aksessnett* knytter forbindelse mellom den enkelte sluttbruker og transport- og tjenestenettene. De faste aksessnettene kan være fiber, hybridfiber eller kobber, og sender trafikk mellom sluttbruker og nærmeste sentral i regionalnettet. Mobilnettene er en type aksessnett hvor det er trådløs forbindelse mellom basestasjoner og brukernes mobiltelefoner. Den enkelte basestasjon dekker et lite geografisk område, og hver basestasjon er knyttet til kjernenettet med en fast linje, eller en radiolinje. For at en tilbyder av mobilnett skal kunne dekke hele landet kreves det et aksessnett med flere tusen basestasjoner. Telenor hadde omkring 10.000 basestasjoner, plassert på 6.500 lokasjoner i 2012 (Post- og teletilsynet, 2012a, s. 8). Andre mobiltilbyderne er avhengig av Telenor sin infrastruktur for å levere sine tjenester (DSB, 2012, s. 15). Innfasing av fjerde generasjon mobiltelefoni (4G) medfører at IP-teknologi også blir tatt i bruk på dette området[21].

Tjenestenett er ikke et selvstendig fysisk overføringsnett, men kan benytte ulike typer infrastruktur som også anvendes til andre typer tjenester. Fasttelefon og mobiltelefon er eksempler på tjenestenett. Tjenestenettene består av diverse systemer og utstyr som er nødvendig for å levere de ulike tjenestene. *Drifts- og støttesystemene* er IT-systemer som overvåker og styrer ekom-nett og tjenestenett. DSB sier drift- og støttesystemene kan utgjøre en kritisk del av infrastrukturen (DSB, 2012, s. 15-16). Funksjonene er gjerne sentralisert og er derfor selv avhengige av ekom for å overvåke og styre komponentene i nettene.

[21] 2G og 3G vil ikke fases ut, men fortsatt eksistere ved siden av 4G (DSB, 2013b, s. 23)

4.4 Cyberdomenet

Ekom-tjenestene har blitt mer avansert, mer tilgjengelig og mer integrert i folks dagligliv. Økt bruk av internett er en generell trend i hele vesten. Omtrent 40 prosent av verdens befolkning er på internett (S. T. Johnsen & Kveberg, 2014). Det er internett mange tenker på når de hører begrepet cyberdomenet. Etter FD sin definisjon består cyberdomenet av fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data (Forsvarsdepartementet, 2014, s. 4). Cyberdomenet omfatter altså både de nett som er tilgjengelig fra internett (åpne nett) og de som ikke er det (lukkede nett), både infrastrukturen og dataene som er lagret der. Cyberbegrepene er abstrakte, relativt nye, og de brukes forskjellig. For å kunne drøfte Cyberforsvarets rolle ved et *cyberangrep* er det derfor nødvendig å ta en begrepsgjennomgang.

Cyberangrep

Cyber er et prefiks som indikerer at en aktivitet foregår i cyberdomenet (Forsvarsdepartementet, 2014). Aktiviteten i seg selv har gjerne en definisjon fra før av. En *cyberkrise* er dermed definert til å være en *krise* som har oppstått i eller gjennom cyberdomenet. Imidlertid er det ikke slik at alle aktiviteter har en klar definisjon fra før. *Angrep* er en slik aktivitet[22]. *Manual i krigens folkerett* beskriver den folkerettslige betydningen av begrepet *cyberangrep*: «Med cyberangrep menes en cyberoperasjon som er forventet å forårsake død eller skade på personell eller skade eller ødeleggelse på objekter»[23] (Forsvaret, 2013, s. 190). I media og blant folk flest brukes begrepet cyberangrep, data-angrep og IKT-angrep om hverandre og om hendelser av forskjellig alvorlighetsgrad (Utheim, 2013). I Cyberforsvaret har man, i tråd med krigens folkerett, vært restriktiv med bruk av begrepet. Generalmajor Sundseth, daværende sjef for Cyberforsvaret, begrunnet det slik i Oslo Militære samfund i februar 2013: «For oss fagmilitære er det slik at begrepet *angrep* veier tungt. Det å bli angrepet er ikke noe som vi tar lett på, og det er en handling som hos oss møtes med klar respons. Det er, med andre ord, et tyngre vektet begrep i den fagmilitære verden enn det er i resten av samfunnet» (Sundseth, 2013). FD har i ettertid definert cyberangrep som: «Handlinger i eller gjennom cyberdomenet med hensikt å skade eller

[22] Krise er også et begrep uten en klar definisjon men dette begrepet ble omtalt i 3.1.1
[23] Den generelle definisjonen av angrep gis i punkt 2.2 i manualen.

påvirke personell, materiell eller konfidensialiteten[24], integriteten[25], tilgjengeligheten[26] eller autentisiteten[27] til et informasjonssystem» (Forsvarsdepartementet, 2014, s. 5). Et angrep innbefatter en villet handling fra en aktør som har til hensikt å påvirke informasjonssystemet eller informasjonen som ligger lagret der, effekten av angrepet kan ramme selve informasjonssystemet eller infrastruktur som styres av informasjonssystemet (Forsvarsdepartementet, 2014, s. 5). FD sin definisjon av angrep omfatter målrettede angrep med ulike formål, herunder både spionasje og sabotasje. Angrep er ikke avgrenset til de hendelser som går utover overlevelsesevnen men omfatter også de som påfører ulempe, eller påvirker livskvaliteten. Denne oppgaven baseres på FD sine definisjoner.

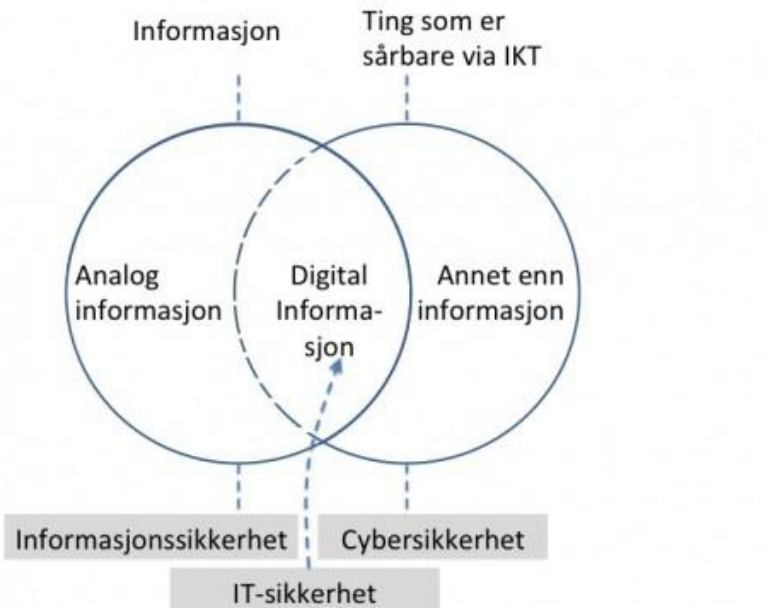
FD bruker begrepet cyberhendelse både om situasjoner der IKT-systemer blir utsatt for cyberangrep, og ved utilsiktet svikt og har definert alvorlige cyberhendelser til å være: «cyberhendelser som rammer samfunnskritisk infrastruktur, samfunnskritisk informasjon eller samfunnskritiske funksjoner på en slik måte at det får betydning for samfunnets og befolkningens trygghet» (Forsvarsdepartementet, 2014, s. 5).

Informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet

Regjeringen sier de vil koble Cyberforsvaret inn i sivil cybersikkerhet, men hva innebærer cybersikkerhet? Informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet er begreper som brukes om hverandre, og folk legger tilsynelatende litt forskjellig i begrepene. En som har forsøkt å skape klarhet i begrepsbruken er Morten Irgens, viserektor for forskning ved Høgskolen i Gjøvik og dekan ved høgskolens avdeling for informatikk og medieteknikk. Han sier at *informasjonssikkerhet* har med sikring av informasjon å gjøre, uavhengig av om den er lagret digitalt eller ikke. *IT-sikkerhet* derimot har med sikring av selve informasjons- og kommunikasjonsteknologien (IKT), altså maskinvare og programvare. *Cybersikkerhet* dreier seg derimot om sikring av alt som er sårbart via IKT. Irgens har laget en modell (figur 10) som

[24] Sikkerhet for at nærmere angitt informasjon ikke avsløres for uvedkommende, og at kun autoriserte personer får tilgang til denne (Forsvarsdepartementet, 2014, s. 23).
[25] Sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter (Forsvarsdepartementet, 2014, s. 23).
[26] Sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov (Forsvarsdepartementet, 2014, s. 23).
[27] «Ekthet» (Forsvarsdepartementet, 2014, s. 21)

illustrerer forskjellen på begrepene:



Figur 10: Sammenhengen mellom informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet. (Irgens, 2013)

Analog informasjon omfatter all informasjon, herunder bøker og håndskrevne notater, men også den informasjonen som gis muntlig. *Annet enn informasjon* dekker mengden av ting som er sårbare via IKT. Et eksempel er urananrikningssentrifugene i iranske Natanz, som ble rammet av dataormen *Stuxnet*. Stuxnet skal angivelig ha manipulert spin-syklusene til sentrifugene slik at de ristet seg selv i stykker. Irgens argumenterer for at også naturen, dyr og mennesker kommer inn under denne kategorien, han eksemplifiserer med at dersom noen sender råseptik ut i drikkevannet i Oslo via kontrollsystemet på renseanlegget oppe ved Maridalsvannet, - vil det naturlig nok få konsekvenser for natur, dyr og mennesker. Irgens sin forståelse av begrepet stemmer tilsynelatende godt med Langø og Sandvik sin beskrivelse i artikkelen *Cyberspace og sikkerhet*: «Når vi snakker om cybersikkerhet, snakker vi i første rekke om trusler mot individer, organisasjoner eller samfunn gjennom og i dette cyberspace-Miljøet» (Løngø & Sandvik, 2013, s. 222).

Det eksisterer ingen nasjonal strategi for cybersikkerhet men Regjeringen har gitt ut en nasjonal strategi for informasjonssikkerhet. Strategien er sektorovergripende og omhandler også Forsvarets ansvar innen informasjonssikkerhet. FD ga ut sine cyberretningslinjer, for

forsvarssektoren, 1.mars 2014, retningslinjene er innrettet mot håndtering av digital informasjon og informasjonssystemer (Forsvarsdepartementet, 2014). Disse dokumentene til sammen kan forventes å gi en indikasjon på hvilke aktører som har ansvar og roller dersom sivil kritisk infrastruktur utsettes for et cyberangrep.

4.5 Nytt domene - nye utfordringer?

Det er sivile myndigheter, med politiet i spissen, som skal sørge for den indre sikkerheten i Norge, mens Forsvaret skal ivareta rikets sikkerhet i forhold til eksterne trusler (kapittel 3.2). Kristin Bergtora Sandvik, seniorforsker ved PRIO, sier at cyberangrep kan befinne seg i en *gråsone* mellom Forsvar og politi, fordi angriperen kan inneha flere roller: være en såkalt *patriotisk hacker* og samtidig jobbe på direkte oppdrag fra en statsmakt. Om cyberangrepet skal defineres å være økonomisk eller militært motivert, mener hun vil avhenge av «hvor omfattende og sofistikert angrepet er, men også av geopolitiske betraktninger, av de strategiske ressursene til landet som blir angrepet, og av hvem aggressoren antas å være» (Sandvik, 2013, s. 252). Høyrepolitiker Anders Werp mener det vil være så vanskelig å fastslå om et cyberangrep er en kriminell handling eller krigshandling at det kan bli full forvirring om hvem som har ansvaret dersom nasjonen vår rammes av et alvorlig cyberangrep. Han hevder «det er komplett umulig å skille mellom det militære og sivile ansvaret» (Gabrielsen, 2013).

Det er kriminelle aktører som står bak størsteparten av den illegale aktiviteten på nettet, men E-tjenesten sier det er statlige aktører som utgjør den største trusselen mot norske interesser. «Statlige aktører utvikler svært avanserte digitale etterretningskapasiteter og skadevare som kan benyttes i det digitale rom. Målene for disse operasjonene er i hovedsak norsk sivil og militær kunnskap og teknologi. Politiske beslutninger og beslutningsprosesser, forsvar, infrastruktur og industri er også høyt prioriterte mål for utenlandske etterretningstjenester» (Etterretningstjenesten, 2014, s. 59) Det er bare nasjonalstatene som antas å ha tilstrekkelig kapasitet til å utrette betydelig skade, ressurser til å kunne planlegge store angrep, gjennomføre dem og analysere dem etterpå (Etterretningstjenesten, 2014; Hillestad & Sandli, 2013).

FD sier at digitale angrep er særegne på den måten at «de som hovedregel forårsaker relativt beskjedne eller ingen direkte fysiske skader, samtidig som den umiddelbare konsekvensen og de avledede/indirekte skadene kan være betydelig (Forsvarsdepartementet, 2012, s. 1,2). Et

cyberangrep vil i første rekke kunne ramme samfunnssikkerheten ved at kritiske funksjoner settes ut av spill, men Forsvaret sier at det også kan true statssikkerheten, - avhengig av omfang og mål (Prop. 73 S (2011-2012), s. 24). Imidlertid vil det kunne være vanskelig å fastslå angrepets mål. Et og samme system kan brukes til både militære og sivile formål og systemer kan, som vist i kapittel 4.1, være knyttet sammen på en måte som gjøre at angrep på den ene får konsekvenser i den andre. Et angrep vil kunne få følgeskader som ikke var tiltenkt. På den annen side vil de tette koblingene også kunne utnyttes. «Erfaring fra moderne krigs- og konfliktsituasjoner viser at cyberoperasjoner rettet mot sivil IKT-infrastruktur må kunne forventes å være en del av et militært anslag fra en statspart» (Innst. 388 S (2011-2012), 2012, s. 80). En fiende vil kunne angripe Telenors datasystemer for å ramme offentlige myndigheter (NUPI, 2011).

JD er som vist i kapittel 3.1.3 gitt i ansvar å være fast lederdepartement for sivile nasjonale kriser inntil noe annet blir bestemt. Det kan være vanskelig å fastslå hvem som står bak et cyberangrep og hva som var angrepets mål. Angrepene kan ligge i en gråsone mellom kriminell virksomhet og krigshandlinger, mellom politi og Forsvar, men hovedregelen er at cyberangrep mot sivil infrastruktur ledes av sivile myndigheter inntil Regjeringen beslutter noe annet.

Et lovverk som ikke dekker utfordringene?

Sandvik hevder, i artikkelen *Cyberkrig og internasjonal rett,* at cyberkriminalitet, cyberterrorisme og cyberkrig stiller nasjonale myndigheter og det internasjonale samfunnet overfor store lovtekniske utfordringer. Alvorlige cyberangrep kan representere forbudt maktbruk, men Sandvik påpeker at det er omdiskutert hvor denne grensen går. Hun sier en tilnærming er å se på brukt instrument og vurdere hvorvidt konsekvensene tilsvarer kinetisk maktbruk, en annen tilnærming har vært å betrakte alle angrep på kritisk infrastruktur som væpnet angrep og den tredje tilnærmingen er å se på de samlede konsekvensene for staten (Sandvik, 2013, s. 258). Hun beskriver vilkårene for å kunne tilskrive en stat ansvaret for angrep utført av en tredjepart fra statens territorium som omdiskutert, og sier videre det er usikkert om det eksisterende rammeverket er i stand til å skille mellom ulike aktiviteter som cyberspionasje og nettverksangrep og de som krysser terskelen for å utgjøre *væpnede angrep*.

FD mener det avgjørende kriteriet for at en stat kan gjøres ansvarlig for et cyberangrep utført av ikke-statlige aktører er at: «staten har effektiv kontroll over eller direkte instruerer, den gjeldende grenseoverskridende rettstridige cyberoperasjonen begått av den ikke-statlige aktøren» (Forsvarsdepartementet, 2012, s. 3). FN-paktens artikkel 2(4) innebærer et klart definert forbud mot statlig maktbruk mot andre stater og FD sier det er naturlig å se på hvilket skadepotensiale virkemidlet har ikke bare hvilket virkemiddel som brukes. Cyberangrep vil bare unntaksvis være tilstrekkelig alvorlige til å utløse reglene om maktbruk og selvforsvar etter folkeretten, oftest vil det dreie seg om forstyrrelser der det vil være aktuelt å iverksette mottiltak. «Mottiltak defineres som ellers ulovlige handlinger som gjøres lovlige på grunn av en forutgående ulovlig handling – i denne sammenheng et ulovlig dataangrep» (Forsvarsdepartementet, 2012, s. 3) Som mottiltak nevner FD diplomatiske reaksjoner og import- og eksportforbud som eksempler.

Espen Barth Eide ble i sin tid som forsvarsminister spurt om hvor massivt et cyberangrep må bli for at Norge skal ringe NATO sa han at *denne grensen* ikke var avklart, men at Norges holdning er at dataangrepet må gå over i den fysiske verden. At konsekvensene av cyberangrepet påvirker liv og helse, eller skaper store ødeleggelser i det fysiske rom (Hamnes, 2012). I siste langtidsplan for Forsvaret presiseres det at et cyberangrep vil vurderes på bakgrunn av «formål og legitimitet, samt angrepets styrke og konsekvenser» (Prop. 73 S (2011-2012), s. 24).

I *Manual i krigens folkerett* påpekes det at det er internasjonal enighet om at krigens folkerett skal gjelde også for cyberoperasjoner. «Cyberangrep er underlagt de samme begrensninger og reguleringer som andre typer angrep[28]» (Forsvaret, 2013, s. 190). Men det erkjennes samtidig at den konkrete anvendelsen likevel kan by på utfordringer.

Trusler som rammer uten forvarsel og eskalerer kjapt

En cybertrussel kan oppstå helt uten forvarsel, sa Forsvarsminister Ine Eriksen Søreide under årets sikkerhetskonferanse, og kalte det en fundamental erkjennelse. Hun påpekte at dette utfordrer beredskapssystemet vårt, som er tuftet på at vi har tid til å sette inn mottiltak. En hendelse kan eskalere fra lokalt nivå til nasjonalt og videre til internasjonalt på sekunder. Søreide fremhevet viktigheten av at alle samarbeider godt og erkjente samtidig at samarbeid på tvers av

[28] Det er bare når en operasjon mot sivile personer eller sivile objekter, eller andre beskyttede personer eller objekter, kvalifiserer til å være et angrep, at den vil være forbudt etter krigens folkerett(Forsvaret, 2013)

sektorene er ikke godt nok i dag (Søreide, 2014). Det at et angrep kan ramme uten forvarsel er likevel ikke helt unikt for cyberdomenet. Det var ingen som hadde forutsett angrepene den 22/7, og det er ikke tvil om at bomben rammet regjeringskvartalet både kjapt og brutalt. Imidlertid innebar allikevel angrepet en fysisk forberedelse og det andre angrepet den 22.juli en fysisk forflytning som kanskje kunne ha vært oppdaget og stoppet. Roger Johnsen påpeker i artikkelen *Cyberkrigføring og Forsvarets operative evne* at det ikke er enkelt å observere styrkeoppbygging i cyberdomenet. Eskalering av konflikten krever ikke fremføring av militære styrker og angripers fysiske posisjon er lite relevant (R. Johnsen, 2013, s. 245).

4.6 Oppsummering

Elektroniske kommunikasjonsnett er en forutsetning for å kunne opprettholde samfunnskritiske tjenester og det finnes få eller ingen alternativer som kan erstatte infrastrukturen. Tette koblinger mellom ekom-infrastrukturen og andre systemer gjør at svikt i én komponent kan gi negative konsekvenser for funksjonaliteten i andre systemer og slik gi sektorovergripende konsekvenser. Det er nærmere 200 leverandører av ekom-nett og ekom-tjenester i Norge, men Telenor er den dominerende leverandøren. De fleste samfunnskritiske ekom-tjenester, mobil- og nødnetts tjenester avhenger av Telenors stamnett. Denne infrastrukturen, og de tilhørende drifts- og støttesystemene, regnes derfor som samfunnskritisk.

Forsvaret har et eget landsdekkende ikke-kommersielt transportnett, - Forsvarets kommunikasjonsinfrastruktur.

Et cyberangrep kan ramme helt uten forvarsel og eskalere fra lokalt nivå til nasjonalt og videre til internasjonalt på sekunder. En alvorlig cyberhendelse vil i første rekke ramme samfunnssikkerheten, men angripers identitet og motiver kan være uklare og angrepet kan slik befinne seg i en gråsone mellom kriminelle handlinger og krigshandlinger. Hovedregelen er likevel at cyberangrep mot sivil infrastruktur ledes av sivile myndigheter inntil Regjeringen beslutter noe annet. Det er ingen klart definert grense for hva som skal regnes som *væpnet angrep*, men Norges holdning er at det må påvirke liv og helse, eller skaper store ødeleggelser i det fysiske rom for å passere denne grensen.

5 Aktører, ansvar og oppgaver i det nasjonale cyberdomenet

PST har i lengre tid vært bekymret for at myndighetene ikke har god nok kontroll over det norske ekom-nettet. De tok opp sin bekymring knyttet til spionasje og manipulering av telenettet med Regjeringen i 2009 og senest i et intervju med TV2 i februar i år. Når TV2 konfronterte Justisministeren med dette hevdet han at sikkerheten i ekom-nettet hører inn under samferdselsministerens ansvar. Samferdselsministeren på sin side påpekte at han ikke har ansvar for «spionasje og sånne ting», og pekte på justisminister og forsvarsminister. Det er viktig vi fordeler ansvaret der det er riktig at det ligger sa samferdselsminister Kjetil Solvik-Olsen (Østby, 2014). Hvem har egentlig ansvaret?

For å kunne drøfte Cyberforsvarets rolle i en alvorlig cyberhendelse i ekom-infrastrukturen er det en forutsetning å ha kjennskap til de ulike aktørene, deres ansvar og oppgaver. De sivile aktørenes antatte kapasitet indikerer om de vil kunne få behov for bistand eller ei. Mens Cyberforsvarets oppdrag og kapasiteter vil gi en god indikasjon på hva de vil kunne bistå med, og kanskje like viktig – hva de ikke vil bistå med. Ved hjelp av en innholdsanalyse skal dette kapitlet kartlegge og diskutere hvilke aktører som er gitt ansvar, oppgaver og myndighet knyttet til ekom-infrastruktur og håndtering av en eventuell cyberhendelse, samt belyse aktørenes antatte kapasitet.

5.1 Nasjonal strategi for informasjonssikkerhet

Regjeringen ga i 2012 ut *Nasjonal strategi for informasjonssikkerhet*. Strategien skal operasjonaliseres gjennom sju strategiske prioriteringer. Av disse sju er det spesielt tre som er relevante, i forhold til denne oppgavens problemstilling, fordi de omhandler ekom-infrastruktur og håndtering av cyberhendelser (Regjeringen, 2012a):

- Styrke IKT-infrastrukturen
- Sikre samfunnets evne til å oppdage, varsle og håndtere alvorlige IKT-hendelser
- Sikre samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet

De fire andre går mer på forebyggende arbeid, bevisstgjøring og kompetanseheving.

I tillegg til strategidokumentet ble det gitt ut en handlingsplan, som mer detaljert beskriver hvordan strategien skal følges opp (Regjeringen, 2012b). Dokumentene angir hvilket ansvar og oppgaver som påligger virksomhet, myndighet og fagdepartement. Alle fagdepartement har ansvar for forebyggende tiltak, beredskapstiltak og krisehåndtering i egen sektor og tilsyn med underlagte etater. Ved siden av dette ansvaret som påligger hvert fagdepartement, er JD, SD og FD tildelt særskilte roller knyttet til IKT-sikkerhet i samfunnet. Kort fortalt skal JD være en pådriver og koordinator overfor andre sektormyndigheter og har ansvaret for IKT-sikkerheten i sivil sektor. SD på sin side har ansvar for IKT-sikkerheten knyttet til elektroniske kommunikasjonsnett og – tjenester, mens FD sitt ansvar er knyttet til IKT-sikkerhet i militær sektor og etatsstyring av NSM (Regjeringen, 2012a, s. 15-16).

5.2 NSM

NSM og Forsvarssjefens sikkerhetsavdeling (FSA) ble opprettet 1. januar 2003 samtidig som Forsvarets overkommando/Sikkerhetsstaben (FO/S) ble lagt ned. FSA ble opprettet til støtte for Forsvarssjefen, mens NSM ble opprettet som et direktorat under FD for å ivareta overordnede og tverrsektorielle sikkerhetsoppgaver i henhold til sikkerhetsloven (St.prp. nr 1 (2002-2003), s. 30). NSM ivaretar de utøvende funksjoner i sikkerhetsloven på vegne av departementet, fører tilsyn med sikkerhetstilstanden i virksomheter underlagt loven og kan ved behov gi pålegg om forbedringer (Sikkerhetsloven, 1998). Fagmiljøet i NSM er samtidig viktig for å understøtte JD sitt ansvar for IKT-sikkerhet[29] og NSM rapporterer direkte til JD for oppgavene i sivil sektor. VDI ble opprettet høsten 2000 som en prøveordning og ble fra 2003 etablert fast under NSM.

NSM er det sentrale direktorat for informasjons- og objektsikkerhet. I årsrapporten fra NSM innleder direktør Kjetil Nilsen med å si at nasjonen ikke er godt nok sikret når det gjeler internett og datasystemer. NSM har utvidet med 60 nye personer og har nå passert 200 ansatte, - disse skal hjelpe norske virksomheter til å styrke sin egen sikkerhet i fremtiden. Å sikre samfunnets evne til å oppdage, varsle og håndtere alvorlige IKT-hendelser er et prioritert område i *Nasjonal strategi for informasjonssikkerhet*. Målsetningen er at: «Norge skal ha en døgnkontinuerlig, proaktiv operativ beredskap for å kunne forebygge, oppdage og koordinere håndteringen av alvorlige IKT-hendelser» (Regjeringen, 2012a, s. 21). Begrepet alvorlige IKT-hendelser er i strategien definert til å være målrettede angrep mot kritisk IKT-infrastruktur, samt sensitiv,

[29] Justis- og beredskapsdepartementet har overtatt IKT-sikkerhetsansvaret og videreutvikler dette, bl.a. gjennom etablering av eget fagmiljø i Nasjonal sikkerhetsmyndighet (NSM) (Prop. 1 S (2013-2014), s. 128)

taushetsbelagt og gradert informasjon. Det påpekes at både myndigheter og infrastruktureiere skal inngå i samarbeidet, men NorCERT sin rolle som nasjonal CERT fremheves. NorCERT er operasjonssenteret i NSM. NorCERT skal ved hjelp av VDI og nasjonalt samarbeid, ha «evne til å forebygge, oppdage og analysere data knyttet til alvorlige hendelser på internett» (Regjeringen, 2012a, s. 21). NorCERT er i tillegg gitt i ansvar å koordinere håndteringen av slike hendelser, men hva Regjeringen legger i å *koordinere håndteringen* står ikke beskrevet.

NorCERT sier de kontinuerlig er i dialog med norske nett- og tjenesteleverandører (ISPer), for å distribuere informasjon og avverge dataangrep. Etter NorCERT egne uttalelser å dømme er det imidlertid slik at en tredjedel av leverandørene nærmest ignorerer disse henvendelsene, - noe leverandørene står fritt til å gjøre fordi NorCERT ikke har noen myndighet over dem (Sveinbjørnsson, 2012). NSM sin myndighet er begrenset til håndhevelse av sikkerhetsloven.

I årsrapporten fra NSM fremkommer det at NorCERT behandlet 3901 saker manuelt i fjor, ved varsling, dialog og analyse (NSM, 2014a, s. 4). 50 av disse ble kategorisert som alvorlige. NSM sier flere av angriperne kan ha vært inne i datasystemene over flere år, det gir grunn til å stille spørsmål ved vår evne til å oppdage innbrudd. NSM fremstiller sensornettverket, VDI, som den *digitale innbrudds alarmen for AS Norge*, men det kan altså tyde på at AS Norge ikke har alarm på alle dører og vinduer (NSM, 2014b, s. 33).

NSM sier arbeidet med objektsikkerhet har blitt intensivert de siste årene og at det i 2013 ble pekt ut flere hundre *skjermingsverdige objekter*: «eiendom som må beskyttes mot spionasje, sabotasje eller terrorhandlinger av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser» (Sikkerhetsloven, 1998: §3). *Forskrift om objektsikkerhet*[30] gjelder for alle statlige og kommunale forvaltningsorganer samt de virksomheter som er omfattet av sikkerhetsloven (Forsvarsdepartementet, 2009). Forskriften skal sikre at objekter blir identifisert og beskyttet i henhold til en felles standard. Objekteier har ansvar for defensive og forebyggende sikring, mens politiet på sin side skal ivareta de offensive tiltakene og kan om nødvendig bruke makt for å hindre eller begrense anslag mot objekter[31]. Mange av de

[30] Forskrift om objektsikkerhet trådte i kraft 1.1.2011. Departementene skulle ha pekt ut objekter i egen sektor innen 2012 og beskyttelsestiltak skulle vært implementert innen 2013.
[31] «Forsvaret har, dersom riket er i krig, krig truer, eller rikets selvstendighet eller sikkerhet står i fare, et selvstendig ansvar for objektsikring av objekter som har avgjørende betydning for forsvarsevnen og det militære forsvaret og som er lovlige mål i krise og krig, såkalte nøkkelpunkter» (Regjeringen, 2012b, s. 15).

skjermingsverdige objektene vil være avhengig av IKT-infrastruktur for å fungere og deler av denne infrastrukturen kan derfor i seg selv være skjermingsverdig (Forsvarsdepartementet, 2009). I forskriften står det at skjermingsverdige objekter som er tilknyttet internett og hvor denne tilknytningen utgjør en sårbarhet *kan søke om* tilknytning til VDI. Det stilles altså ikke krav til at objekter som defineres å være skjermingsverdig skal tilknyttes det sentrale system for varsling, men NSM påpeker at fysisk og logisk sikring må ses i sammenheng. Det hjelper lite med en kraftig lås dersom angriper kan bryte seg inn på adgangskontroll systemet via nettverket og gi seg selv tilgang (NSM, 2014b).

Ved siden av nevnte oppgaver leder NSM Cyberkoordineringsgruppen (CKG). Gruppen består av NSM, E-tjenesten og PST. Gruppens formål er å fremskaffe tidsriktig informasjon om trusler i cyberdomenet som et beslutningsgrunnlag til den operative og strategiske ledelsen. Gruppen vedlikeholder og gir ut et helhetlig cyberrisikobilde (Forsvarsdepartementet, 2014).

5.3 Justis- og beredskapssektoren

JD fikk 1. april 2013 samordningsansvaret for forebyggende IKT-sikkerhet i samfunnet. DSB, PST og POD er direkte underlagt departementet. DSB skal være en pådriver i arbeidet med å forebygge kriser og skal sørge for en god beredskap og krisehåndtering (Politiet, 2011, s. 57). Men vurdert ut i fra de dokumenter som inngår i denne studien ser det ikke ut til at DSB er gitt noe ansvar eller oppgaver i forbindelse med håndtering av pågående hendelser. Hovedoppgaven til PST er også av forebyggende art, men tjenesten utfører i tillegg etterforskningsoppgaver (Politiet, 2011, s. 49). Det er POD som utgjør det operasjonelle nivået i etaten, og har overordnet myndighet over politidistriktene og særorganene. Direktoratet skal sørge for at personell og materiell er disponible for berørte politimestre og sjefer for særorgan. POD kan gi operasjonsordrer til taktisk nivå i hendelser, men det er politimestrene og sjefene for særorganene som har ansvaret for å utføre politiets oppgaver. Politimesteren sitter med ansvar for og kommandoen ved håndtering av alle hendelser i sitt distrikt (Politiet, 2011).

I *Nasjonal strategi for informasjonssikkerhet* fastslås det at politiet «skal ha tilstrekkelig kompetanse og kapasitet til å avdekke, identifisere og håndtere datakriminalitet» (Regjeringen, 2012a, s. 23). Begrepet datakriminalitet defineres i strategien til å være «kriminalitet rettet mot datasystemer og datanettverk, og kriminalitet hvor sentrale elementer av handlingsforløpet begås ved hjelp av datautstyr eller datanettverk» (Regjeringen, 2012a, s. 22). Datakriminalitet er et

bredere begrep, dekker et større omfang, enn *alvorlige IKT-hendelser* og *alvorlige hendelser på internett*, som NorCERT er gitt i ansvar å koordinere håndteringen av. Ut i fra *Nasjonal strategi for informasjonssikkerhet* har politiet fått i oppgave å håndtere cyberangrep mot kritisk ekom-infrastruktur. Det samsvarer også godt med politiloven. I § 2 i *Lov om politiet* (politiloven) står det at politiet skal beskytte samfunnet og verne om lovlig virksomhet, opprettholde orden og sikkerhet og verne mot alt som truer den alminnelige tryggheten i samfunnet. En arbeidsgruppe nedsatt av POD (heretter omtalt som arbeidsgruppen), kartla politiets arbeid med IKT-kriminalitet, elektroniske spor og politioppgaver på nett for et par år tilbake. Arbeidsgruppen refererte til paragraf § 2 i politiloven og fastslo at: «Dette må også gjelde for Internett» (Storruste & Magnussen, 2012, s. 23). Arbeidsgruppens rapport, *Politiet i det digitale samfunnet*, indikerer imidlertid at politiet ikke har tilstrekkelig kompetanse og kapasitet til å håndtere datakriminalitet i dag. Politidistriktene arbeider i liten grad med denne typen kriminalitet, det er ikke etablert egne enheter for å ivareta disse sakene og sakene fordeles derfor på ulike driftsenheter og etterforskningsmiljøer. Det fremkommer at politiet ikke foretar «noen systematisk patruljering på Internett» og i den grad de i det hele tatt utfører politiarbeid på internett «skjer det sporadisk av tjenestemenn, med forskjellig grad av opplæring og erfaring» (Storruste & Magnussen, 2012, s. 17).

Kripos er et særorgan underlagt POD. Kripos skal ha spisskompetanse på en rekke fagområder, deriblant kommunikasjonskontroll og sporing på internett (Politiet, 2011, s. 46). Arbeidsgruppen påpeker at Kripos har et særskilt ansvar for å etterforske alvorlig IKT-kriminalitet, og at de har erfaring med etterforskning av grove skadeverk. Det omtales ikke i hvilken grad de innehar oppgaver eller erfaring knyttet til håndtering av pågående skadeverk. Det indikeres imidlertid at de har begrenset kapasitet og at det skal være en av grunnene til at distriktene ofte blir stående fast i de sakene som krever datateknisk kompetanse – fordi de ikke får tilgang på bistand fra Kripos. I rapporten står det dataangrep mot sentrale samfunnsinstitusjoner grenser mot PST sitt arbeidsområde, men grensene mellom PST og andre enheter i politiet er ikke nærmere beskrevet i rapporten (Storruste & Magnussen, 2012).

PST er Norges sivile etterretnings- og sikkerhetstjeneste og har ansvar for nasjonens indre sikkerhet. PSTs primære oppgave er, som gitt i politiloven, å forebygge og etterforske straffbare handlinger mot nasjonens sikkerhet. PST utarbeider trusselvurderinger som ledd i arbeidet med å ivareta den norske stats sikkerhet og selvstendighet, og har en rådgivende funksjon for

regjeringen og andre norske myndigheter. PST skal ha fått økte bevilgninger for bruk innen cybersikkerhet de siste årene (Meld. St. nr. 21 (2012-2013), 2013), men det fremkommer ikke, i de dokumentene som inngår i denne analysen, i hvilken grad de har evne til å kunne håndtere pågående cyberangrep.

Det er gjennomgående forebygging og etterforskning som står i fokus i rapporten til POD, håndtering av cyberhendelser ved bruk av den makt og myndighet som tillegger politiet er ikke omtalt i rapporten. Det kan være en indikasjon på at politiet ikke innehar denne kapasiteten. Målsetningen til politiet er å håndheve lov og orden i det digitale samfunnet på en effektiv og sikker måte (Storruste & Magnussen, 2012, s. 25), men innholdet i rapporten for øvrig antyder at dette ikke var tilfelle i 2012. Imidlertid kan det ha skjedd endringer i ettertid.

5.4 Samferdselssektoren

SD har ansvar for sikkerheten knyttet til ekom-nett og ekom-tjenester. Departementet forvalter loven om elektronisk kommunikasjon (ekomloven) og etatsstyrer PT. Å styrke IKT-infrastrukturen oppgis som et prioritert område i *Nasjonal strategi for informasjonssikkerhet*, og i den sammenheng er SD gitt i ansvar å sørge for en robust og pålitelig ekom-infrastruktur, begrense konsekvensene ved utfall og øke sikkerheten i mobilnettene (Regjeringen, 2012b, s. 15-17). PT har på vegne av departementet ansvar for å sette krav til telesikkerhet og teleberedskap, og vurdere tiltak for å øke robustheten i telenettene, samt føre tilsyn med at pålagte tiltak blir iverksatt (Post- og teletilsynet, 2014). PT sin vurdering er at operatørene har gjennomgående god evne til å håndtere løpende drift men at de ikke har tilfredsstillende fokus på og evne til å opprettholde nødvendig sikkerhet i ekstraordinære situasjoner. Denne vurderingen gjorde PT blant annet på grunnlag av sårbarheter i utstyr og nettstrukturer, herunder:

- Defekter og feil i maskinvare og programvare
- Generelle svakheter i nettkonfigurasjonene pga. høy kompleksitet og store endringer i nettstrukturene
- Begrenset robusthet i IP-baserte infrastrukturer
- "Single-point-of-failure" hos alle operatører
- Svakheter i regimene for elektronisk adgang til utstyr i infrastrukturene

(Post- og teletilsynet, 2012b, s. 9,10).

DSB mener, som nevnt i kapittel 4.2, at teknologiskiftet i ekom-infrastrukturen vil få betydning for samfunnets robusthet og sårbarhet. «Redundansen vil bli redusert og ekomnettene vil i større grad enn før bli eksponert for cyberangrep av ulike slag» (DSB, 2013b, s. 6).

Ekomloven stiller krav til at tilbyder må opprettholde nødvendig beredskap og tilby sine ekom-nett og tjenester med forsvarlig sikkerhet i hele spekteret fra fred til krig (Ekomloven, 2003). Dette er helt i tråd med ansvarsprinsippet, som ble presentert innledningsvis i oppgaven (kap 3.1.2). Den som har ansvar for en virksomhet under normale forhold har også et ansvar i en krisesituasjon. I kravet om nødvendig beredskap ligger det at nett og tjenester skal sikres på en slik måte at bruker, selv i situasjoner der nettet utsettes for ekstraordinære påkjenninger, så langt som mulig skal kunne benytte grunnleggende ekom-tjenester.

Nasjonal strategi for informasjonssikkerhet påpeker at infrastruktureierne i sektoren skal inngå i den proaktive operative beredskapen for å kunne forebygge, oppdage og koordinere håndteringen av alvorlige IKT-hendelser. Telenor er, som tidligere omtalt i kapittel 4.2, den dominerende leverandøren av ekom-nett og teletjenester i Norge og vies derfor ekstra oppmerksomhet i denne innholdsanalysen. I et innlegg i debatten om *digital robusthet*, fremhever administrerende direktør i Telenor, Berit Svendsen, at robustheten til et tele- og datakommunikasjonsnett er avhengig av en betydelig drift-, beredskap- og sikkerhetsorganisasjon. Telenor har etablert et eget responsmiljø, Telenor Security Operations Centre, TSOC. Operasjonssentralen overvåker Telenor sin infrastruktur, for å avdekke eventuelle fysiske brudd, programvarefeil og sikkerhetstrusler. «Hvert eneste døgn blir det oppdaget små feil og det blir iverksatt feilretting» sier Svendsen (Svendsen, 2014). Ved hjelp av egne sensorer i sin infrastruktur kan Telenor oppdage og varsle sine kunder om angrep. På bloggen sin sier TSOC at de «driver en 24/7 – tjeneste for sikkerhetsovervåkning av kunders nettverk» og at deres analytikere «gjør kontinuerlig analyse av uønsket aktivitet på internett» (Telenor SOC, 2014).

5.5 Forsvarssektoren

Nasjonal strategi for informasjonssikkerhet konstaterer at FD sitt ansvar relatert til IKT-sikkerhet i Norge er knyttet til militær sektor og etatsstyring av NSM (Regjeringen, 2012a, s. 15-16). I handlingsplanen påpekes det imidlertid at det er flere aktører i forsvarssektoren som har ansvar innenfor informasjonssikkerhet og cyberoperasjoner og FD ble derfor gitt i oppgave å fastsette ansvar, oppgaver og myndighet internt i sektoren (Regjeringen, 2012b, s. 13). FD har i ettertid gitt ut *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner* (FDs cyberretningslinjer), hvor dette fastsettes. Retningslinjene gjelder for hele forsvarssektoren, i fred, krise og krig, og omhandler både håndtering av informasjon og informasjonssystemer (Forsvarsdepartementet, 2014, s. 5).

Informasjonssikkerhet

Målsettingen er at Forsvarssektoren skal ha tilstrekkelig informasjonssikkerhet i cyberdomenet, og til enhver tid forebygge, avdekke, vurdere og forsvare seg mot cyberangrep. Sektoren skal være forberedt på å håndtere alle former for hendelser som kan ramme egne IKT-systemer og ha evne til å gjenopprette normal funksjonalitet. Cyberforsvaret har ansvar å beskytte Forsvarets egen infrastruktur og ivareta håndtering i Forsvaret, mens NSM har et nasjonalt sektorovergripende ansvar for informasjonssikkerhet.

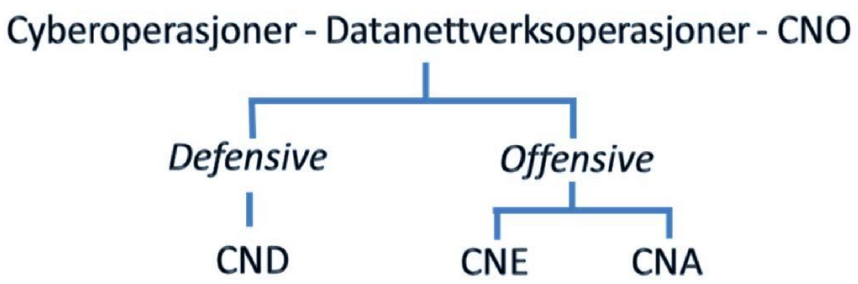
FD fremhever at det er viktig å sikre nødvendig samordning med sivil sektor i cyberkriser, og påpeker at det er NSM som skal koordinere. Samtidig konstater FD at de cyberangrep som krever koordinering på sentralt nivå skal håndteres i henhold til gjeldende prinsipper for sentral krisehåndtering (Forsvarsdepartementet, 2014, s. 11). Den sentrale krisehåndteringen består, som redegjort for i kapittel 3.1.3 av: lederdepartement som skal ivareta samordningen mellom departementene i mindre alvorlige kriser, Kriserådet skal sørge for samordningen i komplekse kriser og Krisestøtteenheten skal være sekretariat for sivil krisehåndtering. Det er den enkelte fagstatsråd som har ansvar for krisehåndtering innenfor egen sektor, og for å samordne denne med øvrige departementer og sektorer. Hvor NSM sin koordineringsrolle kommer inn i det sentrale krisehåndteringsapparatet er ikke spesifisert. FD sier Forsvarets bistand ved cyberhendelser eksempelvis kan innebære faglig rådgivning, støtte fra enheter med særskilt

kompetanse og bistand til gjenoppretting av kommunikasjonsnettverk (Forsvarsdepartementet, 2014, s. 12).

Cyberoperasjoner

Cyberoperasjoner er operasjoner som har til hensikt å nå definerte målsettinger i og gjennom cyberdomenet, herunder tiltak for å påvirke motstanders datanett og beskytte egne nett. Begrepene cyberoperasjoner og datanettverksoperasjoner omtales som synonymer i FDs cyberretningslinjer og tilsvarer det som i NATO kalles Compuer Network Operations (CNO). I NATO doktrinen *Allied Joint Doctrine for Information Operations* (AJP 3.10) beskrives CNO som en av flere informasjonsaktiviteter, som brukes for å påvirke motpartens vilje, forståelse og evne til støtte for alliansens oppdrag, samt å sikre at egen informasjon blir ivaretatt, er trygg og tilgjengelig for egne beslutningstakere (NATO, 2009). CNO omfatter Computer Network Exploration (CNE), Computer Network Attack (CNA) og Computer Network Defence (CND). FD sier at «CNE skal bidra til å søke etter, fange opp, identifisere og lokalisere aktiviteter og informasjon i cyberdomenet i den hensikt å oppnå situasjonsforståelse og for å kunne gjenkjenne trusler» og at «CNA skal bidra til å redusere eller hindre en motstanders evne til å utnytte cyberdomenet til egne operasjoner» mens «CND er å anse som en defensiv aktivitet som skal sikre handlefrihet i egen informasjons-infrastruktur, til tross for offensive aktiviteter fra en motstander» (Forsvarsdepartementet, 2014, s. 6).

Cyberoperasjoner kategoriseres, som vist i figur 11, i offensive og defensive operasjoner. De offensive omfatter både CNE og CNA mens CND er defensiv.



Figur 11: Cyberoperasjoner (Forsvarsdepartementet, 2014, s. 6)

Nasjonalt er det E-tjenesten som har fått ansvar for offensive cyberoperasjoner og Cyberforsvaret for defensive cyberoperasjoner.

Etterretningstjenesten - Offensive cyberoperasjoner

E-tjenesten er underlagt Forsvarssjefen, men er ikke avgrenset til å arbeide med militære problemstillinger. Tjenesten arbeider innenfor de saksfelt overordnede politiske og militære myndigheter prioriterer (Etterretningstjenesten, 2014). I årets Fokus rapport sier E-tjenesten at de primært har fokus på cybertrusler fra statlige aktører, eksempelvis Russland og Kina. Dernest vier de sin oppmerksomhet på «selvstendige, ikke-statlige aktører som opererer på vegne av, støttes eller utnyttes av statlige myndigheter» og organiserte ekstremistgrupper (Etterretningstjenesten, 2014, s. 59).

I cyberretningslinjene fra FD er E-tjenesten gitt i ansvar å:

- Utføre tidlig varsling av mulige cybertrusler fra fremmede stater, organisasjoner eller individer
- Bidra i produksjon av nasjonalt cyberrisikobilde (CKG)
- Være koordinerende myndighet innen cyberoperasjoner
- Gjennomføre offensive cybertiltak (Forsvarsdepartementet, 2014, s. 18)

FD påpeker at offensive cyberoperasjoner skal være underlagt politisk kontroll og strategisk styring, på lik linje med andre militære maktmidler (Forsvarsdepartementet, 2014, s. 12).

Cyberforsvaret - Defensive cyberoperasjoner

Cyberforsvaret ble offisielt etablert 18.september 2012 etter at Regjeringen i langtidsplanen, for perioden 2013-2016, hadde bestemt at Forsvarets informasjonsinfrastruktur (INI) skulle bytte navn til Cyberforsvaret. Bakgrunnen for etableringen var erkjennelsen av at cyberdomenet var blitt et nytt krigføringsområde og at Forsvaret måtte forberede seg på å kunne håndtere cyberangrep mot egne systemer. Cyberforsvarets oppdrag er «å operere Forsvarets informasjonsinfrastruktur, herunder å etablere, drifte, videreutvikle, beskytte og bekjempe trusler knyttet til denne infrastrukturen, samt understøtte Forsvarets operasjoner hjemme og ute» (IVB LTP (2013-2016), 2012, s. 98).

I iverksettingsbrevet for 2013-2016 er Cyberforsvaret gitt fire prioriterte oppgaver:

- Understøtte operative enheter og Forsvarets samlede virksomhet, herunder å sørge for at Forsvaret har effektive, sikre og robuste kommando- og kontrolløsninger
- Ivareta defensive cyberoperasjoner, herunder «å forebygge, avdekke, vurdere og foreta tidlig varsling av digitale angrep mot Forsvarets systemer» (IVB LTP (2013-2016), 2012, s. 97)
- Være faglig pådriver innenfor utvikling av nettverksbasert forsvar
- Yte bistand til sivil sektor ved digitale angrep

Det påpekes at bistand til sivil sektor ikke skal være dimensjonerende for Cyberforsvaret og at det eventuelt skal skje i samarbeid med NorCERT. Det er NSM som har ansvaret for å varsle om og bidra til å koordinere håndteringen av digitale angrep mot kritisk infrastruktur og at «Forsvarets rolle kan blant annet være faglig rådgivning og støtte fra enheter med særskilt kompetanse» (Prop. 73 S (2011-2012), s. 58). Det presiseres samtidig at Forsvarets bistand til sivile myndigheter kun er aktuelt dersom det ikke finnes relevante sivile ressurser. Forsvaret fremhever viktigheten av tidlig varsling av digitale angrep, og rutiner for hurtig iverksettelse av tiltak for å hindre eller minske skadevirkninger. «Som del av dette må det sikres god og hurtig informasjonsdeling mellom relevante aktører på ulike nivåer» (Prop. 73 S (2011-2012), s. 58).

FD påpeker i sine cyberretningslinjer at: «Forsvarets deployerbare IKT- og CND-kapasiteter skal ha en beredskap som er tilpasset Forsvarets behov, og enhetene som etablerer og drifter disse kan ved behov benyttes til støtte for det sivile samfunn i henhold til gjeldende bestemmelser for slik støtte» (Forsvarsdepartementet, 2014, s. 14).

Det er angrep på logiske sårbarheter[32] i ekom-infrastrukturen som står i fokus i denne oppgaven. *Avdeling for beskyttelse av kritisk infrastruktur* (BKI) i Cyberforsvaret antas å ha særskilt kompetanse på dette feltet. BKI miljøet var tidligere en del av FOST (FSA) men ble etter opprettelsen av INI overført dit. BKI skal «bidra til å beskytte Forsvarets infrastruktur gjennom støtte til analyse av sårbarheter, ondsinnet kode og angrep mot Forsvarets systemer. Avdelingen har deployerbare elementer og mulighet til å bistå med rådgivning og liaisonering ved håndtering

[32] Ref pkt 1.4: Logiske sårbarheter omfatter sårbarheter realisert i programvare, herunder protokoller og tjenester samt logisk redundans. Angrepsmidler mot logiske sårbarheter kan være «alt fra utnyttelse og bruk av allmenn

av trusler og angrep mot norsk infrastruktur ute og hjemme» (Prop. 73 S (2011-2012), s. 103). Avdelingen utgjør *Forsvarets sentrale responsmiljø* (CERT).

I en reportasje i Forsvarets Forum i fjor ble BKI og *Cyber-ambulansen* presentert. Utrykningskapasiteten til BKI ble beskrevet som tre biler med tilhørende tilhengere, klargjort og tilpasset for *cyberkrig* og klar til å rykke ut på kort tid. Den militære styrken skal bestå av «noen dusin mannlige og kvinnelige dataingeniører» (Ravnaas, 2013). «I prinsippet kan vi koble oss til og bistå hvem som helst, når som helst og hvor som helst» sa oberstløytnant Gunnar Salberg, daværende sjef for BKI. Men han presiserte samtidig at det er NorCERT og NSM som sitter i *førersetet* når det gjelder bistand til næringsliv og det sivile samfunn, og at BKI er en ekstra ressurs som kan benyttes ved behov. Salberg sa at både banker, strømselskaper og andre viktige aktører kan få nyttig hjelp av styrken, enten til analyse av en hendelse eller hjelp til å løse den (Ravnaas, 2013). Samtidig påpekte han at det er sikring av Forsvarets egne nettverk, eksempelvis ved øvelser og operasjoner som er BKI sitt ansvar: «I likhet med baser som har kringvern i form av soldater og vaktposter, sikrer BKI eksempelvis datanettverk på øvelser» (Ravnaas, 2013). I samme intervju avkreftet Salberg at Cyberforsvaret kan gå til motangrep i cyberspace: «vi har defensive operasjoner der vi overvåker, avslører og setter i gang tiltak for å forhindre nye angrep» forklarte han.

5.6 Oppsummering

Ekom-leverandørene skal kunne forebygge, oppdage og koordinere håndteringen av alvorlige IKT-hendelser i egen infrastruktur. Operasjonssenteret i NSM, NorCERT, skal ved hjelp av VDI og nasjonalt samarbeid ha evne til å oppdage og analysere data knyttet til alvorlige hendelser på internett. Det er imidlertid frivillig å være med i VDI samarbeidet, også for virksomheter som eier kritisk infrastruktur. Dersom en hendelse rammer flere virksomheter har NorCERT fått i ansvar å *koordinere håndteringen* av dem, men det er ikke beskrevet hva denne koordineringen innebærer. NSM sin myndighet er begrenset til håndhevelse av sikkerhetsloven.

Innholdsanalysen viser at politiet er gitt i ansvar å avdekke, identifisere og håndtere datakriminalitet, uavhengig av om denne rammer en eller flere virksomheter. De skal kunne håndtere et pågående cyberangrep mot ekom-infrastrukturen ved bruk av den makt og myndighet

---

tilgjengelig infrastruktur og kode som publiserte nettverksverktøy på Internett, til angrepskode og mer

som tillegger politiet. Imidlertid tilsier funn i den samme analysen at politiet ikke har tilstrekkelig kompetanse og kapasitet til å håndtere datakriminalitet i dag. Politidistriktene arbeider i liten grad med denne typen kriminalitet, de foretar ikke noen systematisk patruljering på internett og i den grad de i det hele tatt utfører politiarbeid på internett skjer det sporadisk av tjenestemenn, med forskjellig grad av opplæring og erfaring. Innholdsanalysen indikerer at politiet ikke vil ha tilstrekkelig kapasitet til å ivareta sitt ansvar dersom ekom-infrastrukturen rammes av en alvorlig cyberhendelse og det vil derfor kunne bli behov for bistand.

Cyberforsvarets ansvar, og myndighet, er knyttet til Forsvarets kommunikasjonsinfrastruktur. Deres oppdrag er å etablere, drifte, videreutvikle, beskytte og bekjempe trusler mot denne infrastrukturen, samt understøtte Forsvarets operasjoner hjemme og ute. Cyberforsvaret skal i tillegg kunne yte bistand til sivil sektor ved digitale angrep, men dette er ikke en dimensjonerende oppgave for Cyberforsvaret, og det skal kun skje dersom det ikke finnes relevante sivile ressurser. I en cyberkrise skal Forsvaret kunne bistå med faglig rådgivning og støtte fra enheter med særskilt kompetanse. Den enheten som vurderes å være mest sentral i forhold angrep på logiske sårbarheter i ekom-infrastrukturen er Cyberforsvarets *Avdeling for beskyttelse av kritisk infrastruktur* (BKI). Avdelingen har deployerbare elementer og mulighet til å bistå med rådgivning og liaisonering ved håndtering av trusler og angrep mot norsk infrastruktur.

Innholdsanalysen indikerer at det vil kunne bli behov for bistand dersom ekom-infrastrukturen rammes av en alvorlig cyberhendelse og samtidig viser analysen at Cyberforsvaret besitter relevante kapasiteter. Det er likevel behov for ytterliggere empiri for å kunne drøfte Cyberforsvarets rolle.

---

spesialskrevne verktøy» (Windvik et al., 2007, s. 23).

6 Cyberforsvarets rolle – en drøfting

Innholdsanalysen indikerte at sivile myndigheter vil kunne få behov for bistand dersom nasjonen rammes av et alvorlig cyberangrep og videre at Cyberforsvaret besitter kompetanse, verktøy og erfaring fra sikring av egen infrastruktur. For å få mer empiri til å kunne drøfte når Cyberforsvaret skal bistå og med hva er det hensiktsmessig å se på håndteringen av to cyberhendelser: industrispionasjen mot Telenor i 2013 og Øvelse CyberDawn i 2013. Ved å sammenstille erfaringer fra disse to casene vil få et godt grunnlag for å drøfte Cyberforsvarets rolle dersom ekom-infrastrukturen rammes av et cyberangrep.

6.1 En casestudie av cyberangrep mot sivil infrastruktur

Denne casestudien vil ha fokus på de oppgavene som er vektlagt i *Nasjonal strategi for informasjonssikkerhet,* herunder *oppdage, analysere, koordinere og håndtere. Analysere* vil deles i to, analyse av malware[33], - som for så vidt kan gjøres fra hvor som helst, og den analyse som forutsetter tilknytning til nettverket (overvåkning). Casestudien vil bygge på funn gjort tidligere i studien. Innholdsanalysen viste hvem som har fått ansvar for å ivareta oppgavene, samt aktørenes antatte kapasitet. Casestudien vil se på hvem som faktisk ivaretok oppgavene i disse casene og hvordan, samt om det viste seg å være behov for støtte? Den ene casen dreide seg om industrispionasje, et målrettet angrep mot Telenors forretningsvirksomhet, mens den andre casen innebar angrep på samfunnskritisk infrastruktur.

De oppgaver hvor det viste seg å være behov for støtte vil så drøftes fortløpende. Har Cyberforsvaret kunnskap og verktøy til å kunne støtte og kan Cyberforsvaret bistå gitt dagens prinsipper for krisehåndtering og regulering av det sivil-militære samarbeidet?

Kildene til denne casestudien består av rapporter[34], video[35], medieoppslag[36] og egne intervjuer[37]. Innledningsvis vil det gis en presentasjon av casene som inngår i caseanalysen.

[33] Malware kommer av de engelske ordene Malicious Software og er en fellesbetegnelse på ondsinnet programvare som eksempel datavirus, ormer og trojanere
[34] Rapport fra Norman Shark i forhold til Industrispionasjesaken. Intern rapport skrevet av Telenor men med bidrag fra alle aktørene, etter øvelse CyberDawn
[35] Telenor gjorde opptak under hele øvelsen og har i ettertid satt i sammen en film. Kort-versjonen av filmen ligger tilgjengelig på internett.

Industrispionasjesaken

I første kvartal 2013 ble Telenor utsatt for et målrettet angrep hvor datamaskinene til flere av sjefene i Telenor ble tømt for data. Innledningsvis var det umulig å si om angrepet kom fra Norge eller utlandet, men mye tydet på at det måtte være godt organiserte og ressurssterke miljøer som stod bak. Industrispionasjen ble oppdaget av Telenor Security Operations Centre (TSOC). Operasjonssentralen reagerte på at det var unormal trafikk til ukjente IP-adresser i utlandet. Angrepet hadde startet med at ledere i Telenor fikk tilsendt elektronisk post fra tilsynelatende kjente forbindelser. E-postene kom som en av flere i en pågående korrespondanse, de var skrevet på norsk og med innhold som forventet. I e-postene var det lenker til infiserte nettsider og/eller infiserte zip-filer. Når disse ble åpnet ble det installert en ondsinnet kode, en trojaner, på datamaskinen, som så sørget for å sende ut data fra maskinen. Logger i Telenor sine systemer viser at e-post, alle typer filer, passord og andre personlige data er blitt tatt. Fordi så mye forskjellig informasjon ble lastet ned var det vanskelig å se hva angriperne egentlig var ute etter. Den ondsinnede koden var skreddersydd og ukjent for Telenor sine underleverandører. Telenor varslet NorCERT og Cyberforsvaret umiddelbart og holdt de løpende orientert under veis. Hendelsen ble anmeldt til politiet (Johansen, 2013; NSMs sikkerhetskonferanse, 2013).

Norman Shark gransket skadevaren og avdekket en omfattende global infrastruktur av såkalte kommandoservere – servere som brukes til å sende data eller skadevare, ta imot stjålne data, samt kontrollere ofrenes datamaskiner. Norman sin analyse tyder på at angrepet på Telenor stammer i fra India og at den samme infrastrukturen har vært benyttet til omfattende spionasje mot ofre i minst 12 land. Angrepene skal ha pågått i minst tre år og pågår fortsatt (Jørgenrud, 2013a). Snorre Fagerland, analysesjef i Norman, sier at majoriteten av angrepene har vært rettet mot militæret og myndighetene i Pakistan, men det er ikke funnet bevis for at angrepene er sponset av eller utført på ordre fra en nasjonalstat (Fagerland et al., 2013).

Øvelse CyberDawn 2013

Telenor var initiativtager til *CyberDawn*, og det var også Telenor som ledet øvelsen. Øvingsdeltagerne var ved siden av Telenor, Cyberforsvaret, DNB, Sparebank 1, NSM og Evry. I tillegg var PT, POD, Kripos og Asker og Bærum Politidistrikt involvert. Øvelsen ble kjørt 3. og 4. september 2013, samtidig som Forsvarets *Øvelse Hovedstad* foregikk i Oslo og Akershus

[36] Øvelse CyberDawn fikk medieoppslag både før, under og etter øvelsen. Sentrale aktører ble intervjuet.

(29.august til 5.september). Fiktive nyheter ble sent ut til de øvende de siste ukene før øvelsen og dannet et globalt bakteppe og trusselbildet for øvelsen: all handel i aksjer og verdipapirer på Nasdaq-børsen i USA var blitt stanset og NRK hadde informasjon som indikerte at norske hackere kunne gjøre det samme mot norske finansinstitusjoner (Dyrlie & Landaasen, 2013; Tønnesen & Landaasen, 2013a).

CyberDawn startet med at datamaskinene til ansatte i Telenor ble kompromittert. I likhet med *Industrispionasjesaken* tok noen utenifra kontroll over Telenor sine maskiner. Angriper fikk mulighet til å samle informasjon og grave seg videre innover i Telenor sine systemer. Til forskjell fra *Industrispionasjesaken* innebar *CyberDawn* at datamaskinene til driftspersonell også ble kompromittert. Angriper fikk tilgang til Telenor sin database over alle samband i Norge og kunne bruke denne til å planlegge angrep mot transportnettet, samtidig som han manipulerte databasen og gjorde det vanskelig for Telenor å feilsøke. Det var uklart hvilken hensikt angriper hadde, men det var klart at den samfunnskritiske infrastrukturen stod i fare og Telenor varslet PT og SD. Administrerende direktør i Telenor ga ordre om at nettet måtte isoleres for å unngå spredning og all tilgjengelig ekspertise måtte hentes inn. En nasjonal krise i det digitale rom var blitt et faktum og Telenor henvendte seg til politiet for å få støtte til å stoppe angrepet. Politiet snudde seg til Forsvaret og FOH ga Cyberforsvaret ordre om å bistå Telenor (Dyrlie & Landaasen, 2013; Tønnesen & Landaasen, 2013a).

Øvingsleder i Telenor, Storm Jarl Landaasen, hevder at hendelsene under *CyberDawn* kunne vært reelle. «Alle scenarioene ble utløst av ondsinnede aktører utenfor Telenor og de kunne skjedd i et større omfang, og med større konsekvenser» (Dyrlie & Landaasen, 2013, s. 4). En angriper med god tid og store ressurser kunne faktisk ha gjennomført alt det de testet under denne øvelsen – og vil trolig fortsatt ha mulighet til det i flere år fremover. Scenarioet var så alvorlig at flere aktører i så fall ville ha blitt involvert, herunder departementene, FOH, kriserådet og KSE (Dyrlie & Landaasen, 2013; Tønnesen & Landaasen, 2013a).

[37] Har intervjuet 8 personer som har mye kunnskap om emnet og som alle sitter i virksomheter som vil være sentrale dersom infrastrukturen skulle rammes av en alvorlig cyberhendelse, herunder to fra Telenor, NSM, POD, FOH, FD og to fra Cyberforsvaret.

6.2 Oppdage hendelsen og varsle

Det å oppdage at uvedkommende har skaffet seg tilgang til nettverket eller dataene som ligger der er en forutsetning for videre håndtering. Innholdsanalysen, i kapittel 5, viste at NorCERT ved hjelp av VDI og nasjonalt samarbeid, herunder samarbeid med den virksomhet som eier ekom-infrastrukturen, skal ha evne til å oppdage alvorlige hendelser på internett.

Hans Christian Pretorius, avdelingsdirektør ved operativ avdeling i NSM, forklarer at NorCERT kan se trafikken som går inn og ut av de nettene hvor de har VDI-sensor. De kan se om virksomheten lekker data, fra hvilke klienter (IP-adresser) det lekker data i fra og til hvilken server på yttersiden disse dataene sendes til. Alarmer trigges dersom det oppdages trafikk fra en kjent server eller dersom det oppdages kjent skadevare[38] (Pretorius, 2014, 20.mars). NorCERT mottar varsler fra nasjonale og internasjonale samarbeidspartnere gjennom det sivile CERT-samarbeidet, herunder informasjon om skadevare og kommandoservere[39], og oppdaterer databasen sin fortløpende med denne informasjonen. Det er imidlertid den som har blitt angrepet, den som har signaturen, som bestemmer i hvilken grad NorCERT kan dele denne informasjonen med andre, - varsle andre (Pretorius, 2014, 20.mars).

Telenor er ikke med i VDI samarbeidet men har egne sensorer i sin infrastruktur. Både industrispionasjen og angrepene i *CyberDawn* ble oppdaget av TSOC (NSMs sikkerhetskonferanse, 2013; Tønnesen & Landaasen, 2013a).

Innholdsanalysen viste at Cyberforsvaret har ansvaret for å oppdage angrep mot Forsvarets infrastruktur samt å foreta varsling. Forsvaret har en fast sensorinfrastruktur, sensorer som er i bruk i Forsvarets nett 24/7, og i tillegg mobile ressurser som kan tas ut ved behov. Behovet kan være å dekke midlertidige behov under operasjoner og øvelser eller å øke eksisterende sensorkapasitet ved hendelser i de militære nettene (Malmedal, 2014, 21.februar; Heen, 2014, 25.februar). Cyberforsvaret har inngått en samarbeidsavtale med Telenor. Intensjonen med avtalen er først og fremst kompetanseheving. Telenor og Cyberforsvaret sender hverandre sikkerhetsvarsler når de oppdager sårbarheter, dette er informasjon som forså vidt kan deles med alle via NorCERT, men de deler denne direkte. Den informasjonen Cyberforsvaret fikk fra Telenor i forbindelse med *Industrispionasjesaken* gjorde Cyberforsvaret i stand til å undersøke

[38] Skadevare og Malware brukes om hverandre som en fellesbetegnelse på ondsinnet programvare, som eksempel datavirus, ormer og trojanere
[39] Servere som brukes til å sende data eller skadevare, ta imot stjålne data, samt kontrollere ofrenes datamaskiner

om Forsvaret var utsatt for tilsvarende angrep (Malmedal, 2014, 21.februar). Dersom Forsvarets nettverk hadde vært rammet ville Cyberforsvaret ha varslet Telenor og NorCERT, men støtter primært ikke med noe utover dette.

6.3 Analyse

Analyse er i denne sammenheng er å etablere situasjonsforståelse, å finne ut hva en er utsatt for, hva skadevaren har gjort og gjør, hva uvedkommende holder på med og hvorfor, samt hvordan en kan minimere konsekvenser og normalisere. Innholdsanalysen, i kapittel 5, viste at NorCERT ved hjelp av VDI og nasjonalt samarbeid, herunder samarbeid med den virksomhet som eier ekom-infrastrukturen, skal ha evne til å analysere alvorlige hendelser på internett.

NorCERT har gjennom VDI-samarbeidet forpliktet seg til å bistå medlemmer og partnere med analyse. Partnere får tilbud om tettere og bedre oppfølging enn medlemmer, som eksempel støtte på egen lokasjon. Både medlemmer og partnere får mer informasjon og støtte fra NorCERT enn de som ikke er tilknyttet dette samarbeidet, uavhengig av om virksomheten forvalter kritisk infrastruktur eller ikke[40] (Pretorius, 2014, 20.mars). Dog er det ikke tilfeldig hvem som er en del av samarbeidet. Pretorius finner det naturlig at de objekter som pekes ut som kritisk infrastruktur også får[41] VDI-sensor etterhvert. Imidlertid er det, som innholdsanalysen viste, opp til eier av objektet å søke om tilknytning til VDI. NorCERT sin intensjon og oppdrag er likevel å støtte, med det de kan, selv om virksomheten ikke er en del av samarbeidet. Det forutsetter imidlertid at virksomheten sender en RFI (request for information) til NorCERT. I dette ligger det at den angrepne virksomheten selv må si i fra om at de *lekker* data til en spesifikk IP-adresse eller at deres sensorer har fanget opp en ukjent signatur for så å spørre om NorCERT har kjennskap til denne fra før. Dersom NorCERT har kjennskap til serveren eller har signaturen i sin database og slik kjenner hvilke egenskaper denne programvaren har kan de informere virksomheten om hvilke plattformer som kan ha blitt infisert, hva de skal lete etter og slik sett bistå (Pretorius, 2014, 20.mars).

Disse to casene innebar analyse av malware og nettverk (overvåkning), det er hensiktsmessig å se på disse hver for seg da den ene forutsetter tilgang til nettverket og den andre ikke.

[40] I en krisesituasjon vil imidlertid NorCERT prioritere tiltak og prosedyrer uavhengig av medlemskap/partnerskap og koordinerer hendelseshåndteringen ut fra en helhetlig nasjonal verdivurdering i en krisesituasjon (NSM).
[41] *Får* kan være misvisende, da virksomhetene er med på å finansiere NorCERT gjennom medlemskap eller partnerskap. Partnere betaler 500 000kr i medlemsavgift, medlemmer 200.000kr (NSM)

Analyse av malware

I situasjoner som *Industrispionasjesaken* vil den angrepne virksomheten kunne få behov for støtte til analyse av malware. Funn fra kapittel 4.4 viste at angrepene kan ramme raskt og uten forvarsel og ha potensiale til å eskalere seg raskt, det er derfor viktig å få oversikt over situasjonen kjapt og slik kunne begrense skadene. Når flere miljøer, ressurser fra forskjellige virksomheter med sine kontaktnett, samarbeider øker muligheten for å *knekke koden* (Dyrlie, 2014, 24.februar).

Dokumentanalysen i kapittel 5.5 viste at Cyberforsvaret skal ha kompetanse og ressurser innen analyse av sårbarheter og ondsinnet kode. Telenor varslet Cyberforsvaret umiddelbart om angrepet i 2013 og holdt de løpende orientert, men BKI støttet ikke. Det nye totalforsvarskonseptet innebærer, som nevnt i kapittel 3.2.3, at Forsvarets ressurser i større grad skal kunne brukes til støtte for politiet og sivile myndigheter og Cyberforsvaret besitter ressurser som teoretisk sett kan støtte. På den annen side kommer ikke Telenor inn under kategorien *myndighet* og Cyberforsvaret kan ikke bistå private selskaper direkte med dagens regulering av det sivil-militære samarbeidet. Når det er snakk om *bistand* er det, som det ble redegjort for i kapittel 3.2.2, primært bistandsinstruksen, altså bistand til politiet. Og sekundært det nasjonale CERT-apparatet hvor Cyberforsvaret kan inngå i en større dugnad koordinert av NorCERT (Malmedal, 2014, 21.februar). Imidlertid kom det ingen anmodning fra NorCERT om å bistå i denne situasjonen, og BKI ville ikke hatt kapasitet til å bidra inn i analysen av koden på daværende tidspunkt, - uten å måtte omdisponere personell (Heen, 2014, 25.februar).

Ansvar, likhet og nærhet prinsippene som ble presentert innledningsvis i oppgaven (kapittel 3.1) innebærer at det er den virksomheten som har ansvar for fagområdet til daglig som også har ansvar for å håndtere ekstraordinære hendelser, hendelsen skal håndteres med en organisasjon som er mest mulig lik den en opererer med i det daglige, og på så lavt nivå som mulig. *Industrispionasjesaken* ble håndtert i tråd med disse prinsippene. Telenor etablerte kriseledelse for å sikre koordinering og beslutninger, og varslet PT, men PT eller departementet hadde ingen rolle i håndteringen. På den annen side er det ingen aktør i samfunnet, hverken privat eller offentlig, som greier å holde oversikt over alle trusler som kan rettes mot nettverk og elektroniske informasjonssystemer. Derfor er det viktig at aktørene har et godt samvirke.

Prinsippene ansvar og samvirke skal, som påpekt i kapittel.3.1.2, være overordnet og styrende i sektorovergripende kriser som scenarioet i CyberDawn. I CyberDawn ble Cyberforsvaret bedt om å bistå i analyse av ondsinnet kode. BKI mottok ondsinnet kode, et *malware sample*[42], fra en av øvelsesdeltagerne og bistod i tråd med samvirkeprinsippet. «NorCERT hadde allerede gjennomført en initial analyse og ønsket at BKI skulle støtte opp under de vurderinger som var gjort» (Dyrlie & Landaasen, 2013, s. 7). Innholdsanalysen i kapittel 5.2 viste at NorCERT håndterer flere tusen cyberhendelser årlig og besitter mye kunnskap og erfaring relatert til datanettverk, trusler og sårbarheter. Det kan være grunn til å stille spørsmål ved behovet for bistand fra Cyberforsvaret til denne oppgaven. På den annen side besitter Cyberforsvaret mye kunnskap og erfaring relatert til denne type infrastruktur og analyse av malware, og har samtidig et annet kontaktnett enn NorCERT. Når ressurser fra forskjellige virksomheter med sine kontaktnett samarbeider øker muligheten for å lykkes.

Forsvarets ressurser skal kunne tas i bruk til støtte for sivile myndigheter, som NSM, i henhold til det nye totalforsvarskonseptet, som ble presentert i kapittel 3.2.3[43]. Cyberforsvaret vil kunne få spørsmål om å bistå gjennom CERT-samarbeidet også i andre hendelser. På den annen side har Cyberforsvaret begrenset kapasitet og det vil, som beskrevet i kapittel 3.2.4, være opp til FOH å avgjøre om det skal brukes militære ressurser - så fremt det faller inn under alminnelig bistand. Roger Johnsen ved J6 på FOH mener en slik beslutning vil kunne fattes i løpet av noen minutter (Johnsen, 2014, 5.mars).

Analyse av nettverk/overvåkning

Det andre scenarioet som involverte Cyberforsvaret i *CyberDawn* var sikkerhetsmessig overvåkning av driftsnettet til Telenor. Telenor hadde bedt politiet om støtte til å se hva de var utsatt for, finne ut hva denne angriperen faktisk holdt på med og hvordan de kunne normalisere og minimalisere konsekvensene av hendelsen (Landaasen, 2014, 24.februar). Politiet hadde vendt seg til Forsvaret og Cyberforsvaret fikk ordre om å bistå (Tønnesen & Landaasen, 2013b). Hvor realistisk er dette scenarioet? Hva kan Cyberforsvaret bistå med, utover det Telenor selv kan? På den ene siden fremstår det lite sannsynlig at en virksomhet som Telenor har behov for ressurser fra Cyberforsvaret. Telenor er, som redegjort for i kapittel 4, den dominerende

[42] Malware kommer av de engelske ordene Malicious Software og er en fellesbetegnelse på ondsinnet programvare, som eksempel datavirus, ormer og trojanere
[43] Instruksen for bistand til sivile myndigheter foreligger ikke ennå.

leverandøren av ekom-tjenester i Norge, og eksperter på dette feltet. Videre viste dokumentanalysen, i kapittel 5.4, at Telenor har en egen operasjonssentral som kontinuerlig overvåker infrastrukturen og iverksetter tiltak. På den annen side innebar scenarioet i *CyberDawn* at det nettet Telenor bruker til drift og overvåkning ble angrepet. Noen hadde *tuklet* med dataene slik at driftspersonellet ikke kunne ikke stole på det de så på sine skjermer (Landaasen, 2014, 24.februar). Drifts- og støttesystemene overvåker og styrer ekom-nettene og er som tidligere påpekt, i kapittel 4, en kritisk del av infrastrukturen. I en slik situasjon ville Telenor kunne få behov for støtte.

Det er likevel NorCERT som primært skal bistå eier av kritisk infrastruktur ved tilsiktede hendelser, - ikke Cyberforsvaret. På den annen side har ikke NorCERT sensorer i Telenor sin infrastruktur og besitter heller ikke mobile kapasiteter, noe som vil begrense deres mulighet til å bistå i en slik situasjon. Gjennomgangen av ekom-infrastrukturen i kapittel 4.3 viste at Cyberforsvaret på lik linje med Telenor er leverandør av landsdekkende kommunikasjonsinfrastruktur. Telenor og Cyberforsvaret sitter på mye av det samme utstyret, teknologien og kompetansen. Samarbeidsavtalen mellom Cyberforsvaret og Telenor har bidratt til å skape en felles arena for faglig samarbeid, en arena hvor personell fra Cyberforsvaret og Telenor i fellesskap kan se på konkrete problemer, teste nytt utstyr og ha samtrenings-øvelser (Malmedal, 2014, 21.februar). De har derfor kjennskap til hverandres organisasjon og infrastruktur. Dersom infrastrukturen blir infisert vil partene kunne støtte hverandre, sjekke om den andre parten har tilsvarende enheter i sine nett og om disse er infisert. Siden de bruker ulike verktøy, sitter på hver sin del av situasjonsbildet og har ulike kontaktnett er det også mulighet for å utfylle hverandre. Innholdsanalysen, i kapittel 5.5, viste at Cyberforsvaret har mobile ressurser, ressurser som i prinsippet skulle kunne bistå hvem som helst, når som helst og hvor som helst. Bjarte Malmedal, i Cyberforsvaret bekrefter at Cyberforsvaret har bygd opp teknologi og materiell som gjør dem i stand til å koble seg til nærmest alle IP-baserte nettverk (Malmedal, 2014, 21.februar). Forutsatt at BKI får nødvendig støtte, fra en som har god kjennskap til nettet, kan de koble til sitt mobile utstyr, kartlegge og overvåke og bidra med sine vurderinger og råd. På den annen side bidro ikke denne øvelsen til å påvise hva Cyberforsvaret faktisk kan bistå med. Cyberforsvarets målsetting med øvelse *CyberDawn* var først og fremst å øve prosessen for tilkopling av utstyret, herunder skaffe til veie nødvendig informasjon og tilganger, fremfor å utføre overvåkning. Prosessen for tilkopling er omfattende og tidkrevende, og ble løst med direkte kontakt mellom teknisk personell i Telenor og BKI. Det er imidlertid den samme

prosessen som brukes når BKI kobler seg til militære ugradert nettverk, eksempelvis under vinterøvelsen, forklarer Stig Rune Heen som selv er analytiker i BKI (Heen, 2014, 25.februar).

Det er få, om noen, andre nasjonale ressurser enn Cyberforsvarets som har nødvendig verktøy og kompetanse dersom Telenor skulle trenge støtte mener Dyrlie og Landaasen (Dyrlie, 2014, 24.februar; Landaasen, 2014, 24.februar). På den annen side viste dokumentanalysen, i kapittel 5.5, at Cyberforsvarets ressurser er dimensjonert for å beskytte Forsvarets egne systemer, basert på Forsvarets ambisjonsnivå. Cyberforsvaret er ikke dimensjonert for å sikre sivile nettverk. Torbjørn Braastad Tynning i FD2-4 påpeker at det er stor sannsynlighet for at Forsvaret vil ha behov for sine cyberressurser selv dersom nasjonen rammes av en alvorlig cyberhendelse (Tynning, 2014, 28.februar). Som beskrevet i kapittel 4.5 viser erfaring fra moderne krigs- og konfliktsituasjoner at cyberoperasjoner rettet mot sivil IKT-infrastruktur kan være en del av et militært anslag fra en statspart. En alvorlig cyberhendelse vil kunne fordre at Forsvaret øker overvåkningen av egne nettverk og har ressurser tilgjengelig dersom krisen eskalerer. På den annen side viste *22/7-hendelsen* at Forsvaret strekker seg langt for å bistå de sivile samfunn selv i situasjoner hvor det er uklart hva Norge står overfor. Som beskrevet tidligere i dette delkapitlet kan ikke Cyberforsvaret bistå eier av kritisk infrastruktur direkte. Cyberforsvaret vil kunne bistå men det må skje etter anmodning om bistand fra politiet, slik det ble gjort i CyberDawn.

6.4 Koordinering og håndtering

Håndtere innebærer i denne sammenheng å gjennomføre nødvendige tiltak for å minimere konsekvenser og normalisere.

Virksomhetens håndtering, forstås som bruk av de menneskelige, finansielle eller tekniske ressurser virksomheten disponerer. Ansvarsprinsippet innebærer at den virksomhet, myndighet eller etat som har ansvar for et fagområde til daglig også har ansvar for å håndtere ekstraordinære hendelser på området. Kritisk infrastruktur er som påpekt i kapittel 3.1.2 ikke noe unntak fra ansvarsprinsippet. Innholdsanalysen understøttet dette, - den viste at tilbyder er pålagt å opprettholde nødvendig beredskap og tilby sine ekom-nett og tjenester med forsvarlig sikkerhet i hele spekteret fra fred til krig. Ved hendelser i Telenor sin infrastruktur er det de som har ansvaret for å få tjenestene opp og gå igjen. Det er heller ingen andre enn Telenor som *kan* håndtere hendelser i Telenor sitt nett sier Landaasen, Chief Security Intelligence officer i Telenor (Landaasen, 2014, 24.februar). Han får støtte fra Hans Christian Pretorius, Avdelingsdirektør

operativ avdeling i NSM. Pretorius forklarer dette med det han kaller *verdikjedekompetanse* - kjennskap til infrastrukturen og de tjenestene som kjøres. Pretorius sier NorCERT vil kunne gi virksomheten råd, men den angrepne virksomheten må ha mulighet til *selvberging* – verktøy og kunnskap til å kunne iverksette tiltakene som blir anbefalt (Pretorius, 2014, 20.mars). Cyberforsvaret sier det samme. Forutsatt at BKI får nødvendig støtte kan de koble til sitt mobile utstyr, kartlegge og gi sine vurderinger og råd, men de gjør ikke noe utover dette. De ruter ikke om trafikk, filtrerer ikke trafikk, eller stenger ned porter – det må eier av nettverket gjøre selv (Heen, 2014, 25.februar).

Industrispionasjesaken var et angrep mot Telenors forretningsvirksomhet, det rammet ikke andre norske virksomheter og påvirket ikke ekom-tjenestene. Telenor koordinerte og håndterte hendelsen. Dokumentanalysen viste at politiet er gitt ansvar for å håndtere datakriminalitet, men i denne hendelsen ble ikke politiet involvert før etter at Telenor hadde situasjonen under *kontroll* (NSMs sikkerhetskonferanse, 2013).

CyberDawn innebar at flere virksomheter ble rammet samtidig, uten at man innledningsvis kunne påvise noen sammenheng mellom hendelsene. I slike situasjoner er NorCERT gitt i ansvar å *koordinere håndteringen*. NorCERT skal ta ledelsen og koordinere gjenoppretting av normaltilstand på de digitale systemene. Det å *koordinere* innebærer ikke å prioritere bruk av eller styre andres ressurser, men det å være et naturlig kontaktpunkt som raskt får overblikk over kompleksitet og helheten (Pretorius, 2014, 20.mars). Med andre ord å etablere et situasjonsbilde.

På den annen side innebar scenarioet i *CyberDawn* angrep på samfunnskritisk infrastruktur. Situasjonen dreide seg om en pågående alvorlig kriminell handling som hadde potensiale til å ramme liv og helse. Slike situasjoner kommer inn under politiets ansvar. Håndtering ville kunne innebære å måtte ta ned en spesifikk tjeneste eller tjenester i et gitt område, for å isolere problemet. Politiet skal kunne håndtere situasjonen med den makt og myndighet som tilligger politiet. I det utilsiktede utfallet i Sunnmøre, som ble nevnt innledningsvis i oppgaven, satte politiet stab, kalte inn liason fra Telenor, beordret egne folk ut i gatene og instruerte befolkningen i forhold til bruk av ekom-tjenestene (Dagbladet, 2014; Korsnes et al., 2014; Rosbach & Utne, 2014). Politiet viste at de greier å håndtere konsekvensene av utfall i ekom-infrastrukturen, imidlertid indikerte funn i innholdsanalysen at politiet ikke har tilstrekkelig kompetanse og verktøy til å håndtere selve cyberangrepet, - utøve makt i cyberdomenet. Torgeir

Magnussen, politiinspektør i POD, bekrefter dette og sier øvelsen avdekket at politiet ikke har tilstrekkelige ressurser og kompetanse til å utføre det politiarbeidet som vil være nødvendig i en nasjonal krise med utgangspunkt i cyberdomenet (Magnussen, 2014, 11.mars). Rapporten som inngikk i innholdsanalysen, *Politiet i det digitale samfunnet*, ble skrevet i 2012, men Magnussen sier det ikke har skjedd store endringer på dette feltet i ettertid. Noe av forklaringen, kan være Gjørv-kommisjonens[44] ensidige fokus på beredskap i det fysiske domenet. En annen årsak synes å være en overdreven tiltro til hva NSM har hjemmel og kompetanse til å gjøre i forbindelse med en slik krise (Magnussen, 2014, 11.mars).

POD har fått i oppdrag av JD å lage et utkast til nasjonal strategi for bekjempelse av IKT-kriminalitet. Dette utvalget vil se på disse hvilke kapasiteter politiet bør ha i fremtiden (Magnussen, 2014, 11.mars). Som beskrevet i kapittel 3.2.4 er forutsetningen for bistand, i den nye bistandsinstruksen, at politiets ressurser normalt skal være uttømt eller funnet utilstrekkelig for å løse oppdraget. I mangel på ressurser kan politiet, i tråd med bistandsinstruksen, snu seg til Forsvaret. Forsvaret står i en særstilling hva gjelder ansvar for å bekjempe fiendtlige datanettverksoperasjoner og skal ha evne til å gjennomføre mottiltak i form av cyberoperasjoner, herunder CND, CNE og CNA. Hva politiet trenger bistand til avgjør om Cyberforsvaret er en relevant ressurs eller ei.

6.5 Bruk av bistandsinstruksen

Blant de bestemmelser som regulerer bruk av Forsvarets ressurser i fredstid står bistandsinstruksen, som redegjort for i kapittel 3.2, særlig sentralt. Det er imidlertid ikke gitt at instruksen er egnet for bruk ved hendelser i cyberdomenet. Instruksen har så langt ikke vært i bruk i forbindelse med noen reell cyberhendelse, men den ble brukt under øvelsen CyberDawn og i sluttrapporten fremhever politiet viktigheten av å håndtere hendelser i cyberdomenet etter de samme retningslinjer som hendelser i andre domener i (Dyrlie & Landaasen, 2013, s. 9).

Bistandsinstruksens virkeområde er gitt i instruksens generelle bestemmelser. Den omfatter, som beskrevet i kapittel 3.2.4, enhver form for støtte av militært personell og materiell, til politiet, i fred, krise og krig. Støtte fra Cyberforsvarets personell og materiell til analyse av ondsinnet kode og sikkerhetsmessigovervåkning skulle derfor komme inn under instruksens virkeområde. I ettertid har det imidlertid blitt stilt spørsmål ved om dette var bistand til Telenor eller politiet. Å

[44] Rapport fra 22.juli-kommisjonen

overvåke et driftsnett, *til støtte for Telenor*, fremstår i utgangspunktet ikke som politiarbeid. Bistand til politiet dreier seg om bistand til det som er politiets ansvar og politiets oppgaver (Tynning, 2014, 28.februar). På den annen side er Regjeringens viktigste oppgave, som nevnt i kapittel 3.2.3, å forebygge hendelser og kriser. Dersom de likevel oppstår er målet å håndtere de raskt og effektivt ved bruk av samfunnets ressurser. Forsvaret skal primært bistå politiet i politioppgaver, men dersom krisen kommer opp på strategisk nivå vil forsvarsministeren kunne legge sitt bidrag på bordet til lederdepartement eller Kriserådet, og det kan bli besluttet at Forsvaret skal bistå med det de kan. Forsvaret vil kunne hjelpe samfunnet å håndtere en krise, der hvor det er omfattende skader og politiet har en form for skadestedsledelse (Johnsen, 2014, 5.mars).

I CyberDawn ble analyse og overvåkning uansett håndtert som politioppgaver. Politiet sier de ikke ønsker å se på cyberdomenet som noe spesielt, de forholder seg til de oppgavene politiet har – uavhengig av domene. Imidlertid påpekes det at hendelser i cyberdomenet må håndteres noe forskjellig fra hendelser i fysiske domener: «objekteier vil ha en mer sentral rolle i denne type hendelser enn det man ser i den tradisjonelle krisehåndteringen» (Dyrlie & Landaasen, 2013, s. 9). Alle respondentene støtter tilsynelatende at infrastruktureier vil ha en annen rolle dersom hendelsen skjer digitalt enn om det er en fysisk trussel. Men hvor stor rolle skal eier ha og hvordan skal bistanden organiseres? På den ene siden er det naturlig at den som eier og drifter infrastrukturen også må lede og koordinere håndtering i sin infrastruktur i en krise. Det ville være i tråd med ansvar, nærhet og likhetsprinsippene (kapittel 3.1.2). Det er eier av kritisk infrastruktur som kjenner sine systemer best. Det er virksomheten selv som besitter påkrevd kunnskap, verktøy og rutiner for å kunne iverksette nødvendige tiltak i infrastrukturen for å kunne normalisere situasjonen, - eventuelt med den støtten de trenger fra Cyberforsvaret. Cyberforsvaret kunne hatt en egen innsatsleder - en representant i Telenor sin kriseledelse, i en nasjonal cyberkrise. En representant som kunne vært med å diskutere tiltak og som kjente til hva Cyberforsvaret kunne bistå med (Dyrlie, 2014, 24.februar). På den annen side vil krisen få mange ringvirkninger, og liv og helse må gå foran alt annet i krisehåndtering. Det taler for at politiet må styre krisehåndteringen. Eierens fokus vil være på gjenoppretting av systemene mens politiet har fokus på liv og helse. En krise trenger en enhetlig ledelse (Magnussen, 2014, 11.mars). Som presisert i i presentasjonen av de sentrale prinsippene, i kapittel 3.1.2, er det ideelle at beslutninger fattes så lavt som mulig, men likevel på tilstrekkelig høyt nivå til at overordnede målsettinger blir ivaretatt. Det er ingen grunn til at noen andre enn politiet skal ha ledelsen i en sivil krise fordi den har utgangspunkt i det digitale rom (Magnussen, 2014,

11.mars).

Johnsen sier FOH ville krevd stedlig politiledelse i en reell situasjon. Oppdraget til bistandsenheten må være like tydelig som om det var en fysisk trussel. Forsvaret har, som vist i kapittel 3.2.4, en rapporteringsvei, og det er til overordnet politimester. Infrastruktureier har mye kompetanse på sin infrastruktur - men dette dreier seg om maktanvendelse (Johnsen, 2014, 5.mars). På den annen side viser funn gjort i denne studien at politiet ikke har tilstrekkelig kunnskap og erfaring med håndtering av slike hendelser, og bruk av makt i dette domenet. Politiet vil være mer avhengig av kunnskapen og kompetansen til de som eier infrastrukturen enn det man vil være i den fysiske verden. Men like fullt er det altså den politimester som anmoder om bistand som har overordnet ledelse av operasjonen og skal se etter at de midler som tas i bruk ikke overskrider rettslige eller andre grenser satt for politiets virksomhet (Magnussen, 2014, 11.mars). Dette er i tråd med føringene i instruksen som vist i kapittel 3.2.4. Hvordan politimesteren evner å følge opp og lede operasjonen uten en *våpeninstruks* for bruk av cybermakt og med begrenset kunnskap og erfaring gir ikke denne studien noe svar på.

Under *CyberDawn* kategoriserte politiet først overvåkning av Telenor sitt driftsnett som alminnelig bistand. Forsvaret[45] var uenig og definerte det som håndhevelsesbistand. Dersom et stort privat selskap blir utsatt for en tilsiktet hendelse som forstyrrer IKT-systemene deres i veldig stor grad, og politiet ber om bistand fra Forsvaret, så er det meget sannsynlig at det ville bli vurdert som håndhevelsesbistand, sier Johnsen (Johnsen, 2014, 5.mars). Det kan imidlertid være problematisk å ha en bistandsinstruks som *normalt* vil utløse håndhevelsesbistand. Det tar millisekunder fra tastetrykk gjøres på andre siden av kloden til de kan få effekt her. En cyberhendelse kan, som vi så i kapittel 4, eskalere hurtig og gi alvorlige konsekvenser. Respondentene fra Telenor og POD fremhever, i tråd med dette, viktigheten av rask behandling av bistandsanmodningen for at sivil sektor skal få effekt av Forsvaret i den kritiske fasen. Selv prosedyren for alminnelig bistand vil kunne ta for lang tid ved slike hendelser mener Magnussen og indikerer at vi trenger en annen prosedyre for godkjenning av bistand for at samfunnet skal få effekt av bistanden.

Under CyberDawn ble Asker og Bærum politidistrikt kontaktet av Telenor. Politidistriktet kontaktet så Kripos og i fellesskap formulerte de en bistandsanmodning, basert på den beskrivelsen Telenor hadde sendt til dem. Anmodningen ble så håndtert i POD. I en reell

[45] Forsvaret er i dette tilfellet det personellet i Øvelse Hovedstad som spilte FOH

situasjon skulle anmodningen, som beskrevet i kapittel 3.2.4, gått fra ansvarlig politimester via POD, JD, FD, FST og så til FOH, men departementene og FST var ikke med på øvelsen[46]. I *CyberDawn* scenarioet fungerte både telefon og mail, likevel tok det relativt lang tid å håndtere anmodningen. Det er ingen ting som alene tar for lang tid men det er alle delene i sammen, beslutningssløyfen for håndhevelsesbistand er for lang (Landaasen, 2014, 24.februar; Magnussen, 2014, 11.mars). På den annen side legger den nye bistandsinstruksen opp til at bistanden kan forberedes før den er godkjent, - i hastesituasjoner. Samtidig viste erfaringene fra 22/7, som referert i kapittel 3.2.3, at prosessen gikk fort. Under øvelse *CyberDawn* stod allerede Cyberforsvarets biler på Fornebu da øvelsen startet, i en reell situasjon ville de måttet klargjøres og kjøres ut, det ville uansett ta noe tid. Samtidig har det fremkommet tidligere i denne studien at prosessen for tilkopling av sensorer også tar noe tid, deler av dette arbeidet vil kunne utføres parallelt med at anmodningen går sin gang.

6.6 Oppsummering

Denne caseanalysen viste at Cyberforsvaret vil kunne bli anmodet om å bistå gjennom CERT-samarbeidet, koordinert av NorCERT, dersom sivil infrastruktur rammes av et cyberangrep, men det vil være opp til FOH å beslutte om det skal avgis ressurser, - så fremt det faller inn under alminnelig bistand.

Funn gjort i denne studien bekrefter at politiet vil få behov for bistand dersom de skal håndtere en alvorlig cyberhendelse, som i *CyberDawn*. Cyberangrep mot samfunnskritisk ekom-infrastruktur vil kunne fordre støtte fra Forsvaret til analyse. Forsvaret skal, som påpekt i kapittel 3.2.4, ikke ta på seg oppgaver som bør, kan eller skal ivaretas av sivile aktører, men funn gjort i denne studien tilsier at Cyberforsvaret er en av få, kanskje den eneste, nasjonale ressursen som har nødvendig verktøy og kompetanse dersom kritisk ekom-infrastruktur skulle bli rammet av så alvorlig cyberangrep. Studien utelukker ikke at det også kan bli behov for annen type bistand men det er ikke funn i denne studien som gir tilstrekkelig empiri til å si noe om dette.

Cyberforsvaret har kompetanse på analyse av sårbarheter og ondsinnet kode, de besitter mobile kapasiteter og har erfaring med bruk av dem. Disse ressursene skal i henhold til det nye totalforsvarskonseptet kunne stilles til disposisjon for sivile myndigheter. Videre er det funn som

[46] FOH ble «spilt» av personell i Øvelse Hovedstad

tilsier at Forsvaret kanskje ikke vil kunne avgi cyberressurser dersom nasjonen rammes av en alvorlig cyberhendelse. Studien viser at beslutningen om å avgi ressurser til politiet for håndtering av et cyberangrep mot kritisk ekom-infrastrukturen sannsynligvis vil fattes på strategisk nivå. Det er viktig at beslutningen tas raskt for å oppnå ønsket effekt av bistanden. Samtidig er det viktig å sikre seg tilstrekkelig informasjon for å fatte den beste beslutningen. Cyberforsvaret er dimensjonert for å sikre Forsvarets egne systemer, systemer som er avgjørende for Forsvarets operative evne og effektivitet. Samtidig vil håndhevelsesbistand, som nevnt i kapittel 3.2.3, kunne ha politiske implikasjoner. Beslutningsprosessen omfatter mange ledd og vil kunne ta tid dersom det er uklart hva nasjonen står overfor.

7 Avslutning

Temaet for denne studien er sivil-militært samarbeid i en cyberkrise og oppgaven har fokusert på Cyberforsvarets rolle dersom sivil elektronisk kommunikasjonsinfrastruktur (ekom-infrastruktur) rammes av et cyberangrep. Dette kapitlet vil først oppsummere de viktigste funnene fra studien og deretter besvare problemstillingen.

Studiens teoretiske grunnlag

Det nasjonale systemet for krisehåndtering, hvordan kriser prinsipielt håndteres i Norge, og bruken av militære ressurser i fredstid er uavhengig av domenet krisen oppstår i. I Norge er forholdet mellom sivile og militære myndigheter regulert slik at Forsvaret skal ivareta rikets sikkerhet i forhold til eksterne trusler, mens politiet skal sørge for landets indre sikkerhet. Det nye totalforsvarskonseptet innebærer imidlertid gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn. Forsvaret skal bistå det sivile samfunn når viktige samfunnsinteresser og liv og helse står på spill, - med tilgjengelige kapasiteter, kompetanse og ressurser. Dette dreier seg om bistand både til politiet og til det øvrige sivile samfunn. Forsvarets bistand til politiet er regulert gjennom bistandsinstruksen. Det er også under utarbeidelse en egen instruks for Forsvarets bistand til andre sivile myndigheter. Bistandsinstruksen gjelder all form for støtte, herunder både personell og materiell, i fred, krise og krig. Forutsetningen for bistand, er at politiets ressurser skal være uttømt eller funnet utilstrekkelig for å løse oppdraget. Utgangspunktet er fortsatt at sivile kriser håndteres med sivile ressurser, men terskelen for å be om bistand fra Forsvaret skal ha blitt lavere.

Håndteringen av en alvorlig cyberhendelser må forholde seg til systemet for nasjonal krisehåndtering og sivil-militært samarbeid. Hovedregelen er at Forsvaret skal kunne bistå sivile myndigheter ved hendelser i cyberdomenet etter de samme prinsipper og regler som for annen militær bistand til samfunnssikkerhet. Dette systemet definerer i stor grad både *når* og med *hva* Cyberforsvaret vil kunne bistå. Cyberforsvaret kan bistå sivile myndigheter ved et cyberangrep mot ekom-infrastrukturen dersom hendelsen setter viktige samfunnsinteresser, liv og helse på spill, - og under forutsetning av at politiets personell og materielle ressurser ikke strekker til. Cyberforsvaret vil i så fall kunne bistå med all tilgjengelig kompetanse og ressurser. For å besvare problemstillingen måtte studien derfor vise hva som skal til for at et cyberangrep får

konsekvenser for samfunnssikkerheten, hvilke cyberressurser det sivile samfunnet har og hva som skal til for at politiets personell og materiell ikke strekker til. Og sist men ikke minst var det nødvendig å gjøre rede for hvilken kompetanse og ressurser Cyberforsvaret besitter.

Funn

Studien er delt i tre deler. Den første delen omhandler ekom-infrastrukturen og cyberdomenet. Samfunnet vårt er blitt helt avhengig av fungerende ekom-nett og funn i studien viser at det er få, om noen, alternativer som kan erstatte Telenor sin landsdekkende infrastruktur. Samtidig viser studien at det er så tette koblinger mellom Telenor sin infrastruktur og andre systemer at svikt hos Telenor kan få negative følger for funksjonaliteten i andre systemer og slik gi sektorovergripende konsekvenser. Deler av Telenor sin ekom-infrastruktur, herunder stamnett og drifts- og overvåkningssystemene, defineres derfor som kritisk for det norske samfunnet. Studien utelukker ikke på noen måte at også andre ekom-virksomheter besitter samfunnskritisk infrastruktur, men funn viser at Telenor er den dominerende leverandøren av ekom-nett og ekom-tjenester i Norge, og Telenor fikk derfor en sentral plass i oppgaven.
Cyberangrep ble definert å være målrettede angrep med ulike formål, herunder både spionasje og sabotasje. Funn viser at angrepene er vanskelig å definere, fordi angripernes identitet og motiver kan være uklare. Angrepene kan ligge i en gråsone mellom kriminell virksomhet og krigshandlinger, mellom politi og Forsvar sine ansvarsområder. Hovedregelen er likevel at cyberangrep mot sivil infrastruktur ledes av sivile myndigheter inntil Regjeringen beslutter noe annet.

Andre del av studien kartla og diskuterte aktører, ansvar, oppgaver og myndighet i det nasjonale cyberdomenet. Dette ble gjort ved en innholdsanalyse med utgangspunkt i *Nasjonal strategi for informasjonssikkerhet*. Funn viser at ekom-leverandøren er gitt i ansvar å oppdage, analysere og håndtere hendelser i egen infrastruktur, mens operasjonssenteret i NSM, NorCERT, ved hjelp av Varslingssystem for digital infrastruktur (VDI) og nasjonalt samarbeid, skal ha evne til å oppdage og analysere data knyttet til alvorlige hendelser på internett. Det er imidlertid frivillig å være med i VDI samarbeidet, også for de virksomheter som eier samfunnskritisk infrastruktur. Dersom en hendelse rammer flere virksomheter har NorCERT fått i ansvar å koordinere håndteringen av dem. NSM sin myndighet er begrenset til håndhevelse av sikkerhetsloven. Studien viser at politiet er gitt i ansvar å forebygge, avdekke, identifisere og håndtere datakriminalitet. Politiet skal kunne håndtere et pågående cyberangrep mot ekom-infrastrukturen,

ved bruk av den makt og myndighet som tillegger politiet, men funn i innholdsanalysen indikerte at de ikke har tilstrekkelig kunnskap eller verktøy til å utøve makt i dette domenet i dag.

I tredje del av studien studerte jeg to caser som innebar cyberangrep mot sivil infrastruktur, for å se hvordan disse ble håndtert og hvilken bistand det var behov for i disse to casene. De oppgaver hvor det viste seg å være behov for støtte ble så drøftet fortløpende basert på det teoretiske grunnlaget og funn gjort tidligere i studien. Funn viste at politiet hadde behov for bistand til analyse, - etablere situasjonsforståelse, herunder finne ut hva skadevaren har gjort og gjør, hva uvedkommende holder på med og hvorfor, samt gi råd om hvordan en kan minimere konsekvenser og normalisere. Studien utelukker ikke at politiet også vil få behov for annen type bistand men det er ikke funn i denne studien som gir tilstrekkelig empiri til å si noe om dette.

Cyberforsvarets rolle dersom sivil elektronisk kommunikasjonsinfrastruktur rammes av et cyberangrep?

Studien viser at Cyberforsvarets ansvar og oppgaver primært er knyttet til Forsvarets nettverk. Cyberforsvarets ressurser er dimensjonert for å sikre Forsvarets egne systemer, - systemer som er avgjørende for Forsvarets operative evne og effektivitet. Cyberforsvarets rolle er først og fremst å støtte oppunder den nasjonale sikkerheten igjennom å sikre Forsvarets kommunikasjonsinfrastruktur og understøtte Forsvarets operasjoner hjemme og ute. Cyberforsvaret vil samtidig, som Forsvaret for øvrig, ha en bistands rolle dersom viktige samfunnsinteresser, liv og helse står på spill, - men dette er ikke en dimensjonerende oppgave.

Når kan Cyberforsvaret bistå?

Cyberforsvaret *kan* bistå dersom sivil ekom-infrastruktur rammes av et cyberangrep som truer samfunnssikkerheten, - og politiets personell og materielle ressurser ikke strekker til. Studien viser at et cyberangrep mot Telenor sin samfunnskritiske ekom-infrastruktur, herunder stamnett og drifts- og støttesystemer vil ha potensiale til true viktige samfunnsinteresser. Samtidig viser studien at politiet ikke har tilstrekkelige kompetanse og ressurser til å kunne håndtere slike alvorlige cyberhendelser alene. Om Forsvaret kan avgi cyberressursene dersom samfunnskritisk infrastruktur rammes av et cyberangrep vil avhenge av det totale situasjonsbildet.

Hva kan Cyberforsvaret bistå med?

Cyberforsvaret har teknologi, kompetanse og erfaring fra drift og overvåkning av egen landsdekkende ekom-infrastruktur. De har kompetanse på analyse av sårbarheter og ondsinnet kode, besitter mobile kapasiteter og har erfaring med bruk av dem i nettverk de har lite kjennskap til fra før. Cyberforsvaret vil kunne bistå med all tilgjengelig kompetanse og ressurser dersom det besluttes at Forsvaret kan avgi disse ressursene.

Fortsatt *et sårbart samfunn*?

Bistandsanmodningen om å bistå politiet ved håndtering av et cyberangrep mot kritisk ekom-infrastruktur vil måtte behandles på strategisk nivå. Det er viktig å sikre seg tilstrekkelig informasjon for å fatte den beste beslutningen. Samtidig er det viktig at bistandsressursene blir stilt til disposisjon kjapt for at samfunnet skal få ønsket effekt av bistanden. Beslutningsprosessen for håndhevelsesbistand omfatter mange ledd og vil kunne ta tid dersom det er uklart hva nasjonen står overfor. Sårbarhetsutvalget beskrev utfordringene samfunnet stod overfor i 2000 som en voksende og vanskelig definerbar risiko, som følge av bevisste handlinger i en gråsone mellom fred og krig. De argumenterte for at samarbeidet mellom politi og Forsvar måtte bli bedre, fordi politiet hadde begrenset kapasitet til å møte de nye utfordringene samfunnet stod overfor. Funn gjort i denne studien viser at dagens utfordringer i cyberdomenet ennå passer inn i beskrivelsen fra 2000, og at politiet har begrenset med ressurser og kompetanse til å utføre det politiarbeidet som vil være nødvendig i en nasjonal cyberkrise. Sårbarhetsutvalget etterlyste en avklaring på hvordan samvirket mellom politi og militære styrker skulle kunne etableres i det som ble vurdert som særlig kritiske situasjoner uten at det krevde medvirkning fra vedkommende departementer. Utvalget mente det var nødvendig med en raskere beslutningsprosess for å begrense tap, men kunne imidlertid ikke vise til klare eksempler på hvorfor det skulle være behov for å justere instruksverket på området. Scenarioet i CyberDawn innebar en kritisk situasjon for nasjonen vår og scenarioet hevdes å være høyst realistisk, - og vil kunne være det i flere år fremover. Det er gått 14 år siden Willoch leverte rapporten sin, og bistandsinstruksen er endret to ganger siden den gang. Terskelen for å be om bistand fra Forsvaret skal ha blitt lavere med den nye instruksen, men beslutningssløyfen er fortsatt lang. Det er grunn til å spørre om beslutningsprosessen ivaretar cybertrusler i tilstrekkelig grad. Samtidig vil det i dag, som i 2000, være vanskelig å argumentere for at den ikke gjør det så lenge det ikke finnes reelle eksempler å vise til.

Studien har vist at håndtering av et cyberangrep mot sivil kritisk ekom-infrastruktur vil kunne kreve et godt samvirke mellom private og offentlige aktører, politi og Forsvar, men det gjenstår å se om ressursene finner hverandre, i tide, dersom nasjonen rammes av en cyberkrise.

8 Kildeliste

Andersen, R. (2013). *Politiets ansvar og rolle ved krisehåndtering.* Paper presentert på Foredrag for Stabsstudiet 7.6.2013, Forsvarets stabsskole.

Beredskapsloven. (1950). LOV-1950-12-15-7: Lov om særlige rådegjerer under krig, krigsfare og liknende forhold fra http://lovdata.no/dokument/NL/lov/1950-12-15-7?q=beredskapsloven

Bistandsinstruksen. (2012). FOR-2012-06-22-581: Instruks om Forsvarets bistand til politiet. fra http://lovdata.no/dokument/INS/forskrift/2012-06-22-581?q=bistandsin

Bjerga, K. I. (2012). Tettere sivilmilitært samarbeid etter 22.juli. *Trygge samfunn,* (4), 9. Hentet fra http://www.kfb.no/hoved/Hovedside.asp?hovedId=2&Nivaa1Id=16

Bjerga, K. I., & Håkenstad, M. (2012a). Hvem eier krisen? Politi, forsvar og 22.juli. I A. Kjølberg & T. Heier (Red.), *Mellom fred og krig* (s. 54-74). Oslo: Universitetsforlaget.

Bjerga, K. I., & Håkenstad, M. (Red.). (2012b). *Mellom fred og krig - Norsk militær krisehåndtering*. Oslo: Universitetsforlaget.

Bjørgo, T., Burgess, J. P., Kjølle, G. H., Lomell, H. M., Njå, O., Rykkja, L. H., . . . Haugland, R. K. (2013). *Program for samfunnssikkerhet SAMRISK II*. Oslo: Norges Forskningsråd.

Bogen, L., & Mørkestøl, K. (2005). *Håndtering av IKT-kriser - aktører og roller*. (FFI-rapport 2005/03536). Kjeller: Forsvarets forskningsinstitutt (FFI).

Brattekås, K., Hagen, J. M., & Sandrup, T. (2011). *Evaluering av øvingseffekatar - EKOM 2011*. (FFI-rapport 2011/01905). Kjeller: Forsvarets forskningsinstitutt (FFI).

Breivik, T., & Kjenseth, K. (2014). Representantforslag fra stortingsrepresentantene Terje Breivik og Kjetil Kjenseth om etablering av en nasjonal bredbåndsplan. *Dokument 8:19 S (2013-2014)*. Hentet fra https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Representantforslag/2013-2014/dok8-201314-019/1/#a1.2

Broadnet. (2014). Om oss. Hentet 14.3, 2014, fra www.broadnet.no/no/om_oss/

Cresswell, J. W. (2013). *Research Design*. California: SAGE Publications.

Dagbladet. (2014). Nødnettet gikk ned, politiet måtte ut i gatene. Hentet 18.3.2014, fra http://www.dagbladet.no/2014/03/06/nyheter/politi/brannvesen/nodtelefon/32165796/

DSB. (2012). Samfunnets sårbarhet overfor bortfall av elektronisk kommunikasjon. Tønsberg: DSB.

DSB. (2013a). Nasjonalt risikobilde *Katastrofer som kan ramme det norske samfunnet*. Tønsberg: DSB.

DSB. (2013b). Teknologiskiftet i Telenors infrastruktur. Tønsberg: DSB.

Dyndal, G. L. (Red.). (2010). *Strategisk ledelse i krise og krig*. Bergen: Fagbokforlaget.

Dyndal, G. L., & Simonsen, S. (2013). Krisehåndtering. Sentralisert over-departemental ledelse eller desentalisert sektoransvar? Hentet 24.1.2014, fra http://www.minervanett.no/krisehandtering/

Dyrlie, R., & Landaasen, S. J. (2013). Øvelse CyberDawn 2013 Sluttrapport. Fornebu: Telenor

E-tjenesten, NSM, & PST. (2013). Samordnet vurdering fra E-tjenesten, NSM og PST. Hentet fra http://www.pst.no/media/59018/Trusler_og_sarbarheter_2013.pdf

Ekomloven. (2003). LOV-2003-07-04-83: Lov om elektronisk kommunikasjon. fra http://lovdata.no/dokument/NL/lov/2003-07-04-83?q=ekomloven

Etterretningstjenesten. (2014). Etterretningstjenestens vurdering FOKUS 2014. Hentet fra http://m.forsvaret.no/om-forsvaret/fakta-om-forsvaret/publikasjoner/Documents/Fokus-2014.pdf

Fagerland, S., Kråkvik, M., & Camp, J. (2013). Operation Hangover Unveiling an Indian Cyberattack Infrastructure. Hentet 4.2.2014

fra http://normanshark.com/hangoverreport/

Forskningsrådet. (2013). *Om Programmet*. Hentet 14.3.2014, fra http://www.forskningsradet.no/prognett-samrisk/Om_programmet/1228296552890

Forsvaret. (2013). *Manual i krigens folkerett*. Oslo: Forsvarssjefen.

Forsvarsdepartementet. (2009). Forskrift om objektsikkerhet - Høringsbrev. fra http://lovdata.no/dokument/SF/forskrift/2010-10-22-1362?q=objektsikkerhet*

Forsvarsdepartementet. (2012). *Cyber og folkeretten*. Oslo: Forsvarsdepartementet.

Forsvarsdepartementet. (2013). Høringsnotat - Om lov om Forsvarets ansvar for å avverge luftbårne terroranslag og Forsvarets bistand til politiet. Hentet 10.3.2014, fra http://www.regjeringen.no/nb/dokumentarkiv/stoltenberg-ii/fd/Nyheter-og-pressemeldinger/pressemeldinger/2013/forsvarets-bistand-til-politiet-og-om-fo.html?id=732660

Forsvarsdepartementet. (2014). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner "FDs cyberretningslinjer"*. Hentet fra http://www.regjeringen.no/nb/dep/fd/aktuelt/nyheter/2014/Nye-retningslinjer-for-informasjonssikkerhet-og-cyberoperasjoner-i-forsvarssektoren-.html?id=753949.

Forsvarsstaben. (2014). *Forsvarets fellesoperative doktrine utkast v. 2.1.1 april 2014*. Oslo: Forsvarets stabsskole.

Fridheim, H., & Hagen, J. (2007). *Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer - sluttrapport*. (FFI-rapport 2007/01204). Kjeller: Forsvarets forskningsinstitutt (FFI).

Gabrielsen, C. K. (2013). Høyre frykter "digitalt 22.juli". Hentet 17.10. 2013, fra http://www.tv2.no/nyheter/politisk/hoeyre-frykter-digitalt-22-juli-3993710.html

Grunnloven. (1814). LOV-1814-05-17: Kongeriget Norges Grundlov, given i Rigsforsamlingen paa Eidsvold den 17de Mai 1814. fra http://lovdata.no/dokument/NL/lov/1814-05-17?q=grunnloven

Hagen, J. M., Fridheim, H., & Grunnan, T. (2010). *(U) Sikkerheitspolitisk krise, nasjonal kriseleiing og sivilmilitært samarbeid [Sladdet versjon]*. (FFI-rapport 2010/01009). Kjeller: Forsvarets forskningsinstitutt (FFI).

Hamnes, L. (2012). Norsk tillitskultur passer dårlig i cyberspace. Hentet 5.5.2014, fra http://www.tu.no/it/2012/07/03/norsk-tillitskultur-passer-darlig-i-cyberspace

Heieraas, B. O. (2010). Bajonetter til innvortes bruk: sivil-militære relasjoner i historisk perspektiv. I G. L. Dyndal (Red.), *Strategisk ledelse i krise og krig* (s. 91-107). Bergen: Fagbokforlaget.

Hillestad, L. K., & Sandli, E. (2013). Det er ikke et spørsmål *om* vi blir utsatt for et sånt angrep, der et spørsmål om *når*. *Null CRTL*. Hentet 2.4, 2014, fra http://www.dagbladet.no/2013/10/18/nyheter/inennriks/null_ctrl/data_og_teknologi/datasikkerhet/29826413/

Høyre-Frp-Regjeringen. (2013). Politisk plattform for en regjering utgått av Høyre og Fremskrittspartiet. Hentet 15.10.2013, fra http://www.hoyre.no/filestore/Filer/Politikkdokumenter/plattform.pdf

Innst. 388 S (2011-2012). (2012). *Innstilling fra utenriks- og forsvarskomiteen om Et forsvar for vår tid*. Oslo.

Irgens, M. (2013). Cybersikkerhet er ikke informasjonssikkerhet er ikke IKT-sikkerhet. Hentet 26.3.2014, fra http://mortenirgens.com/?p=769

IVB LTP (2013-2016). (2012). *Iverksettingsbrev til forsvarssektoren for langtidsperioden 2013-2016, "Et forsvar for vår tid"*. Oslo: Forsvarsdepartementet.

Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. Kristiansand: Høyskoleforlaget AS.

Johansen, P. A. (2013). Spionerte på Telenor-sjefer, tømte all e-post og datafiler. Hentet 19.2.2014, fra http://www.aftenposten.no/nyheter/Spionerte-pa-Telenor-sjefer_-tomte-all-e-post-og-datafiler-7149813.html

Johnsen, R. (2013). Cyberkrigføring og Forsvarets operative evne. *Internasjonal Politikk, 71*(2), 241-251.

Johnsen, S. T., & Kveberg, T. (2014). *Cyberdomenet, cybermakt og norske interesser*. (FFI-rapport 2013/02712). Kjeller: Forsvarets forskningsinstitutt (FFI)

Karlsen, S. G. (2013). Dagbladet stakk av med gjev datapris. Hentet 10.3.2014, fra http://www.dagbladet.no/2013/11/27/kultur/dagbladet/gullpil/pris/datasikkerhet/30552414/

Kirknes, L. M. (2013). Cyberforsvaret vil ha cyberstrategi. *Computerworld*. Hentet 10.3.2014, fra http://www.idg.no/computerworld/article277398.ece

Knudsen, E. (2013). Ny, stor skandale avslørt av Snowden-dokumenter. Hentet 10.3.2014, fra http://www.hardware.no/artikler/britiske-nsa-hacket-belgisk-telegigant/137709

Korsnes, M. K., Roaldseth, S. L., & Berg, F. (2014). Politiet har sendt etterforskere til stedet hvor strømbruddet skjedde. Hentet 18.3.2014, fra http://www.nrk.no/mr/pressekonferanse-om-telekollaps-1.11587154

Kveberg, T., & Johnsen, S. T. (2013). *Cyberdomenet, cybermakt og norske interesser*. (FFI-rapport 2013/02712). Kjeller: Forsvarets forskningsinstitutt (FFI).

Løngø, H.-I., & Sandvik, K. B. (2013). Cyberspace og sikkerhet. *Internasjonal Politikk, 71*(2), 221-228.

Meld. St. nr. 21 (2012-2013). (2013). *Terrorberedskap*. Oslo: Justis- og beredskapdepartementet.

Meld. St. nr. 29 (2011-2012). (2012). *Samfunnssikkerhet*. Oslo: Justis- og beredskapsdepartementet.

NATO. (2009). *Allied Joint Doctrine, AJP-3.10*. Brussel: NATO.

NOU 2000: 24. (2000). *Et sårbart samfunn*. Oslo: Statens forvaltningstjeneste Informasjonsforvaltning.

NOU 2006: 6. (2006). *Når sikkerheten er viktigst: beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Oslo: Departementenes servicesenter.

NOU 2012: 14. (2012). *Rapport fra 22. juli-kommisjonen*. Oslo: Departementenes servicesenter Informasjonsforvaltning.

NSM. Partnere & Medlemmer. Hentet 5.5.2014, fra https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/NorCERT-medlemmer/

NSM. (2014a). Sikkerhetstilstanden 2014. 5.5.2014, fra https://www.nsm.stat.no/Documents/Risikovurdering/NSM_Rapportomsikkerhet_digital.pdf

NSM. (2014b). Årsrapport 2013. 5.5.2014, fra https://www.nsm.stat.no/Aktuelt/Nytt-fra-NSM/Arsrapport-2013-og-sikkerhetstilstanden-2014/

NSMs sikkerhetskonferanse. (2013). Rune Dyrlie, Sikkerhetsdirektør i Telenor Norge [videoklipp]. Hentet 6.1, 2014, fra http://nsm.stargatemedia.no/nsm-sikkerhetskonferanse/videos/handtering-av-dataangrep-slik-gjorde-vi-det/

NUPI. (2011). Nye sikkerhetstrusler: cyberangrep. Hvordan forsvarer vi oss? Hentet 15.10.2013, fra http://hvorhenderdet.nupi.no/Artikler/2010-2011/Nye-sikkerhetstrusler-cyberangrep/(part)/6

Nystuen, K. O., & Fridheim, H. (2007). *Sikkerhet og sårbarhet i elektroniske samfunnsinfrastrukturer - refleksjoner rundt regulering og tiltak*. (FFI-rapport 2007/00941). Kjeller: Forsvarets forskningsinstitutt (FFI).

Næringslivets sikkerhetsråd. (2012). Mørketallsundersøkelsen - Informasjonssikkerhet og datakriminalitet. Hentet 13.10.2013, fra http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/moerketall_2012.pdf

Politiet. (2011). *Politiets beredskapssystem del 1 (PBS 1)* Oslo: Politidirektoratet.

Post- og teletilsynet. (2012a). *Foreløpige erfaringer og forslag til tiltak etter ekstremværet Dagmar*. Lillesand: Post- og teletilsynet.

Post- og teletilsynet. (2012b). *Sårbarhetsanalyse av mobilnettene i Norge*. Lillesand: Post- og teletilsynet.

Post- og teletilsynet. (2013). *Det norske markedet for elektroniske kommunikasjonstjenester 1. halvår 2013*. Lillesand: Post- og teletilsynet.

Post- og teletilsynet. (2014). Om Post- og teletilsynet (PT). Hentet 19.12.2013, fra www.npt.no/om-pt

Prop. 1 S (2007-2008). (2007). *Proposisjon til Stortinget (forslag til stortingsvedtak)*. Oslo: Departementenes servicesenter Hentet fra http://www.regjeringen.no/nb/dep/fd/dok/regpubl/stprp/2007-2008/stprp-nr-1-2007-2008-.html?id=484147.

Prop. 1 S (2013-2014). *Proposisjon til Stortinget (forslag til stortingsvedtak)*. Oslo: Departementenes servicesenter.

Prop. 73 S (2011-2012). *Et forsvar for vår tid*. Oslo: Departementenes servicesenter.

Ravnaas, P. (2013). Cyber-ambulansen - Sorte biler rykker ut for å beskytte Forsvaret mot ondsinnede koder eller virus. Hentet 3.3.2014, fra http://www.fofo.no/Cyber-ambulansen.b7C_w7LQYJ.ips

Regjeringen. (2012a). *Nasjonal strategi for informasjonssikkerhet*. Oslo: FAD Hentet fra http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Nasjonal_strategi_infosikkerhet.pdf.

Regjeringen. (2012b). *Nasjonal strategi for informasjonssikkerhet - Handlingsplan*. Oslo: FAD Hentet fra http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Nasjonal_strategi_infosikkerhet.pdf.

Regjeringen. (2013a). Forsvarets bistand til politiet og Forsvarets ansvar for å avverge luftbårne terroranslag. Hentet 5.5, 2014, fra http://www.regjeringen.no/nb/dokumentarkiv/stoltenberg-ii/fd/Nyheter-og-pressemeldinger/pressemeldinger/2013/forsvarets-bistand-til-politiet-og-om-fo.html?id=732660

Regjeringen. (2013b). Klargjering om bistandsinstruksen og Grunnloven §99. Hentet 5.5, 2014, fra http://www.regjeringen.no/nb/dokumentarkiv/stoltenberg-ii/fd/Nyheter-og-pressemeldinger/Nyheter/2013/klargjering-om-bistandsinstruksen-og-gru.html?id=714564

Ringdal, K. (2013) *Enhet og mangfold*. Oslo: Fagbokforlaget.

Rosbach, M., & Utne, T. (2014). Omfattende feil med telefon og internett. Hentet 18.3.2014, fra http://www.smp.no/nyheter/article9268475.ece

Rui, J. P. (2011). Politiets behov for støtte fra Forsvaret: Lovgivning er nødvendig. *Lov og rett, vol. 50, 8, 2011*, s 445-446.

Sandvik, K. B. (2013). Cyberkrig og internasjonal rett. *Internasjonal Politikk, 71*(2), s 252-263.

Senel, E., & Hattrem, E. (2014). Slik skal Lærdal få mobildekning igjen. Hentet 31.1.2014, fra http://www.nrk.no/norge/mobile-basestasjoner-pa-plass-1.11480308

Sikkerhetsloven. (1998). LOV-1998-03-20-10: Lov om forebyggende sikkerhetstjeneste fra http://lovdata.no/dokument/NL/lov/1998-03-20-10

Spiegel Online International. (2013). Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm. Hentet 10.3.2014, fra http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

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

St. meld nr. 37 (2004-2005). (2005). *Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering*. Oslo: Justis- politidepartementet.

St. meld nr. 39 (2003-2004). (2004). *Samfunnssikkerhet og sivilt-militært samarbeid*. Oslo: Justis- politidepartementet.

St. meld. nr. 17 (2001-2002). (2002). *Samfunnssikkerhet - Veien til et mindre sårbart samfunn*. Oslo: Justis- og politidepartementet.

St.prp. nr 1 (2002-2003). *For budsjetterminen 2003*. Oslo: Hentet fra http://www.regjeringen.no/nb/dep/fd/dok/regpubl/stprp/20022003/stprp-nr-1-2002-2003-.html?id=295513.

Stenseth, A. (2003). *Nettverk: en beretning om Forsvarets tele- og datatjeneste 1953-2001*. Bærum: FLO/IKT.

Storruste, B., & Magnussen, T. (2012). *Politiet i det digitale samfunnet - en arbeidsgrupperapport om: elektroniske spor, IKT-kriminalitet og politiarbeid på internett*. Oslo: Politidirektoratet.

Sundseth, R. (2013). Cyberoperasjoner - Utfordringer i Cyber. Hentet 20.1.2014, fra http://www.oslomilsamfund.no/oms_arkiv/2013/2013-02-18-Sundseth.html

Sveinbjørnsson, S. (2012). Hver tredje ISP bryr seg ikke. Hentet 3.2.2014, fra http://www.digi.no/895023/hver-tredje-isp-bryr-seg-ikke

Svendsen, B. (2014). Digital robusthet - mer enn fiberkabler. Hentet 14.3.2014, fra http://e24.no/kommentarer/kommentar-digital-robusthet-mer-enn-fiberkabler/22762465

Søreide, I. E. (2014). Åpning av sikkerhetskonferansen - Part 1 [videoklipp]. fra https://www.nsm.stat.no

Telenor SOC. (2014). TSOC-nyhetsbrev - daglige oppdataeringer fra TSOC. 5.5.2014, fra http://telenorsoc.blogspot.no/

Tønnesen, K. V., & Landaasen, S. J. (Writers). (2013a). Cyberkriser må koordineres på tvers [USB]. In Telenor Norge (Producer): Telenor Norge.

Tønnesen, K. V., & Landaasen, S. J. (2013b). Cyberkriser må koordineres på tvers [videoklipp]. 2.4.2014, fra https://www.youtube.com/watch?v=OW3pMscYPJ4

Utheim, E. B. (2013). Eksplosjon i antall norske data-angrep. Hentet 10.3.2014, fra http://e24.no/digital/eksplosjon-i-antall-norske-data-angrep/20374421

Windvik, R., Thuv, A., Nystuen, K. O., & Sivertsen, T. (2007). *Sårbarheter i Internett*. (FFI-rapport 2007/00903). Kjeller: Forsvarets forskningsinstitutt (FFI).

Østby, L. (2014). PST frykter kinesisk 4G-spionasje. Hentet 27.2.2014, fra http://www.tv2.no/a/5279820

Vedlegg 1 Respondentoversikt

Respondent: Bjarte Malmedal
Samtale (dato, tid og sted): 21.februar 2014, kl. 12:00-13:30, Cyberforsvaret, Jørstadmoen
Stilling: Oblt. CST Plan og utvikling, Cyberforsvaret

Respondent: Stig Rune Heen
Samtale (dato, tid og sted): 25.februar 2014, kl. 13:00-13:40, telefonmøte
Stilling: Maj. CTO BKI CND, Cyberforsvaret
Deltok som analytiker på CyberDawn.

Respondent: Rune Dyrlie
Samtale (dato, tid og sted): 24.februar 2014, kl. 11:30-13:30, Telenor, Fornebu
Stilling: Chief Security Officer Technology, Telenor
Håndterte Industrispionasjesaken i 2013

Respondent: Storm Jarl Landaasen
Samtale (dato, tid og sted): 24.februar 2014, kl. 13:30-15:30, Telenor, Fornebu
Stilling: Chief Security Intelligence officer, Telenor
Var øvingsleder for CyberDawn 2013

Respondent: Torbjørn Braastad Tynning
Samtale (dato, tid og sted): 28.februar 2014, kl. 9:00-10:00, FD, Akershus festning
Stilling: Seniorrådgiver FD 2-4, Forsvarsdepartementet

Respondent: Roger Johnsen
Samtale (dato, tid og sted): 5.mars 2014, kl. 18:00-19:00, Oslo
Stilling: Oblt. OPS J6 Plan-Sys, Forsvarets operative hovedkvarter
Johnsen har tidligere vært sjef for Forsvarets senter for beskyttelse av kritisk infrastruktur (BKI) og skolesjef ved Forsvarets ingeniørhøgskole

Respondent: Torgeir Magnussen

Samtale (dato, tid og sted): 11.mars 2014, kl. 12:00-13:00, POD, Hammersborggata

Stilling: Politiinspektør

Spilte POD under CyberDawn 2013

Respondent: Hans Christian Pretorius

Samtale (dato, tid og sted): 20.mars 2014, kl. 10:00-11:30, NSM, Bryn

Stilling: Avdelingsdirektør operativ avdeling.

Vedlegg 2 Informasjonsskriv til respondent

Forespørsel om deltakelse i forskningsprosjektet

"Sivilmilitært samarbeid i en cyberkrise"

Bakgrunn og formål

Jeg gjennomfører for tiden en masterstudie på Forsvarets Høgskole. Temaet for oppgaven jeg skriver er: Sivilmilitært samarbeid i en cyberkrise.

Norge og norske interesser utsettes daglig for cyberangrep. Angrepene blir stadig mer avanserte og har potensiale for å kunne slå ut kritisk infrastruktur og stoppe kritiske samfunnsfunksjoner. Vår evne til å forebygge, begrense og håndtere hendelser i cyberdomenet er derfor av avgjørende betydning for samfunnssikkerheten.

Hensikten med denne oppgaven er å se på Forsvarets bistand til sivile myndigheter dersom kritisk infrastruktur rammes av et cyberangrep. Hva kan Cyberforsvaret bistå med, hvem kan de bistå og er bistandsinstruksen egnet til dette formål?

Hva innebærer deltakelse i studien?

Det legges opp til et delvis strukturert intervju. Du vil få tilsendt mine spørsmål i forkant av intervjuet, men du står fri til å beskrive også andre forhold som har betydning for problemstillingen. Jeg vil ta opp samtalen (taleopptak på mobiltelefon).

Hva skjer med informasjonen om deg?

Det er kun jeg og veileder som vil ha tilgang til datamaterialet.
Intervjuobjekter kommer til å gjenkjennes med navn og/eller funksjon/stilling i oppgaven når den publiseres.
Prosjektet skal avsluttes 1.juli 2014. Alt intervjumateriale vil da innen rimelig tid anonymiseres.
Behandlingen av personopplysninger vil være i samsvar med retningslinjene ved Forsvarets høgskole.

Frivillig deltakelse

Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Dersom du trekker deg, vil alle opplysninger om deg bli anonymisert. Dersom du er villig til å la deg intervjue, ber jeg deg om å gi meg en tilbakemelding på e-post. Jeg tar deretter kontakt for å avtale tidspunkt for intervjuet.

Undersøkelsen er finansiert av Forsvarets Høgskole.
Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste AS.

Hvis det er noe du lurer på kan du ringe meg på 90 83 44 11, eller sende en e-post til igustavsen@fhs.mil.no.
Du kan også kontakte min veileder Gert Lage Dyndal på telefon 23 09 57 80, eller epost gdyndal@fhs.mil.no.

Mvh
Ingunn Harildstad Gustavsen
Oing/Forsvarets logistikkorganisasjon - Divisjon for IKT-kapasiteter

Samtykke til deltakelse i studien

Samtykke kan evt meddeles på mail.

Jeg har lest og forstått informasjonen over og gir mitt samtykke til å delta i intervjuet

_____ _____

Sted og dato Signatur