Forsvarets høgskole

våren 2015

Masteroppgave

Cybersikkerhet i væpnet konflikt

Er norsk organisering optimal?

Nils Gaute Prestmo

Abstract

The theme in this study is cybersecurity in an armed conflict. Cybersecurity is in peacetime handled by a large set of players both in public and private sector. The total defense concept gives some regulations on civil military cooperation. In peacetime the Armed Forces are to support civil administration. In war this is turned around, and the Armed Forces will be supported.

In case of armed conflict it is likely to face cyber-attacks such as sabotage and espionage in addition to regular forces. In addition the nation will face cyberattacks integrated info information operation. This is in line with reports from Estonia to Ukraine. The data so far doesn't indicate that cyberattack will be used alone in an armed conflict. On certain conditions cyber-attacks may give the right to self-defense according to UN charter article 51.

This thesis shows that in case of an armed conflict, the Norwegian Armed Forces will face some problems when managing national cyber security. The task covering cyber defense is restricted to Armed Forces systems alone. This task combined with a large set of national players that have to be exercised together in order to have a quick response to hostile acts. The best preparation for cyber defense is by establishing a network for information sharing in both public and private sector.

Sammendrag

Temaet for denne oppgave er cybersikkerhet i væpnet konflikt. I Norge er ivaretagelse av cybersikkerhet og beskyttelse mot cyberangrep fordelt mellom ulike aktører i offentlig og privat sektor. Oppgaven drøfter hva som er et væpnet cyberangrep og om norsk organisering er optimal for å takle et slikt.

Oppgaven er løst som en kvalitativ studie. I tillegg til litteraturstudie ble det gjennomført en tversektoriell workshop. Det er lite tilgjengelig litteratur på bruk av cyberangrep i væpnet konflikt. Til oppgaven bel det laget en casestudie som satte ulike cyberangrep inn i rammen på et strategisk overfall av Finnmark.

Oppgaven ser på teori om cybersikkerhet og om organisering for krisehåndtering. Cyberdomenet er relativt nytt, og det er lite teori som beskriver potensialet til cyberangrep. Det er videre viktig å ha evne til å gjøre defensive tiltak i domenet gjennom å ha gode hjelpemiddel. Informasjonsdeling er viktig for å øke robustheten. Flest mulig må ha mulighet til å forebygge cyberangrep. Krisehåndtering i offentlig sektor er hendelsesbasert. Episoder og kriser kategoriseres, og organisering av kriseledelse velges ut fra dette. Totalforsvarskonseptet beskriver at Forsvaret støttes av det sivile samfunn ved en væpnet konflikt. Totalforsvaret danner rammen for å etablere samarbeid både i stand av koordineringsfora og arenaer for samarbeid.

Analysen av casestudie viser at Forsvaret vil møte store utfordringer knyttet til cybersikkerhet. I en væpnet konflikt vil det være cyberangrep som sabotasje og spionasje. I tillegg vil det være cyberangrep som del av informasjonsoperasjoner mot befolkning og politikere. Forsvaret har en stående kommandostruktur og må ta ansvar ved et militært angrep mot Norge. Oppdraget knyttet til cybersikkerhet er begrenset til egne systemer i fred og væpnet konflikt. Dette påvirker muligheten til å organisere og lede cybersikkerhet. I tillegg mangler Norge er cybersikkerhetsstrategi. Denne skal blant annet beskrive hvordan sivilt-militært samarbeid skal utvikles, krisehåndtering, beskyttelse av kritisk infrastruktur og informasjonsdeling. Et alvorlig cyberangrep kan være et væpnet cyberangrep og gi rett til selvforsvar etter FN paktens artikkel 51.

Forord

Det er ikke alle forunt å få muligheten til betalt utdanning i voksen alder ved Forsvarets Høgskole. Tildeling av forsvarsmedaljen etter 25 års tjeneste underveis i masterstudiet gjør at en reflekterer litt over dette. Denne oppgaven setter sluttstrek for profesjonsutdanningen som Forsvaret gir mulighet til for sine militært ansatte. Fordypningen som denne oppgaven har gitt mulighet til, gjør det mulig å gjøre en bedre jobb for min arbeidsgiver i en verden som har tatt store teknologiske sprang gjennom de siste tiårene. Cyberforsvaret som jeg tilhører, ble offisielt opprettet så sent som i høsten 2012, er noen annet enn Hærens samband. En troppeart jeg har vært en del av alle disse 25 årene.

Spesiell takk til min veileder og bi-veileder. Hovedveileder Professor Janne Haaland Matlary har vært til uvurderlig hjelp både til å holde oppgavene på et overordnet faglig nivå. Hun har vært en særdeles god dialogpartner, og hun har bidratt til å knytte cyberdomenet til sikkerhetspolitiske utfordringer og til å holde fokus på den røde tråden. Professor Bernard Hämmerli har som bi-veileder vært en særdeles nyttig samtalepartner i forståelsen av utfordringer innenfor cyberdomenet. Samarbeidet med bi-veileder ga mulighet for et større faglig miljø og dialog med internasjonale eksperter. Gode kollegaer i Forsvaret har indirekte bidratt gjennom gode diskusjoner på deler av det som tas opp i oppgaven.

Når som oppgaven er levert er det mulig som familiefar å komme tilbake til hjemmet både fysisk og psykisk. Etter et år som hektisk ukependler og mentalt fraværende så kan det nå bli rom for å være mer tilstede i hverdagen. Spesielt takk også til Nora som denne gangen har holdt seg unna medisinske utfordringer mens pappa har vært på skole.

Lillehammer 22. mai 2015
Nils Gaute Prestmo

Innhold

1 Innledning

Media bruker 'Cyber Pearl Harbor' og 'Cyber 9/11' som dystre beskrivelser på fremtidige cyberangrep. Cyberangrep har vært en del av mellomstatlige konflikter det siste ti-året. Estland i 2007, Georgia i 2008 og Ukraina fra februar 2014. Fra Ukraina har det siden den russiske annekteringen av Krim-halvøya blitt rapportert om bruk av ulike former for cyberangrep (Lee, 2014).

NATOs strategiske konsept fra 2010 satte fokus på cyberangrep. Det strategiske konseptet inkluderte cyberangrep som en av de såkalt nye truslene (Meld. St. 24 (2010-2011), 2011, s. 8), sammen med blant annet terror og spredning av masseødeleggelsesvåpen.

I Norge er ivaretagelse av cybersikkerhet og beskyttelse mot cyberangrep fordelt mellom ulike aktører i offentlig og privat sektor. På militær side er den formelle etableringen av Cyberforsvaret i 2012 et politisk signal om at cyberdomenet og cybertrusselen har militær betydning for Norge. I Prop. 73S *Et forsvar for vår tid* er avdeling for beskyttelse av kritisk infrastruktur (BKI) listet som en av Cyberforsvarets kapasiteter. Avdelingen har som oppdrag å overvåke og detektere cyberangrep mot Forsvarets systemer. Den skal også inneha analysekapasitet, og evne til å sende ut mindre enheter. I tillegg skal den kunne bidra med rådgivning og liaisonering ved angrep på norsk infrastruktur ute og hjemme (Prop. 73 S (2011-2012), 2012, s. 103). Som sivilt element i offentlig sektor har NorCERT[1] rollen som nasjonalt Computer Emergency Reaction Team (CERT). NorCERT er en del av Nasjonal Sikkerhetsmyndighet. I offentlig sektor finnes også flere andre CERT miljøer. I privat sektor er det tilsvarende miljøer, og blant annet Telenor har en egen CERT. Noen bedrifter, som blant annet Statoil[2], har etablert Computer Security Incident Reaction Team (CSIRT).

Til tross for de organisatoriske tiltakene er trusselen stadig økende og påtrengene. Sjefene for både Etterretningstjenesten og Politiets sikkerhetstjeneste beskriver i 2015 at Russland og Kina driver avanserte etterretningsoperasjoner mot norske interesser (Etterretningstjenesten, 2015; Politiets sikkerhetstjeneste, 2015).

Forsvarssjefens tale i Oslo Militære Samfund (OMS) den 12. januar 2015(Admiral Haakon Bruun-Hanssen, 2015):

Trusler og angrep i Cyberdomenet er en stadig større utfordring. Vi har daglige inntrengingsforsøk i våre systemer. Aktørene er både statlige og enkeltindivider/grupper.

[1] Hentet fra http://nsm.stat.no/tjenester/handtering, den 4. mai 2015

Vellykkede angrep på nasjonens vitale systemer kan være katastrofale. Vår evne til å sikre beredskapssystemene for fortsatt å fungere etter et cyberangrep blir stadig viktigere. Dette gjelder ikke bare for Forsvaret, men for alle sektorer og næringslivet.

Med konflikter nærmere norske grenser enn på mange år er det på ny fokus på nasjonal sikkerhet, beredskap og totalforsvarskonseptet. Den gjensidige støtten og samordningen mellom Forsvaret og det sivile samfunn er bærebjelken i totalforsvarskonseptet. I gjeldende strategisk konsept for Forsvaret er det beskrevet at totalforsvarskonseptet skal bidra til å effektivisere ressursinnsatsen på nasjonalt nivå langs hele krisespekteret. Etter den kalde krigens slutt er konseptet modernisert. Støtte fra Forsvaret til det sivile samfunn baseres på tilgjengelige kapasiteter. I en væpnet konflikt vil omfattende og pliktmessig sivil støtte til Forsvaret kreve at beredskapslovgivningen kan anvendes (Forsvarsdepartementet, 2009, s. 71-72).

På Forsvarets forskingsinstitutt (FFI) sitt seminar november 2014[3] ble det fra salen kommentert at med fokus på nasjonale operasjoner ville Forsvaret igjen stille krav til det sivile samfunnet.

1.1 Problemstilling

I denne oppgaven vil jeg fokusere på krisehåndtering av cybersikkerhet ved en væpnet konflikt. Ved alle kriser skal de nasjonale prinsipper for krisehåndtering benyttes. Disse er ansvar, nærhet, likhet og samvirke. Samvirke ble innført som prinsipp sommeren 2012 (Meld. St. 29 (2011-2012), 2012). Den siste større erfaring med krisehåndtering for offentlig sektor er terrorangrepet 22. juli 2011. Rapporten om terrorangrepet viser at offentlig krisehåndtering fortsatt kan forbedres (NOU 2012:14, 2012)

Et væpnet angrep på Norge bringer nasjonen inn i en væpnet konflikt mot en eller flere andre aktører. En slik alvorlig krise utfordrer offentlig sektor og Forsvaret på krisehåndtering. Prinsippene for krisehåndtering er gjeldende, og samvirke gjelder også med et utall aktører i sivil sektor. Et militært angrep vil ha cyberangrep som et av flere virkemidler. Forsvaret har noe erfaring fra væpnet konflikt gjennom internasjonale operasjoner de siste tiårene. I disse konfliktene har det vært få eller ingen cyberangrep. Konfliktene i Georgia og Ukraina viser med tydelighet at cyberangrep er en del av virkemidlene som benyttes. Cyberangrepene gjennomføres av militærmakten eller av sympatisører, og er med på å skape forutsetning for å få overtaket i konflikten. Cyberangrepene har endret seg fra Estland i 2007 til Ukraina i 2014. Cyberdomenet er relativt nytt og truslene her er i konstant utvikling. Problemstillingen blir dermed:

[2] Hentet fra http://www.statoil.com/no/EnvironmentSociety/security/Pages/CSIRT.aspx, den 4. mai 2015
[3] FFI Forum i Oslo Militære Samfund 25. november 2014: Krisehåndtering i et sårbart cybersamfunn

Hva er et væpnet cyberangrep? Er norsk organisering adekvat for å takle et slikt?

I dag lever vi i en nasjon i dyp fred, men samtidig er nye trusler fra cyberangrep og andre globale trusler som terrorisme nærmere enn noen gang. Både PST og E-tj rapporterer om pågående etterretningsoperasjoner mot Norge. Det er derfor interessant å se hvordan krisehåndtering av cyberangrep gjennomføres i den andre enden av kriseskalaen. Totalforsvarskonseptet tilsier at Forsvaret skal lede krisehåndtering i en væpnet konflikt, og at det sivile samfunn skal gi støtte.

For å svare på problemstillingen er det nødvendig å forklare sentrale grunnleggende forhold som både cybersikkerhet, og organisasjonsteori knyttet til offentlig sektor. Vår sikkerhet i cyberdomenet utfordres av ulike former for angrep. Cybertrusselen innebærer mange typer angrep. Jeg vil forklare teoretiske forhold knyttet til utviklingen i cyberdomenet. Offentlig sektor er i dag tuftet på noen prinsipper. Dette forklares i kapittel 2.

Studiens andre del vil analysere både begrepet cyberangrep og hva som er grunnlag for å kreve rett til selvforsvar, samt væpnet konflikt med cyberangrep som virkemiddel. I mangel på en konkret konflikt som kan analyseres, har jeg laget en sikkerhetspolitisk casestudie. I denne er cyberangrep et av virkemiddelene som blir brukt mot Norge. Terroraksjonen 22. juli 2011 utfordret kriseledelse i offentlig sektor. Casestudien skal sette fokus på krisehåndtering i en væpnet konflikt. Avslutningsvis i denne delen ses det på hvordan andre nasjoner har innrettet sin offentlige virksomhet for å ivareta cybersikkerhet. Et militært angrep på Norge er et ytre sjokk og vil gi rett til selvforsvar. Et militært angrep kan bestå av ett eller flere virkemiddel. Og cyberangrep er ett av virkemidlene en aggressor kan velge blant. I en væpnet konflikt kan cyberangrep påvirke mange dimensjoner både militært og sivilt.

Mitt bidrag med denne oppgaven er å se på cybersikkerhet som del av væpnet konflikt, og hvilken betydning nasjonal organisering har for håndtering av dette. Totalforsvarskonseptet beskriver at Forsvaret skal lede innsatsen for å ivareta statssikkerheten. De militære kapasiteter har en rolle i en væpnet konflikt. I fredstid kan de samme kapasitetene gi støtte til de sivile samfunn etter bestemte regler. Den daglige ivaretagelsen av cybersikkerhet håndteres av ulike sektorer. Ved en væpnet konflikt må de ulike ressursene ses i sammenheng. Evne til å prioritere i både tid og rom kan sette kriseledelse på prøve. Er det stor likhet mellom fred og væpnet konflikt bør muligheten for å lykkes med krisehåndtering være god.

Cyberdomenet er et nytt domene for påvirkning og maktprojeksjon. Det er grenseløst og er hverken bundet av territorium eller grenser. Cyberdomenet eller Cyberspace er et av de fem

globale allmenninger[4], og sammenkoblingen av nettverkene på tvers av grenser, gjør at nasjoner, organisasjoner og individer kan påvirke og gjennomføre målrettede cyberangrep uavhengig av geografisk plassering.

Cyberdomenet er dermed unikt sammenlignet med andre når det gjelder en felles plattform, eller et felles utgangspunkt for aktivitet og utvikling. I en globalisert verden kan samhandling eller ondsinnede handlinger gjennomføres uten barrierer som avstand, språk og kulturforskjeller. Med utgangspunkt i dette er det interessant å se hvilket potensiale som ligger i cyberdomenet, samt hvilke metoder som kan benyttes å virke i cyberdomenet.

De ulike cybertruslene kan gjennomføres ved to former for angrep. Enten et åpent eller et skjult angrep. Et åpent angrep gjennomføres på en slik måte at det ikke er tvil om hva som hender. Det mest vanlige er å benytte distribuert tjenestenekt (DDoS[5]) eller tjenestenekt (DoS[6]) til slike åpne angrep. Disse lammer deler av nettet i en tidsperiode, og årsaken er åpenbar. Defacing kan også benyttes som et åpent angrep hvis det er åpenbart at endringen som gjennomføres er utført med intensjon. Her er det helt tydelig at det nye budskapet kan attribueres eksternt, og til andre enn eieren av siden. Det utføres ved å endre et nettsted til å se annerledes ut eller å erstatte nettstedet med bilder eller tekst som avviker fra hensikten til det opprinnelige. Slike åpne angrep kan være en del av en større informasjonsoperasjon (INFOOPS).

Et skjult angrep gjennomføres i den hensikt å ikke bli oppdaget. I dette ligger at angriperen forsøker å gjennomføre aktivitet i nettet. De mest sannsynlige skjulte angrepene er spionasje, sabotasje eller subversjon (Rid, 2011). Den amerikanske Director of National Intelligence (DNI) definerer trusselen som kun cyberangrep og cyber spionasje (Clapper, 2013, s. 1).

Spionasje gjennomføres ved å trenge inn i nettverket enten direkte eller indirekte for å hente ut viktig og relevant informasjon. Direkte inntrenging utnytter sårbarheter i kritisk infrastruktur. Og denne formen for aktivitet er sårbar for oppdateringer av programvare. Når sikkerhetshull oppdages, og produsenten sender ut oppdateringer kan sikkerhetshull stenges. Sikkerhetshull kan også etableres gjennom manipulasjon av hardvare og programvare. Dette er særdeles vanskelig å få til både før og etter at en komponent eller program settes i et system. Endringer i etterkant kan utføres av en utro tjener på systemet. En utro tjener kan også bidra til en indirekte inntrengning i nettverket ved å flytte informasjon inn og ut av nettverk. En annen form for indirekte

[4] Fra engelsk Global Commons. Områder som ikke styres av en stat: det åpne hav, de polare områdende, verdensrommet, de høye luftlag og internett
[5] Distributed Denial-of-Service (DDoS)
[6] Denial-of-Service (DoS)

inntrengning er å lage programmer som kan følge minneenheter mellom nettverk. Disse programmene samler data, og sender ut data når minneenheten igjen er tilkoblet det initielle nettverket.

Sabotasje er den andre formen for angrep. Stuxnet[7] er den mest kjente sabotasjen gjennomført så langt. I tillegg er dette det eneste kjente cyberangrep som fysisk har ødelagt komponenter. Stuxnet ble gjennomført ved å utvikle en ondsinnet kode som ble plantet inn i systemene (Rid, 2011, s. 17). Koden var laget for å spionere på og omprogrammerer industrielle systemer. Målet for koden var styringen av hastigheten på sentrifugene ved det iranske atomanlegget. Styringen ble manipulert til å spinne ukontrollert, og sentrifugene ble ødelagt. Sabotasje kan videre være ondsinnede programmer som sletter informasjon på målsystemene, eller at de endrer data slik at de blir ubrukelige. Et tenkt eksempel på det siste ville vært et program som klarte å endre alle tidspunkter og kartreferanser i en motstanders operasjonsplan. Dragonfly eller HAVEX var en skadevare mot industrielle styringssystemer (SCADA-systemer[8]) som mål. Sommeren 2014 var det en større hendelse både mot oljebransjen i Norge og energisektoren i Europa (Bakken, Christensen, & Ånestad, 2014). Skadevaren ble oppdaget. Og det viste seg at hackernes verktøy i angrepet mot norske olje- og energiselskaper var konstruert for å utføre sabotasje (Bakken & Aarseth, 2014). Selv om dette ble oppdaget og det ikke kom til skade kan det være forberedelser til en senere konflikt. Sporene pekte mot Kina. I tillegg til skadevare kan DDoS og DoS også benyttes til sabotasje. Tjenestenektangrep vil sabotere tilgang til maskiner og komponenter, eller gjøre nettverksressurser utilgjengelige.

Til slutt er det subversjon. Her gjennomføres handlinger ofte i sammenheng med eller i tilknytning til informasjonsoperasjoner. Hensikten er å endre innhold slik at budskapet endrer karakter og derigjennom undergraver maktinstitusjoner eller -personer. Under den russiske annekteringen av Krim i 2014 tok de kontroll på telekommunikasjonsinfrastruktur. Russerne fikk derigjennom mulighet til å styre tilgang til tv og radiostasjoner, samt mobiloperatører (Franke, 2015). En enklere metode kan være å sende ut falske eposter som utgir seg for å være ekte, samt å endre innhold på nettside. En annen metode kan enten være å etablere falske nettsteder som brukere rutes til når de søker informasjon på nett. Et annet kjent eksempel på forsøk på

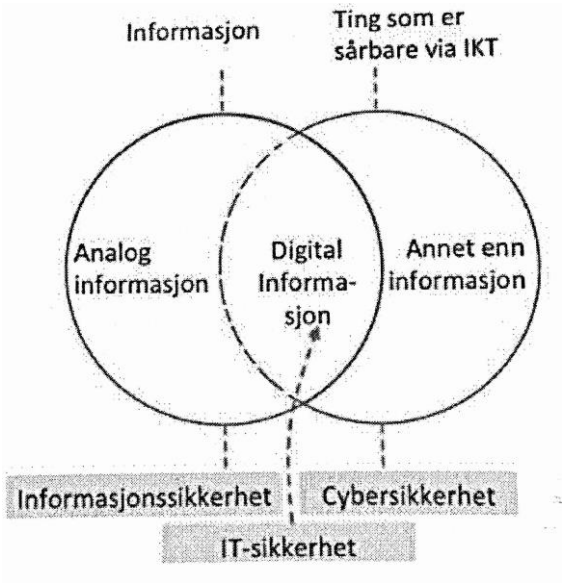
[7] Stuxnet er en Advanced Persistent Threat (APT). En avansert vedvarende trussel i form av en ondsinnet programvare. Det kreves mye ressurser for å lage et målrettet program som skal virke over tid.
[8] SCADA er forkortelsen for Supervisory Control and Data Acquisition

subversjon er nyheten om Obamas død som ble lagt ut på Fox News sin Twitter konto i 2011[9]. Nyheten førte umiddelbart til et stort børsfall i USA.

1.2 Begrepsavklaring

Denne oppgaven omhandler cybersikkerhet. Store norske leksikon beskriver at ordet sikkerhet brukes om tiltakene som benyttes for å oppnå denne tilstanden (Sikkerhet, 2013). I media tillegges informasjonssikkerhet og cybersikkerhet ofte samme betydning. Informasjonssikkerhet er derimot informasjon i både fysisk og digital form. Tiltak for å beskytte bøker i et bibliotek vil være informasjonssikkerhet. Det samme vil være å beskytte sensitiv informasjon mot tap eller innsyn.

Følgende Venn-diagram viser en forenklet sammenheng mellom begrepene. Kilden er websiden til Senter for cyber- og informasjonssikkerhet (CCIS) på Gjøvik (Senter for cyber- og informasjonssikkerhet 2014):



Cybersikkerhet omfatter det som kan påvirkes av og er sårbare via informasjons- og kommunikasjonsteknologi (IKT). Dette er både digital informasjon og annen informasjon som data og kontrollsystemer. NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) beskriver at cybersikkerhet favner både IKT sikkerhet, nettverkssikkerhet og internett sikkerhet (Klimburg, 2012, s. 10). Her er nettverks- og internettsikkerhet er knyttet til beskyttelse av kritisk infrastruktur.

[9] Hentet fra http://www.theguardian.com/news/blog/2011/jul/04/fox-news-hacked-twitter-obama-dead, den 5. mai 2015

Cybersikkerhet er et eget fagområde som favner mer enn det som defineres inn under områdene data sikkerhet og IKT sikkerhet. Hendelser som kommer frem og diskuteres i media er oftest knyttet til beskyttelse av digital informasjon. Dette senest i 2014 hvor Aftenposten avslørte falske basestasjoner i mobilnettet, såkalte IMSI-catchere, i Oslo (Foss, Johansen, & Hager-Thoresen, 2014).

1.3 Tidligere forskning

Det er tidligere skrevet to masteroppgaver ved Forsvarets høgskole som grenser mot tematikken i denne oppgaven. Den ene oppgaven er fra 2011 og ser på forholdet mellom ansvarsprinsippet og helhetlig tilnærming til cybersecurity i Norge (Skillingshaug, 2011). Den andre ser på sivilt-militært samarbeid i en cyberkrise, og har fokus på Cyberforsvarets rolle (Gustavsen, 2014).

Den første oppgaven er skrevet og levert før terrorangrepet mot Norge 22. juli 2011. I etterkant av denne hendelsen er samvirke innført som et prinsipp for offentlig krisehåndtering, og Gjørv-kommisjonen har sett på krisehåndtering i relasjon til terroren 22. juli.

Når det gjelder den andre oppgaven favner den freds- og delvis krisedimensjonen av konfliktspekteret. Bistandsinstruksen danner grunnlag for militær støtte til det sivile samfunn, og en felles øvelse Cyber Down hos Telenor i 2013[10] brukes som en av to casestudier. Oppgaven konkluderer med at Cyberforsvaret kan yte støtte til sivile virksomheter ved en krise.

1.4 Avgrensing

Denne oppgaven vil se på organisatoriske muligheter i den defensive delen av cybersikkerhet. Offensive kapasiteter er en del av utøvelsen av aktivt forsvar. I Norge er den offensive kapasiteten underlagt Etterretningstjenesten (E-tj). Informasjon om denne type kapasitet er høyt gradert og unntatt offentlighet i Norge samt andre sammenlignbare land. Thomas Rid fra King's College i London argumenterer i en video publisert på NATO Review Magazine at det ikke er en sammenheng mellom offensive og defensive cyber kapasiteter. Dette er avvikende i forhold til andre militære kapasiteter (NATO, 2013a).

1.5 Oppbygging av oppgaven

Første del av oppgaven fokuserer på det teoretiske grunnlaget for håndtering av cybersikkerhet og organisering for kriser. Her brukes både primærkilder og sekundærkilder. Bøkene til Clarke og Rid er primærkilder som det ofte siteres fra i ulike sammenhenger innenfor cyberdomenet. For innsyn i andre dimensjoner av cybertrusselen er dette hentet fra sekundærkilder som

[10] Hentet fra http://www.telenor.com/no/media/pressemeldinger/telenor-over-pa-cyberkrise/, den 15.mai 2015

avisartikler, innlegg i debatter og ulike rapporter. Organisering for krisehåndtering er i hovedsak beskrevet i offisielle dokumenter fra Stortinget og de teorier som det henvises til her.

Andre del av oppgaven bygger på et scenario. I mangel av en væpnet konflikt som er dokumentert med et større innslag av cyberhendelser, er det laget et scenario. Beskrivelsen av organisering og prosesser er hentet fra primærkilder som Stortingsmeldinger og – proposisjoner med tilhørende Norsk offentlig utredninger, samt instrukser til statlige etater og virksomheter. I tillegg til dokumenter er det hentet informasjon fra offentlige websider både i Norge og i utlandet. Som primærkilde er også rapporten fra en arrangert workshop[11] og intervjuer med representanter fra Kripos og Utenriksdepartementet (UD). Annen informasjon om dagens organisering og mulige utviklingstrekk i cyberdomenet er hentet fra sekundærkilder. Sekundærkilder til oppgaven er bøker, artikler i media og kommentarer/kronikker i media. Felles for disse er at de omhandler cybersikkerhet eller organisasjonsteori.

[11] Oppsummering etter tverrsektoriell workshop15. april 2015

2 Analytisk rammeverk

2.1 Metoder og kilder

Cybersikkerhet handler om å ha tiltak som oppnår sikkerhet. Stor norske leksikon beskriver at tiltakene kan deles opp i tre kategorier: teknologiske, organisatoriske og menneskelige (Sikkerhet, 2013). Teknologi er forhold i cyberdomenet og organisering er ivaretagelse av krisehåndtering. I dette kapittelet vil i tillegg til metode og kilder forklare teori knyttet både til cybertrusselen, og til det organisatoriske grunnlaget krisehåndtering i offentlig sektor.

Oppgaven er basert på bruk av kvalitativ metode. Tematikken rundt problemstillingen er lite belyst, og det er lite forhåndskunnskaper. Litteraturstudium er benyttet for både å forklare hva som ligger i cybertrusselen nå og i fremtiden, samt hva som ligger til grunn for organisering av offentlig sektor. I tillegg er det søkt etter litteratur som beskriver generelle prinsipper for krisehåndtering.

Ut over litteraturstudie som ble benyttet for å danne ramme, oversikt og for å klarlegge definisjoner ble det gjennomført en workshop. Innledningsvis ble også intervjuer vurdert som metode for å ha primærkilder til de ulike utfordringer knyttet til temaet. Utfordringen med intervjuobjektene er imidlertid deres posisjon som aktør i et landskap som kan preges av rivalisering og posisjonering. For å unngå en sirkel hvor aktørene peker til siden, ble det planlagt og gjennomført en tverrsektoriell workshop (rundebordskonferanse). Her ble deltagerne i fellesskap utfordret på fremtidig nasjonal hendelseshåndtering og forebyggende tiltak. Tre hendelser, caser, var beskrevet på forhånd ut fra litteraturstudie om fremtidig trussel i cyberdomenet. Hendelsene var i spekteret fra væpnet konflikt til ordinær cyberkriminalitet. Casene var utformet for å utforske samvirke innenfor cybersikkerhet, samt om samvirke mellom aktørene var ulikt i fred og i væpnet konflikt.

2.1.1 Casestudie

Dokumentstudier ga ikke klare svar på samarbeidet i en væpnet konflikt. I hovedsak er det fordi hverken Norge eller andre NATO land har fått slik erfaring. Konflikter de siste tiårene har vært mot teknologisk underlegne motstandere. Georgia i 2008 har vært i konflikt hvor cybervirkemidler var en del av virkemidlene som ble brukt mot dem. Ukraina er i en konflikt nå som involverer et annet sett med cyberangrep. Erfaringer fra begge er mest om hva slags cyberangrep som ble brukt, og minimalt om hvordan nasjonene fikk samlet ressursene for å forvare seg i cyberdomenet. I tillegg har nasjonene lite til felles med norsk offentlig sektor, og erfaringer fra krisehåndtering har liten overføringsverdi.

En casestudie er en form for studie hvor selve studieobjektet er avgrenset i tid og rom (Jacobsen, 2005). I dette tilfellet ønsker jeg å se på en væpnet konflikt over et begrenset tidsrom. Krisen som grunnlag for studien må være alvorligere en 22. juli og den må være innen for tolkningen av væpnet angrep. Casestudien oppfyller kravene til å være en spesiell situasjon (Jacobsen, 2005, s. 87-101).

Til denne oppgaven er det utviklet en casestudie for å se på krisehåndtering av cyberangrep i en væpnet konflikt. Denne ble presentert som case på en tversektoriell workshop om nasjonalt samarbeid om cybersikkerhet[12]. For bruk i denne oppgaven spesifikt er den i ettertid utvidet til å bli en casestudie. Som grunnlag for denne casen ble det hentet informasjon fra to kapittel i DSB sin rapport *Nasjonalt risikobilde 2014* (Direktoratet for samfunnssikkerhet og beredskap, 2014), samt informasjon om cyberangrep fra konflikter de seneste ti-årene. De to kapitelene i rapporten er strategisk overfall og angrep på EKOM-infrastruktur. Dette er hendelser som DSB anser som både tenkelige og alvorlige scenarioer. Hendelsene har lav sannsynlighet, men har samtidig relativ stor konsekvens. Begrepet «sannsynlighet» i Nasjonalt risikobilde har mer til felles med den engelske termen «likelihood» enn «probability» (DSB, 2014, p 25). Casen var en av de tre som ble diskutert under en tversektoriell workshop innenfor cybersikkerhet[13]. De to andre var ulike former for cyberangrep i fredstid. Dette for å avdekke eventuelle ulikheter i samvirke mellom aktørene i fred og i væpnet konflikt.

Metoden som ble benyttet ved gjennomføringen av workshop hadde tre steg. Det første var beskrivelse av en case med cyberangrep, deretter hendelseshåndtering av cyberangrep i case og til slutt mulige tiltak for å redusere konsekvensen av cyberangrep i forkant.

Innledning til casene ble gjennomført av undertegnede som deretter inntok rollen som referent. Diskusjonen ble ledet av en egen ekstern moderator. I etterkant ble det utarbeidet en rapport som oppsummerte gruppens arbeid. Ved å innta rollen som referent og ikke deltagere i diskusjonen unngås at diskusjonen påvirkes opp mot funn i prosessen så langt. Metoden er sårbar manglende for deltagelse. Selv om invitasjon var sendt ut i stor bredde, var det mange som ikke svarte eller meldte forfall. Dette utfordrer validiteten i gruppens tilsvar på hvordan hendelsene skal håndteres av de nasjonale aktørene, og hvordan konsekvenser av hendelsene kan reduseres i forkant.

Invitasjon til workshop ble sendt ut for å oppnå bred tversektoriell representasjon. Deltagere som møtte var representanter fra Cyberforsvaret (CYFOR), NorCERT, KraftCERT, Nasjonal Kommunikasjonsmyndighet (NKOM), Høgskolen på Gjøvik, Norsk senter for

[12] Oppsummering etter tverrsektoriell workshop15. april 2015

informasjonssikring (NORSIS) og Kongsberg Defence and Aerospace (KDA)[14]. Bredden av de som møtte var god. Deltagerne var både fra offentlig og privat sektor, samt fra militær og sivil side. Deltagelse fra akademia ga mulighet til å holde diskusjonene på et faglig riktig nivå.

For noen av deltagere som ikke møtte ble det gjennomført supplerende intervjuer. Dette gjelder for representanter for Utenriksdepartementet (UD) og Kripos. Intervjuene var delvis strukturerte og fulgte en intervjuguide. Respondenten fikk tilsendt intervjuguide i forkant, og de ble anmodet om å ta opp andre problemstillinger.

2.1.2 Kilder

Kilder til oppgaven er i hovedsak bøker om cybersikkerhet og krisehåndtering. I tillegg kommer meldinger fra Stortinget som omhandler samfunnssikkerhet og organisering av offentlig sektor. Som sekundærkilder er artikler i aviser og på nett, samt rapporter om cyberhendelser.

Innenfor cyberteori er bøkene til Clarke, Rid og Krepinevich. I tillegg kommer nettsider til NATO og EU etater som NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) og European Union Agency for Network and Information Security (ENISA). Begge disse har som hovedformål å bedre cybersikkerhet hos sine medlemmer. Primærlitteratur for krisehåndtering er bøker av Fimreite, Dyndal (red), Colbjørnsen og Boin. Disse ser alle på ulike sider ved krisehåndtering i offentlig sektor, og hvordan den kan gjennomføres.

Sekundærlitteratur er artikler på nett og i aviser. Her er det en del empiri om hendelser, samt en del innlegg i diskusjonen omkring både cybersikkerhet og krisehåndtering. Flere av artiklene henviser tilbake til bøkene som er benyttet som primærlitteratur.

2.2 Teori om cyber

Cyberdomenet er relativt nytt. Det er flere som har meninger om hvilken effekt og potensiale som ligger i påvirkning av andre gjennom dette domenet. Det er lite tilgjengelig teori om emnet. I dette avsnittet forklares de teknologiske tiltakene innenfor cybersikkerhet. Innledningsvis redegjøres for hvilket potensiale det ligger i et cyberangrep. Dette ved en gjennomgang av tre ulike syn på cyberdomenet. Deretter beskrives hvordan det kan velges verktøy for å møte cyberangrep. Til slutt redegjøres for hvordan informasjonsdeling kan bidra til bedre cybersikkerhet.

[13] Oppsummering etter tverrsektoriell workshop15. april 2015
[14] Oppsummering etter tverrsektoriell workshop15. april 2015

2.2.1 Potensiale til cyberangrep

Hans Inge Langø har skrevet en artikkel som kategoriserer de ulike miljøenes syn på potensialet i cyberdomenet. I artikkelen Den akademiske debatten om cybersikkerhet beskrives tre ulike skoleretninger innenfor cybersikkerhet(Langø, 2013, s. 229). Disse tre er teoretiske forklaringer på hva som kan ventes i cyberdomenet. Den første kalles *revolusjonistene*. De ser for seg en ny type krigføring som er mulig med informasjonsrevolusjonen. Krigen vinnes av den med best informasjon om slagmarken (Arquilla & Ronfeldt, 1997, s. 23). Den som best evner å utnytte nettverkene får en styrkemultiplikator. Videre vil cyberangrep, både forstyrrende og ødeleggende, ha en egen strategisk verdi i konflikter. I boken Cyber War advarer Richard A. Clarke mot et elektronisk Perl Harbor (R. A. Clarke & Knake, 2010). En utfordring med cyberangrep mot infrastrukturen er at angriperens egne operative evne kan reduseres. Begge parter ønsker å utnytte samme infrastruktur. Oppsummert har revolusjonistene et økende fokus på temaet samt de ser potensial for at cyberspace og cyberverktøy danner grunnlag for nye konsept og ideer (Langø, 2013, s. 232).

Den andre retningen er *tradisjonalistene*. De ser også på informasjonskrigføring, men i den forstand at de mener tanken er lite realistisk eller den ikke er gjennomførbar. Argumentasjonen går på den manglende empiri om temaet, og de betviler at et «Cyber Pearl Harbour» kan ramme en eller flere nasjoner. Thomas Rid er en av tradisjonalistene og han nedtoner i sin artikkel «Cyber War Will not Take Place» betydningen av en egen cyberkrig (Rid, 2011). Han har to begrunnelser for dette. For det første passer begrepet ikke til Clausewitz definisjon av krig grunnet fraværet av vold. Og for det andre viser empirien et større innslag av metoder som spionasje, sabotasje og subversjon i cyberpace. Tradisjonalistene ser videre for seg at cyberkrig kan ha en strategisk nytteverdi.

Til slutt har vi den retningen som beskriver cybersikkerhet fra et økologisk perspektiv. De analyserer cyberspace som domene eller miljø. Cyberangrep kan ha en sjokkeffekt, men mangler kjernevåpenets eksistensielle trussel. Videre kan cyberangrep ha en forstyrrende effekt som kan ligne på effekten ved luftbombing (Krepinevich, 2012). Den dimensjonen som cyberangrep ikke understøtter er direkte fysisk ødeleggelse. Revolusjonen innenfor teknologi samt kostnadsaspektet gjør cyberdomenet mer tilgjengelig for nye og andre aktører enn de tradisjonelle, og maktbalansen endres over tid i dette domenet.

2.2.2 Verktøy

Klassifisering av cyberangrep letter prosessen med å finne riktig verktøy. Et slikt grunnlag med fokus på både hvordan og hvorfor gir merverdi i hendelseshåndtering. Det letter også samvirke

med andre virksomheter. De ulike formene for cyberangrep krever ulik tilnærming. Hvilke verktøy som skal brukes avhenger av type angrep og hvordan det er klassifisert. I enkleste forstand DDoS er støy på forbindelsen, og forhindrer informasjonsflyten både inn og ut av virksomheten. Her må adressen til avsender sperres slik at denne trafikken ikke blokkerer.

Mot Advanced Persistent Threat (APT) er det behov for andre og mer avanserte verktøy. APT er unike former for cyberangrep som er avanserte og vedvarende trusler. Cyber Kill Chain®[15] er en metodikk for å møte cyberangrep i form av APT i ulike faser av gjennomføringen. Denne følger samme sju steg som er kjent fra andre etterretningsdrevne operasjoner. Disse er rekognosering, klargjøring (weaponization), leveranse, utnyttelse, installering, kommando og kontroll samt målrettet angrep. Det er unike karakteristika ved de ulike fasene, og ved å sette inn ulike mottiltak forhindres iverksettelse av det målrettede angrepet. Ut fra denne metodikken kan et angrep forhindres ved å oppdage rekognoseringen eller i beste fall forhindre den. Metodikken skal gi bedre effekt av de ressurser som brukes for å unngå cyberangrep. Effekten av tiltak er best tidlig i fasene. Fra den fysiske verden kan det sammenlignes med å kutte tilførsel av deler til en bilbombe i stedet for å lete etter en gul bil med bombe blant flere hundre andre.

Klassifisering er viktig for å velge riktig verktøy for mottiltak. Evne til klassifisering og valg av metode stiller store krav til kompetanse og helhetsforståelse. Noen verktøy tilhører virksomheten selv, andre er innenfor politiets ansvarsområde og noen få kan løftes til politisk nivå. Klassifisering av cybertrusselen kan skisseres på følgende måte:

[15] Cyber Kill Chain® er utviklet av Lockheed Martin for å møte Advanced Persistent Threat (APT)

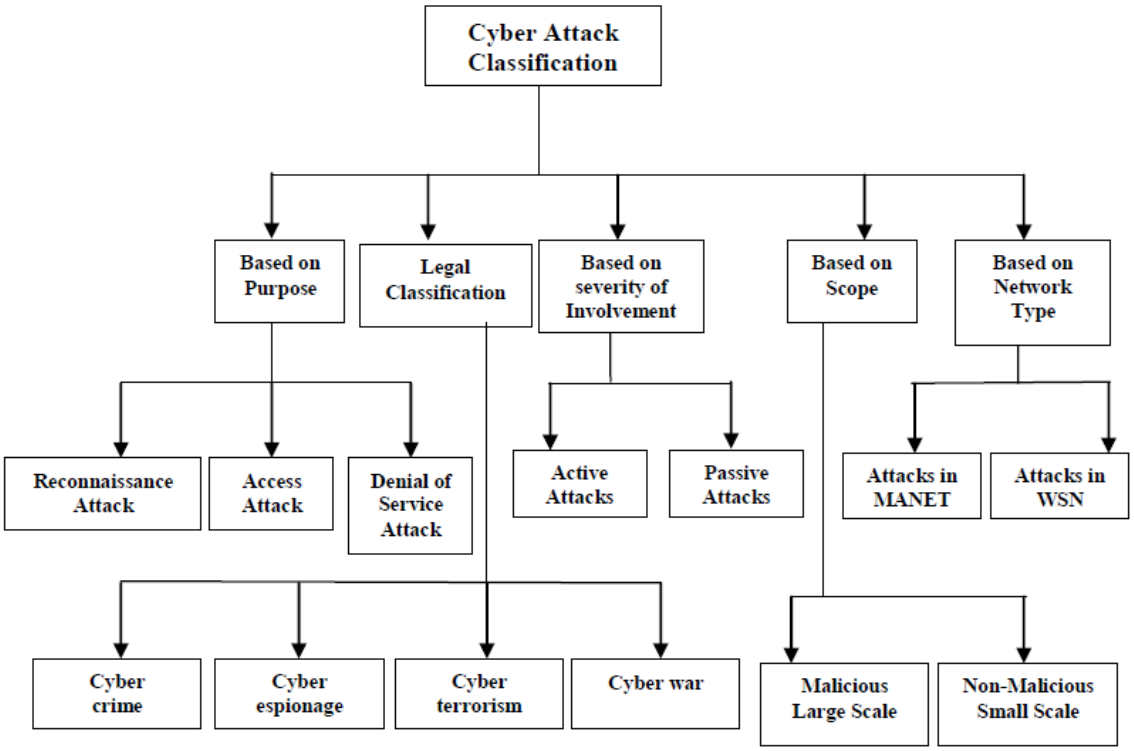


Figure 1: Attack classification diagram

(Uma & Padmavathi, 2013)

Når det gjelder klassifisering etter hensikt er det stor forskjell på rekognosering og DDoS angrep, og verktøyene vil være forskjellige. DDoS angrep er relativt tidsbegrenset og gjennomføres ofte kun mot et fåtall adresser eller punkter i nettverket.

Juridisk klassifisering er komplisert. Kriminalitet, terror og «cyberkrig[16]» krever alle ulike former for verktøy og bruk av nasjonens virkemidler. Kriminalitet er politiets oppgave. Hvis kriminaliteten har utgangspunkt utenfor Norge må det samarbeides med andre land, Europol og Interpol. Terror og væpnet konflikt involverer bruk av militære maktmidler for å forsvare nasjonens interesser.

Verktøyene som kan benyttes mot cyberangrep er fordelt mellom de ulike aktørene i offentlig og privat sektor. Verktøyene har konstant knytning til sin virksomhet eller etat. Ledelse av og utnyttelse av verktøyene er situasjonsbestemt. I væpnet konflikt vil Forsvaret ha en rolle.

2.2.3 Informasjonsdeling

Litteraturen beskriver informasjonsdeling som et godt alternativ for å forebygge cyberangrep. Informasjonsdeling har to funksjoner. Det ene er for å bygge robusthet og det andre for hendelseshåndtering. Robusthet skapes ved å dele 'best practise' i grupper av virksomheter.

[16] Oversatt fra engelsk Cyberwar

Internasjonalt er det flere grupper med virksomheter som deler informasjon, og som er knyttet mot nasjonene. I Europa er European Union Agency for Network and Information Security (ENISA) et nav i informasjonsutveksling, deling av Best Practice og kunnskap. Videre er det Forum of Incident Response Teams (FIRST), som er en global interesseorganisasjon. Her er det ti norske medlemmer inkludert NorCERT[17]. De fleste CERT og CSIRT enhetene har også en Information Sharing and Analyst Centre (ISAC) rolle. I Europa er det etablert et offentlig-privat samarbeid Fi-ISAC, som er et organ hvor bankvirksomhet, nasjonale CERT miljøer og juridiske etater jobber sammen mot cyber-kriminalitet. Informasjonen som deles bidrar til å redusere gjenbruk av karakteristika ved et cyberangrep. En angriper må derfor sette inn ekstra ressurser for å utvikle en avart til neste gjennomføring.

Den andre funksjonen er for hendelseshåndtering. Her bidrar informasjonen til å oppnå situasjons bevissthet. Informasjon om trender og pågående angrep spres mellom aktørene. De ulike CERT miljøene kan holde fokus på enkelte områder.

2.3 Krisehåndtering i offentlig sektor

Organisatoriske tiltak er et element for å oppnå sikkerhet. Organisasjon med tilhørende ansvar og myndighet påvirker krisehåndtering. Innledningsvis i dette avsnitte forklares krise. Deretter beskrives krisehåndtering ved væpnet konflikt. Til slutt kommer strategiske forventninger til Forsvaret som kriseledelse i væpnet konflikt. Sentralt her er totalforsvarskonseptet.

2.3.1 Krise

I *Store norske leksikon* på nett defineres krise som en vanskelig situasjon, ett avgjørende vendepunkt eller en plutselig forandring, og den kan medføre en akutt politisk vanskelighet (regjeringskrise) (Krise, 2009). I boken *Organisering, samfunnssikkerhet og krisehåndtering* skilles det mellom to dimensjoner for en krise (Fimreite, 2011, s. 12). Den ene er knyttet til årsak og den andre til krisens faser. Årsaker for kriser deles i menneskeskapte eller naturlige. Cyberangrep og militært angrep er menneskeskapte kriser. Denne oppgaven fokuserer på den årsaken. Fasene i krise er forebygging og håndtering. Både for menneskeskapte og naturlige kriser et det mulig å forebygge. Vulkanutbruddet på Island i 2010 var en naturlig krise, og flyforbud ble iverksatt for å forebygge hendelser i flytrafikken. Menneskeskapte kriser som terror forebygges med antiterrortiltak (Fimreite, 2011, s. 12). Forebygging kan også være andre tiltak. Arjen Boin skriver også om krisehåndtering. Evnen til å håndtere kriser bedres ved å forberede de som skal bistå i første linje og gi dem trening (Boin & McConnell, 2007, s. 52-53). Forebygging er både tiltak for å redusere tiltak og trening eller øvelse.

[17] Hentet fra https://www.first.org/members/map#NO, den 19.april 2015

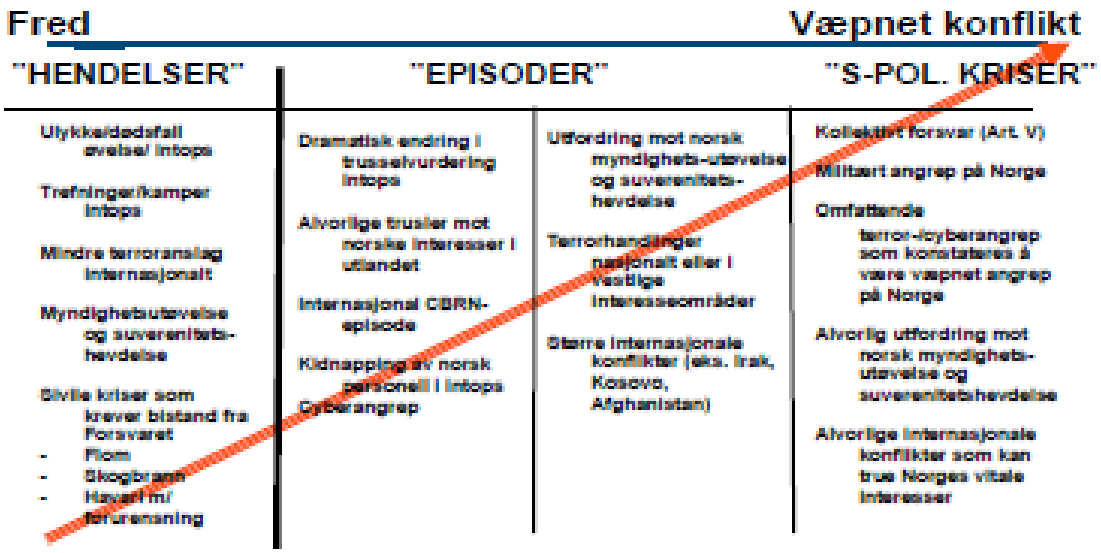
Krisehåndtering er å systematisere og iverksette tiltak mot uventede hendelser. Krise er en hendelse som oppstår uten forvarsel og som har et omfang som gjør det vanskelig å håndtere med normale rutiner og organisasjon. Med krise menes i denne sammenhengen en alvorlig trussel mot grunnleggende samfunnsstrukturer eller sentrale verdier knyttet til sikkerhet, velferd, liv og helse som krever hurtig reaksjon under stor grad av usikkerhet (Boin, 2008, s. XVIII; Fimreite, 2011, s. 14). I en væpnet konflikt er det statssikkerheten som er truet. I tillegg vil det råde kaos og i enkelte geografiske områder kan det være hendelser som har betydning for samfunnssikkerheten. St. meld 22 definerer samfunnssikkerhet som (St. meld. 22 (2007-2008), 2008, s. 8):

Samfunnssikkerhetsbegrepet brukes bredt og dekker sikkerhet mot hele spekteret av utfordringer, fra begrensede hendelser, via større krisesituasjoner som representerer omfattende fare for liv, helse, miljø og materielle verdier, til sikkerhetsutfordringer som truer nasjonens selvstendighet eller eksistens.

Cyberangrep kan skape en krise i seg selv eller det kan være et element av en større krise. Et cyberangrep som kan medføre krise må være overaskende, plutselig og omfattende. Hvis angrepet kan attribueres til en nasjonalstat kan det oppstå en sikkerhetspolitisk krise. Cyberangrep er en menneskeskapt og villet hendelse iverksatt i en hensikt å oppnå en fordel.

Kriseforløp kan ha fem faser (Fimreite, 2011, s. 14). Disse er kriseerkjennelse, krisebeslutninger, krisekommunikasjon, kriseavslutning og kriselæring. Den siste er viktig med tanke på videre utvikling og læring til neste hendelse.

Iverksettelse av nasjonal krisehåndtering er post-hendelse. Med dette forstås at hendelsen må skje, og den må analyseres og kategoriseres for å velge rett krisehåndtering. Kriseskalaen beskriver de ulike former for kriser og er et hjelpemiddel for å definere omfang. De ulike definerte krisene er gruppert innenfor områdene hendelser, episoder og kriser. Hendelser er aktivitet som håndteres med normal fredstidsorganisasjon. Konfliktskala under hentet fra fellesoperativ doktrine (Forsvarsstaben, 2014, s. 66):



De fleste kriser er tidskritiske og en analyse må raskt plassere hendelsen i en forhåndsdefinert kategori. FFOF sier at begrepene imidlertid ikke er absolutte, og i mange tilfeller er det først mulig å foreta kategoriseringen av dem i etterhånd (Forsvarsstaben, 2014, s. 66). For de alvorligste kategoriene innenfor episoder og sikkerhetspolitiske kriser sammenkalles regjeringens kriseråd.

I en trusselbasert krisehåndteringsmodell ville regjeringens kriseråd blitt sammenkalt ut fra en trusselvurdering. Terrortrusselen mot Norge og politiet spesielt i 2014 fikk ingen konsekvenser for krisehåndtering. Det ble ikke sammensatt en kriseledelse til å forberede seg på en hendelse. Det ble kun iverksatt bevæpning[18] av politiet. For tidskritisk krisehåndtering må kriseledelse være etablert eller ha kort varslingstid for oppmøte.

2.3.2 Krisehåndtering ved væpnet konflikt

Krisehåndtering ved væpnet konflikt skiller seg fra alvorlig krise på ett vesentlig punkt. Når nasjonen står overfor et militært angrep samles Regjeringen og konstaterer at Norge er under et væpnet angrep i henhold til grunnlovens § 26 (Forsvarets høgskole/Forsvarets stabsskole, 2013, s. 8; Grunnloven, 1814).

Ministerstyre[19] og sektorprinsippet er gjeldende i offentlig sektor i Norge. Sektorprinsippet innebærer at inndelingen i statsforvaltningen er sammenfallende med statsrådens ansvarsområde

[18] Pressemelding Nr: 76 – 2014 Samtykke til bevæpning hentet fra https://www.regjeringen.no/nb/aktuelt/Samtykke-til-bevapning/id2341743/ , den 29. april 2015

[19] Hentet fra http://no.wikipedia.org/wiki/Ministerstyre, den 14. mai 2015: «Ministerstyre er et begrep som innebærer at en minister har rett til å detaljstyre den delen av forvaltningen som er underlagt statsråden (ministeren), mye som en administrerende direktør i et selskap. Når ministerstyre råder er det statsråden som har overordnet ansvar for alle beslutninger og handlinger utført innenfor hans eller hennes avdeling eller tjeneste

(Direktoratet for forvaltning og IKT, 2014, s. 27). Organiseringen har ved flere anledninger blitt utfordret med alternative løsninger. Sårbarhetsutvalget ledet av Kåre Willoch foreslo blant annet et beredskapsdepartement (NOU 2000:24, 2000). I etterkant av 22. juli rapporten ble det også tatt til orde av enkelte at det burde være en justering av organisasjonen (Fimreite, Lango, Lægreid, & Rykkja, 2012).

Utviklingen av nasjonal krisehåndtering har siden Sårbarhetsutvalget la frem sin anbefaling i 2000 vært preget av erfaring fra større alvorlige hendelser. Både terrorangrepet 9. september 2001, Tsunamien i Indiahavet 26. desember 2004 og terrorangrepet i Norge 22. juli 2011. Terrorangrepet i USA 2001 er tatt med som grunnlag i Stortingsmelding 17 om samfunnssikkerhet fra 2002 (St.meld. nr. 17 (2001-2002), 2002) og denne presiserer gjeldende prinsipper for krisehåndtering. Ansvar er knyttet til sektorprinsippet og linjeansvar for det enkelte fagdepartement. Det departement som er berørt har ansvar også i krise. Nærhetsprinsippet er at krisen skal håndteres så lavt som mulig i linjeorganisasjonen. Ved alvorlig krise løftes dette opp til regjeringsnivå. Til slutt skal organiseringen av kriser være mest mulig lik den daglige organiseringen, også beskrevet som likhetsprinsippet. Erfaring fra kriseledelse under Tsunamien i 2004 medførte etablering av både regjeringens kriseråd og krisestøtteenheten (KSE) i JD, samt en presisering på lederdepartement. Dette beskrives i en Stortingsmelding om Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering (St.meld. nr. 37 (2004–2005), 2005, s. 29). Kriseledelse med regjeringens kriseråd, lededepartement og krisestøtteenheten er også beskrevet i *Når sikkerheten er viktigst* (NOU 2006:6, 2006, s. 150). I etterkant av terrorangrepet i Norge 2011 er samvirke innført som et fjerde prinsipp for krisehåndtering gjennom en ny Stortingsmelding om samfunnssikkerhet (Meld. St. 29 (2011-2012), 2012).

Terrorangrepet 22. juli utfordret krisestyringsprinsippene. Ansvars- og nærhetsprinsippet ble utfordret ved at selve terrorhandlingen var todelt, og at terroristen beveget seg mellom to politidistrikter. For det første måtte det raskt fastslås om dette var innenfor ansvarsområdet til JD eller FD. Med dette på plass kunne krisen håndteres av politiressurser inkludert Delta. Og for det andre hvilket politidistrikt som hadde nærhet til handlingen og deretter handlingene. Det samme kan være gjeldende for et større cyberangrep som hverken er geografisk avgrenset eller som er knyttet til kun en kritisk infrastruktur. Mindre alvorlige cyberangrep håndterers som kriminalitet opp til et visst nivå. Dette er en utfordring i cyberdomenet. Her kan omfang endres underveis, og

(departementsnivå) overfor den lovgivende forsamling, statsministeren eller statsoverhode; for eksempel, kan en minister gå inn i enkeltsaker, overstyre underordnede tjenestemenn og ta endelige beslutninger»

bli noe annet og større. Hendelsen kan inkludere flere sektorer, men den enkelte er ikke alvorlig nok til å utløse kriseledelse.

Planer kan redusere usikkerheten ved en krise. Direktoratet for sivil beredskap (DSB) fører tilsyn med beredskapsplaner i departementene og er underlagt Justis- og beredskapsdepartementet. I tillegg utarbeider direktoratet et nasjonalt risikobilde, planlegger og gjennomfører øvelser samt andre tiltak innenfor samfunnssikkerhet[20]. De sjekker i at virksomheter og etater har beredskapsplaner. Kritikken som rettes mot denne ordningen er at innholdet får lite fokus (Fimreite, 2011, s. 54). Måleparameter er kvantitativt gjennom beredskapsplanen i seg selv, og ikke kvalitativ med fokus på innhold og om planene øves. Samvirke mellom aktørene oppnås ved prosesser for utvikling av planer og gjennomføring av øvelser. Ansvar knyttet til å lede planprosesser og øvelser kommer av plassering i sektoren. Planer utarbeides for å møte kommende utfordringer. Planen er ikke viktig i seg selv, men prosessen med å utvikle planen og etableringen av nettverket er viktigst (Fimreite et al., 2012). Beredskapsplaner bør øves. Sektorprinsippet kan medføre at de ulike etater iverksetter øvelser innenfor sine områder. Nasjonal kommunikasjonsmyndighet (NKOM) kan gjennomføre øvelser for å kvalitetssikre at konsesjonsvilkårene oppfylles av de som drifter kritisk infrastruktur. For å øve kriseledelse må kriseledelsen øve slik det er forutsatt og på lignende kriser som man antas kan oppstå.

Væpnet konflikt er en kompleks situasjon som krever at Regjeringens kriseråd[21] sammenkalles, og situasjonen tilsier at FD settes som lederdepartement. I komplekse krisesituasjoner er det behov for styrket koordinering mellom departementene, og i slike situasjoner trer Regjeringens kriseråd i funksjon. Dette rådet ble etablert i etterkant av håndteringen av Tsunamien i 2.juledag 2004. Regjeringen Bondevik fremmet et forslag til Stortinget om etablering av Regjeringens kriseråd. Dette er beskrevet i stortingsmeldingen som omhandlet flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering (St.meld. nr. 37 (2004–2005), 2005, s. 30). Forsvarssektoren setter fokus på opprettholdelse av statssikkerheten, mens justissektoren må ha fokus på samfunnssikkerheten også i de områdene som ikke direkte er berørt av konflikten. Politidistriktene setter stab og samarbeider med kommunale og fylkeskommunale aktører i tillegg til Sivilforsvaret og Forsvaret. Forsvaret avdeler styrker til operasjonelt nivå for å gjennomføre fellesoperasjoner i et definert operasjonsområde. I andre deler av nasjonalt territorium styrer politiet aktiviteten. NorCERT er nasjonal CERT og rapporterer cyberhendelser

[20] Hentet fra http://www.dsb.no/nn/toppmeny/Om-DSB/Ansvarsomrade/, den19. april 2015

[21] Regjeringens kriseråd har følgende faste medlemmer: regjeringsråden ved Statsministerens kontor, departementsråden i Justisdepartementet, departementsråden i Forsvarsdepartementet, departementsråden i Helse- og omsorgsdepartementet og utenriksråden i Utenriksdepartementet

til regjeringens kriseråd samt til NATO Computer Incident Response Capability (NCIRC) i NATO. I tillegg vil samarbeidende CERT/CSIRT nasjonalt og internasjonalt få rapporter.

2.3.3 Strategiske forventninger

Totalforsvarskonseptet beskriver utnyttelse av samfunnets ressurser i en krise. Konseptet har forankring tilbake til tiden etter 2. verdenskrig. starter Kapittelet *Totalforsvar og sivilt-militært samarbeid* i Stortingsmelding nr 39 fra 2004 innledes med følgende tekst (St.meld. nr. 39 (2003-2004), 2004):

Totalforsvarskonseptets grunnprinsipp har siden 1946 vært at samfunnets samlede ressurser, om nødvendig også private ressurser, skal kunne settes inn for å understøtte forsvaret av Norge. Formålet har vært å verne om Norges territorium, selvstendighet og nasjonale verdier og verne om sivilbefolkningen.

Sårbarhetsutvalget ledet av Kåre Willoch så på utvikling av forholdet mellom politi og forsvar (NOU 2000:24, 2000). I innledningen på kapittel 5 beskrives begge sider av et sivilt-militært samarbeid. Det sivile samfunn skulle håndtere naturkatastrofer og ulykker selv, med bistand fra forsvaret i enkeltsaker. Ved væpnet konflikt skal sivile myndigheter og ressurser være med på å støtte opp under forsvarskampen. Terrorangrepene i USA i 2001viste at et moderne samfunn er utsatt for kriser også i fredstid. Stortingsmelding *Samfunnssikkerhet–Veien til et mindre sårbart samfunn* kom året etter. Her fastslås at ikke-statlige aktører dukker opp i trusselbildet. Selv om andre kriser får fokus fastslås fortsatt at sivil støtte til Forsvaret er den mest grunnleggende formen for sivilt-militært samarbeid. Det står også at i situasjoner hvor ikke beredskapslovgivninger er trådt i kraft, så forutsettes det at samhandlingen mellom Forsvaret og sivile leverandører i stor utstrekning baserer seg på vanlige kommersielle vilkår (St.meld. nr. 17 (2001-2002), 2002, s. 93).

I stortingsmelding *Samfunnssikkerhet og sivilt-militært samarbeid* beskrives også planlegging og øvelser (St.meld. nr. 39 (2003-2004), 2004, s. 18). Flere andre støtter opp under behovet for å øve sammen. Boin beskriver at planer og øvelser er viktig (Boin & McConnell, 2007, s. 52-53). Øvelser er viktige for å forberede kriseledelse på de utfordringer den kan møte(Dyndal, 2010, s. 318). Planen er ikke viktig i seg selv, men prosessen med å utvikle planen og etableringen av nettverket er viktigst (Fimreite et al., 2012).

Når det gjelder sivilt-militært samarbeid nevnes samarbeidet mellom Forsvarsdepartementet og Justisdepartementet om etatsstyringen av Nasjonal sikkerhetsmyndighet (NSM) som eksemplet på sivilt-militært samarbeid innenfor et nytt totalforsvarskonsept. Selv om samarbeidet mellom

JD og FD fremheves som sivilt-militært samarbeid, skal det være mer enn interdepartementalt samarbeid. Sivilt-militært samarbeid skal også være mot sivile virksomheter utenfor offentlig sektor. Totalforsvaret handler om å få et faglig oppbygd ministerstyrt hierarki til å samvirke både internt og mot privat sektor. De nasjonale krisestyringsprinsippene er: Ansvar, nærhet, likhet og samvirke. Samvirke kom inn som det fjerde fra juni 2012 (Meld. St. 29 (2011-2012), 2012). De fire krisestyringsprinsippene beskrives også i egen instruks for departementene(Instruks for dep.arbeid med samfunnssikkerhet mv, 2012). Denne instruksen er gjeldende for sivil innsats i hele konfliktspekteret. Offentlig sektor er en hierarkisk struktur, og delegasjon av fagansvaret nedover i strukturen vil påvirke kriseledelse. Hvor mange underenheter ansvaret er fordelt på påvirker kontrollspennet, som derigjennom blir smalt (få) eller bredt (mange). Hierarkisk struktur eller klare kommandolinjer legger grunnlaget for hvordan kriseledelse kan gjennomføres. Fra politisk strategisk nivå via operasjonelt nivå ned til taktisk utøvende nivå. I et hierarki er det entydige instruksjons- og rapporteringsvei, og rapportering mellom nivåene følger tjenestevei (Colbjørnsen, 2004). Daglige aktiviteter og hendelser håndteres i sektorene i henhold til prinsippene ansvar og nærhet. I mindre alvorlige krisesituasjoner vil samordningen mellom departementene kunne ivaretas av lederdepartementet alene (St.meld. nr. 37 (2004–2005), 2005, s. 32). Ved en alvorlig krise sammenkalles regjeringens kriseråd. Rapportering og dialog i en hierarkisk struktur følger tjenestevei og er en vertikal prosess (Colbjørnsen, 2004, s. 206). Horisontal samhandling krever at noen bryter dette mønsteret. Denne samhandlingen er en utfordring ved nasjonal krisehåndtering. Regjeringens kriseråd skal koordinere innsatsen mellom de ulike departementene. Utfordringen er at ønsket om å samordne andre er større enn viljen til å bli samordnet (Fimreite, 2011, s. 23). Sektorprinsippet har lang tradisjon i Norge, men har også ved flere anledninger blitt utfordret med alternative løsninger. Sårbarhetsutvalget ledet av Kåre Willoch foreslo blant annet et beredskapsdepartement (NOU 2000:24, 2000).

2.4 Hypotese

Med bakgrunn i teorier som forklarer ulike deler av cybersikkerhet og teori om norsk krisehåndtering, skal denne oppgaven videre teste hvordan den norske organiseringen takler en væpnet konflikt med cyberangrep. Erfaringen fra 22. juli tilsier at Forsvaret vil møte noen av de samme utfordringene som nødetatene. Politi og sikkerhetsressurser som ble brukt i krisehåndteringen i 2011 omfattet ulike aktører i offentlig sektor. En væpnet konflikt vil medføre et utall aktører å forholde seg til i offentlig og privat sektor.

3 Cyberangrep

Dette kapittelet vil analysere hvordan Norge og andre forholder seg til cyberangrep i relasjon til selvforsvar. FN paktens artikkel 2(4) sier at medlemmer skal avholde seg mot bruk av væpnet makt mot andre staters territorielle integritet eller politiske uavhengighet. Brudd på dette gir nasjoner rett til selvforsvar etter paktens artikkel 51[22].

Thomas Rid beskrev at cybertrusselen var tredelt (Rid, 2011). Disse tre er spionasje, sabotasje og subversjon. Dette er delvis sammenfallende med den amerikanske Director of National Intelligence (DNI) som definerer trusselen som kun cyberangrep og cyber spionasje (Clapper, 2013, s. 1).

Et cyberangrep som væpnet angrep må bestå av flere elementer. For det første er den tekniske gjennomføringen og effekten angrepet kan medføre. Et angrep må videre være en menneskeskapt krise, og angrepet må attribueres til et land for at konsekvensen skal bli en mellomstatlig konflikt.

Kriterier for hvordan cyberangrep skal løftes til politisk nivå, og hvordan de skal møtes med sikkerhetspolitiske virkemiddel er det lite litteratur på. Norge og NATO har dokumenter som beskriver dette. Ut fra USAs håndtering av hendelsene mot Sony Pictures i slutten av 2014 vil det være mulig å si noe om deres tilnærming til dette.

Manual i krigens folkerett beskriver at Norge kan kreve rett til selvforsvar[23] hvis et cyberangrep forventes å forårsake død eller skade på personell eller ødeleggelse av objekter (Forsvarets høgskole/Forsvarets stabsskole, 2013, s. 190). Det er regjeringen som fatter en endelig beslutning om et cyberangrep skal anses å være et væpnet angrep (FDs cyberretningslinjer, 2014, s. 11). Med dette setter Norge en klar grense for hva som regnes som cyberangrep, og hva som er cyberoperasjoner. *Manual i krigens folkerett* skriver at spionasje og rekognosering regnes som cyberoperasjoner.

Internt er dette med på å sette fokus, og det er tydelig hva slags indikatorer som skal rapporteres opp i kommandokjeden. Både personell og enheter innen cybersikkerhet har forståelse for hva som skal oppdages, dokumenteres og rapporteres Den norske forståelsen setter en definert grense tilsvarende en fysisk grense. Aktivitet under grenseverdien er ikke en militær oppgave, men må håndteres som kriminalitet.

[22] FN pakten hentet fra http://www.fn.no/Bibliotek/Avtaler/FN-pakten/FN-pakten, den 12. mai 2015
[23] Artikkel 51 i FN pakten

Utfordringene med å sette en klar grense for hva som er cyberangrep er flere. For det første settes standard for bruk av ordet angrep knyttet til hendelser i cyber. Der de fleste andre nasjonalt bruker cyberangrep som synonymt med all ondsinnet aktivitet i cyber, så har forsvaret definert dette til å være en hendelse med en definert alvorlighetsgrad. Både deltagere på workshop og de som ble intervjuet bekreftet bruk av cyberangrep som dekkende for all ondsinnet aktivitet[24]. Den andre utfordringen ligger i den definerte grensen i seg selv. Den gir aggressor en fordel i valg av virkemiddel. Ved å legge seg opptil grensen, men ikke krysse den, blir Norge tvunget inn i et kriminalitetsspor.

I denne sammenheng må det påpekes at det er ulikheter mellom den fysiske dimensjonen og cyberdomenet når det kommer til selvforsvar. I cyberdomenet må et cyberangrep forårsake død eller alvorlig skade på materiell. Mens i det fysiske domenet er det trussel mot territoriell kontroll som utløser rett til selvforsvar. Dette ved at en annen nasjon ikke respekterer norsk grense og besetter deler av vårt territorium.

Når det gjelder cyberangrep som trussel på statssikkerheten har NATO og Norge ulike syn på dette. Norge fokuserer på tap av menneskeliv eller skade på materiell, mens NATO på sin side knytter angrep til trussel mot territoriell integritet, politisk uavhengighet eller sikkerheten til en av partene (FDs cyberretningslinjer, 2014, s. 15; NATO, 2010, s. 4, pkt 12). Ordlyden i NATOs strategiske konsept punkt 12 tilsvarer teksten i artikkel 4 i *Traktat for det nord-atlantiske område* (The Washington Treaty, 1949), og ved et cyberangrep kan en av partene be de andre om konsultasjon[25]. Hvis en nasjon ønsker å iverksette artikkel 5 i selvforsvar må alle være enige. Innenfor cyber er ikke denne terskelen definert. Med mulighet for konsultasjon viser NATO evne til å møte trusselen hos medlemslandene. Sikkerhetspolitisk kan det bidra til å avskrekke aktører fra å gjennomføre angrep.

Konsultasjon i seg selv skaper ingen motreaksjon. NATO kan virke svak hvis cyberangrep bare fører til konsultasjon og ikke handling. Dette kan brukes av andre for å skape splid mellom medlemslandene. Det uforutsigbare gjør det vanskelig for en aggressor å tilpasse egne virkemiddel. Prediktere konsekvens av egne handlinger/angrep.

Mellom Norge og NATO er det en markant forskjell på når cyberangrep løftes til politisk nivå. Ved en lavintensitets konflikt eller cyberhendelser over tid kan den norske tolkningen stå overfor

[24] Oppsummering fra workshop 15. apil 2015
[25] NATO traktaten hentet fra http://www.nato.int/cps/en/natohq/official_texts_17120.htm, den 5. april 2015

det som Richard Clarke beskriver som «Death by thousand cuts[26]» (Rosenbaum, 2012). Med dette menes at små handlinger over tid som for eksempel spionasje kan utfordre nasjonens selvstendighet og inntjening, ved at politiske og økonomiske hemmeligheter flyter ut av landet.

Et strategisk overfall av en del av Norge vil sette politikerne på prøve på hvor mye risiko de ønsker å utsette Forsvaret for i den hensikt å avverge eller slå tilbake. Et slikt overfall uten tap av menneskeliv setter definisjonen av angrep på prøve og det blir uansett en politisk beslutning som må fattes på hvilken tilstand nasjonen skal være i. NATO sin definisjon gir rom for å erklære væpnet konflikt på et tidligere stadium eller basert på andre kriterier.

Det er også interessant å se på USA. USA er både stormakt og medlem av NATO. Litteraturen sier lite om hva slags cyberangrep som kan regnes som krigshandling mot USA. David S. Yost påstår at USA har til gode å definere cyberangrep som krigshandling (Yost, 2010, s. 519). I 2011 utga USA International Strategy for Cyberspace (The White House Office, 2011). Her bekreftes at cyberangrep kan gi rett til selvforsvar etter FN-pakten, men strategien definerer ikke hvilke typer angrep eller effekter som vil utløse denne retten. Under avsnittet avskrekking i strategien beskrives at cyberangrep kan bli møtt med alle nødvendige midler (The White House Office, 2011, s. 13). For å utlede en grense kan hendelsene mot Sony Pictures høsten 2014 brukes som bakteppe. Sony Pictures ble utsatt for både datainnbrudd, offentliggjøring av stjålet informasjon og sletting av servere[27]. I tillegg ble det fremført fysiske trusler mot de kinoene som ønsket å vise filmen. Alle hendelsene var i forbindelse med premiereforberedelser for filmen The Intervju[28]. Hendelsene ble sikkerhetspolitikk for USA, og Nord-Korea anklaget deretter USA for å forstyrre landets internettforbindelser (Fackler, 2014). Dette viser at USA har en grense for å iverksette mottiltak som er mer i tråd med NATO enn med Norge. På en annen side er USA en stormakt som følger noen nasjoner mer nøye enn andre. Hendelsene i Sony Picture passet inn i et definert fiendebilde, og kan dermed ha vært med på å senke terskelen for motangrep. Det er uansett vanskelig for en aggressor å utlede konsekvenser av egne handlinger. Denne usikkerheten kan ha en avskrekkende effekt.

[26] Sitat "Alexander referred to the growing number of hacking incidents targeting US technology and corporate trade secrets as 'death by a thousand cuts.'" Hentet fra http://www.hstoday.us/focused-topics/cybersecurity/single-article-page/us-facing-death-by-a-thousand-cuts-in-cyberspace/4ac6f26957f17cafb8611b6fa5899622.html, den 7. mai 2015
[27] Hentet fra http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts, 13. mai 2015
[28] Komedien The Intervju handler om amerikanske journalister som forsøker et attentat på Nord-Koreas leder Kim Jong-un (http://www.imdb.com/title/tt2788710/, hentet 12. mai 2015)

Sjefen for National Security Agency (NSA) Admiral Mikael Rogers har pekt på den amerikanske energisektorens infrastruktur som en akilleshæl[29]. Underforstått at denne er et sårbart punkt med stor konsekvens. Et angrep her kan føre til motaksjoner. Tyrkia har opplevd et større nasjonalt strømbrudd. Selv om media spekulerte, ble det ikke offentlig pekt på et cyberangrep(Senel, Hirsti, & Bruland, 2015).

Et cyberangrep er en menneskeskapt krise og en villet handling av en angriper. Cyberangrep favoriserer angriper med tanke på attribusjon. Et væpnet angrep som fyller kriteriene utløser rett til selvforsvar. Dette medfører at det må være en annen part. Attribusjon handler om å peke ut den som står bak. Det er alltid noen bak menneskeskapte kriser. Noen i den fysiske verden kan knyttes til cyberangrepet. Cyberdomenet gir mulighet for å opptre både anonymt og til å skjule opprinnelsessted. Direkte attribusjon til en nasjons offentlig kontrollerte virksomheter kan være vanskelig. En indirekte metodikk kan benyttes mot en nasjon hvor opprinnelsessted er bekreftet å være innenfor nasjonens grenser. Det diskuteres internasjonalt om en nasjonen kan gjøres medansvarlig vis den ikke iverksetter tilstrekkelige tiltak for å hindre et cyberangrep (Dokument 8:147S (2011-2012), 2012).

Avslutningsvis en vurdering om cyberangrep kan være et væpnet angrep alene eller om cyberangrep er en del av en militær operasjon. Som forklart i kapittel 2, argumenterer Clarke med at potensialet er på plass for å skape stor effekt. For å plassere alvorligheten som cyberangrep kan forårsake benyttes begrep som 'Cyber 9/11' og 'Cyber Perl Harbor' (R. A. Clarke & Knake, 2010). I dette ligger det at nasjoner har rett til å svare i selvforsvar. Rid på sin side mener at effekten av cyberangrep oppnås ved sabotasje, spionasje og subversjon. Og at en cyberkrig ikke vil være sannsynlig (Rid, 2011). Empiriske data fra de siste tiårene fra Estland i 2007 til Ukraina støtter Rid sin påstand. Cyberangrepen mot Estland i 2007 og Georgia i 2008 var en kombinasjon av Denial of Service (DoS) og Distributed Denial of Service (DDoS)[30] angrep, endring av web sider og offentliggjøring av e-postadresser (Tikk et al., 2008, s. 7). Det siste for å tilrettelegge for massiv spam av epost kontoer og for å kunne sende mail med virus. Clarke har også endret syn og uttaler at spionasje er en større trussel mot nasjonene enn et eventuelt 'Cyber Perl Harbor' (Rosenbaum, 2012). Intervju med UD bekrefter at ingen nasjoner så langt har tatt til orde for diplomatiske reaksjoner som følge cyberangrep[31]. USA sitt antatte

[29] Hentet fra https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf, den5. mai 2015
[30] DoS og DDoS er tjenestenekt og distribuert tjenestenekt
[31] Svar fra UD på intervjuforespørsel 12. mai 2015

motangrep på Nord-Korea kan være eneste eksempel på bruk av selvforsvar som svar på et cyberangrep.

3.1 Delkonklusjon

I ytterste konsekvens kan summen av eller et enkelt cyberangrep gi rett til selvforsvar etter FN paktens artikkel 51. Konsekvens og alvorlighetsgrad må være stor. Selvforsvar krever at angrepet kan attribueres til en nasjon. Som beskrevet i kapittel 2 er attribusjon en utfordring i cyberdomenet.

Den norske tolkningen av rett til selvforsvar ved cyberangrep gir to utfordringer. For det første bør norsk militær bruk av termen cyberangrep justeres for å passe med den allmenne bruk av ordet. I stedet for å skille mellom cyberangrep og cyberoperasjoner bør alvorligheten ved cyberangrep graderes. Et cyberangrep så alvorlig at det medfører tap av liv eller materielle skader kan gi rett til selvforsvar, kan være et tilpasset alternativ til teksten i dagens beskrivelse.

Den andre utfordringen ligger i hva som skal til før sikkerhetspolitiske virkemiddel benyttes. Når det kommer til rett til selvforsvar er det forskjell på hva Norge legger i alvorlighetsgrad av et cyberangrep, og hva NATO og USA legger til grunn for å reagere. En udefinert grense for hva som kan være en krigshandling kan virke avskrekkende på en aggressor. Den klart definerte grensen som Norge har satt, kan utfordres ved å gjennomføre cyberangrep som er under denne terskelen.

Det kan ikke sannsynliggjøres at cyberangrep vil være et væpnet cyberangrep alene. Det mest sannsynlige er cyberangrep som en del av flere virkemidler i en militær operasjon. Empiri fra de siste ti årene understøtter denne observasjonen.

4 Væpnet konflikt med cyberangrep

Tidligere i oppgaven er ulike former for cyberangrep beskrevet. Forrige kapittel viser at visse typer cyberangrep i sum eller alene kan gi rett til selvforsvar etter FN paktens artikkel 51. Forutsetningen er at angrepet kan attribueres til en nasjons myndigheter. Oppsummering om cybertrusselen og erfaring med cyberangrep så langt tilsier at trusselen er størst innenfor sabotasje mot kritisk infrastruktur, spionasje og ulike elementer innenfor informasjonsoperasjoner. Derfor vil dette kapittelet analysere en væpnet konflikt som har militære angrep både i det fysiske domenet og i cyberdomenet. Hendelser i det fysiske domenet benyttes kun for å sette en ramme rundt konflikten. Fokus er på hvordan organisasjonen påvirker krisehåndteringen av en væpnet konflikt.

4.1 Casestudie – Strategisk overfall med tilhørende cyberangrep

Casestudien er et strategisk overfall mot Finnmark. Et strategisk overfall er når en stat angriper begrensede geografiske områder av et lands territorium, med mål om å fremtvinge politisk endring i det landet de angriper (Johansen, 2010). Ofte bruker man uttrykket «krigslignende handlinger» om et strategisk overfall. For å belyse hvor alvorlige konsekvensene av en slik hendelse kan bli, er det gjennomført en analyse av et spesifikt scenario hvor en fremmed stat okkuperer strategiske punkter i Norge.

Litteraturstudien viste hvem som har ansvar for de ulike delene av krisehåndteringen. Casestudien presenteres først, og deretter analyseres den for å se om krisehåndteringen er som forventet i henhold til teori. De forhold som analyseres er totalforsvarskonseptet, forebygging, kriseledelse og samvirke. Totalforsvarskonseptet er grunnlaget for den gjensidige støtten mellom sivil og militær side i en væpnet konflikt. Forebygging er både beskrevet i teori innenfor cybersikkerhet og menneskeskapte kriser. Kriseledelse er vår evne til å lede og gjennomføre krisehåndtering. Til slutt analyseres samvirke. Dette er det fjerde prinsippet for nasjonal krisehåndtering.

Norge og Russland har i flere år hatt diplomatiske forhandlinger om rettigheter i nordishavet. Etter hvert som isen smelter i polhavet ønsker begge nasjoner å ta ledelse på den økonomiske utviklingen i området både innenfor skipsfart samt tilgang til olje og gass. Norge planlegger utbygging av de nye oljefeltene som er funnet nord øst for Svalbard. Russland hevder at disse områdene tilhører dem.

Etter en tid med spenning mellom nasjonene besetter Russland deler av Øst-Finnmark, og kontrollerer med dette oljeindustriens fasiliteter på land for Barentsregionen. Regjeringen samles

og konstaterer at Norge er under angrep i henhold til grunnlovens § 26 (Forsvarets høgskole/Forsvarets stabsskole, 2013, s. 8; Grunnloven, 1814). Regjeringens kriseråd samles ved slike alvorlige hendelser, og det understøttes av krisestøtteenheten (KSE) [32]. KSE har et døgnbemannet situasjonssenter og er underlagt JD. Ved behov yter enheten støtte til lederdepartementet og kriserådet i deres krisehåndtering. Forsvarets kommandostruktur settes på krigsfot. Situasjonssenteret i Forsvarsstaben (SITSEN) er på strategisk nivå. Og Fellesoperativt hovedkvarter (FOH) er på operasjonelt nivå. Under dette nivå ledes det på ulike taktiske sjefer i den militære strukturen.

Samtidig med den russiske offensiven inn i Øst-Finnmark iverksettes en større cyberoperasjon mot norsk kritisk infrastruktur. Et cyberangrep mot Telenors transportnett for elektronisk kommunikasjon fører til at sentrale tele- og datanett faller ut[33]. Angrepet oppdages teknisk av CERT miljøet i Telenor som rapporterer dette til NorCERT. Videre rapporterer både Avinor og Forsvaret om flyaktivitet som ikke fanges opp på hverken militære eller sivile bakke til luftradarer. I dette tilfellet er det ikke detektert at det er skadevare i systemet. En fysisk observasjon av avvik mellom det tekniske systemet og virkeligheten, medfører at Forsvaret og AVINOR blir oppmerksomme på cyberangrepet. Forsvaret vil bruke BKI i Cyberforsvaret til å se etter avvik i systemene. Avinor benytter egen driftsavdeling i søk etter avvik. Nettavisene til Aftenposten og VG har på morgenen artikler om en mislykket aksjon av den norske kystvakten. Artiklene beskriver at kystvakten senket et russisk forskningsfartøy og at det antas at over 50 russere omkom. Det tredje cyberangrepet er som del av en del av informasjonsoperasjoner mot Norge. Dette cyberangrepet er mot websider og servere. Websider endres for å presentere et annet budskap. Servere angripes for å slette informasjon eller ødelegge tilgang til informasjon. Et slikt angrep er subversjon og vil være et anliggende mellom virksomheten selv og politiet. Angrepet gjennomføres mot en virksomhet i et land som er i væpnet konflikt.

4.2 Totalforsvarskonseptet

Publikasjonen *Støtte og samarbeid* skal bidra til å forankre gjeldende totalforsvarskonsept i sivil og militær sektor (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2015). I innledningen vektlegges at både sivil og militær sektor bør har god kunnskap om gjeldende ordninger og mekanismer for sivilt-militært samarbeid. Derfor er gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn grunnleggende for ivaretakelsen av både

[32] Hentet fra https://www.regjeringen.no/nb/dep/jd/org/avdelinger/kbs/kse/id709278/, den 3. mai 2015
[33] Setning endret fra "Telenors transportnett for elektronisk kommunikasjon tas ut i Troms og Finnmark, samt nordlige deler av Nordland» av deltagerne på workshop 15. april. Kort oppsummert er det at fysisk bortfall i deler av nettet vil være en konsekvens av en fysisk handling (koble fra).

samfunnssikkerhet og statssikkerhet. Totalforsvarskonseptet setter dermed rammer for utvikling av samarbeidet.

I denne casestudien har Forsvaret fått sin rolle definert. Den sivile sektor støtter opp under Forsvaret sine oppgaver. Konseptet er ikke verktøy for kriseledelse, men det er med på å skape forutsetninger for samarbeid. Forberedelser i fredstid forbereder det sivil-militære forholdet. Totalforsvarskonseptet skaper forutsetning for praktisk utførelse av tiltak på alle nivåer.

Det er to sivil-militære fora som kan knyttes til totalforsvarskonseptet. Sentral totalforsvarsnemd representerer bredden i totalforsvaret (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2015). Forumet samles jevnlig og har bred representasjon fra offentlig sektor. Ledervervet går på rundgang mellom sjef Fellesoperativt Hovedkvarter og sjef Direktoratet for sivil beredskap. Forumet bidrar til orientering, samordning og overordnet koordinering innenfor sivilt-militært, samarbeid, beredskap og samfunnssikkerhet. I en væpnet konflikt har de fortsatt en rolle som koordinerende forum, men ikke knyttet til daglige utfordringer. Cyberkoordineringsgruppen (CKG) er den andre. Denne gruppen er koordineringsansvarlig for EOS tjenestene. E-tj, PST og NSM er faste medlemmer i denne gruppen (FDs cyberretningslinjer, 2014, s. 10). Ved alvorlige hendelser vil en av dem være koordineringsansvarlig. CKG har ikke beslutningsmyndighet (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2015, s. 61).

Teorien beskriver at totalforsvarskonseptet skal danne grunnlag for sivilt-militært samarbeid. Det forventes av Forsvaret skal ta ledelsen ved en alvorlig krise. Deltagerne på den tversektorielle workshopen bekreftet denne forståelsen[34]. Totalforsvarskonseptet beskriver sivilt-militært samarbeid generelt og gir mulighet for å etablere samarbeid. Sentralt totalforsvarsforum og CKG er begge i offentlig sektor, og koordinerer aktiviteter innenfor departementenes ansvarsområder.

I diskusjonsrunden under FFI Forum[35] på OMS ble det kommentert at etter Afghanistan vil Forsvaret igjen stille krav til totalforsvaret. Dette med bakgrunn i fokus på tilstedeværelse i egne grenseområder i Nord-Norge, og de behov som Forsvaret må ha dekket av andre for å ha evne til stridsutholdenhet innenfor alle dimensjoner. Den sivile støtten som Forsvaret har behov for ved væpnet konflikt er ikke øvd og like mye vektlagt de siste tiårene. Mye av tankegodset knyttet til denne dimensjonen ser ut til å ha blitt gradvis redusert siden slutten på den kalde krigen

[34] Oppsummering etter tverrsektoriell workshop15. april 2015
[35] FFI-forum: Krisehåndtering i cybersamfunn, 25. november 2014

Tiltak som gjennomføres i fredstid mellom sivile og militære aktører bidrar til å øke samarbeidet. Tiltak gjennomført forut for væpnet konflikt påvirker evnen til å gjennomføre krisehåndtering. Den gjensidige støtten og samordningen mellom Forsvaret og det sivile samfunn er bærebjelken i totalforsvarskonseptet. Totalforsvarskonseptet skal bidra til å effektivisere ressursinnsatsen på nasjonalt nivå ved en alvorlig krise og i krig. Etter den kalde krigens slutt er konseptet modernisert og beredskapslovgivningen er ikke lenger en forutsetning for at støtten skal tre i kraft (Forsvarsdepartementet, 2009). Det utvidete totalforsvarskonseptet ble også berørt i Forsvarssjefens årlige tale i OMS (Admiral Haakon Bruun-Hanssen, 2015):

«*Det er politiets ansvar å forebygge og beskytte oss mot terror. Forsvarets største bidrag i kampen mot terror er å hindre deres utvikling i egne kjerneområder med militære intervensjoner og militær støtte til politiet her hjemme.»*

Uttalelsen viser at totalforsvarskonseptet ikke er glemt, men den viser også at det fokuseres på fredstidsoppgavene. Forsvaret forventes å støtte det sivile samfunn, men dette er ikke dimensjonerende for forsvarets strukturutvikling. Samarbeid med politiet gir Forsvaret nyttig erfaring og innsikt i samfunnssikkerhetsperspektivet. Bistand til politiet reguleres av bistandsinstruksen. Bistandsinstruksen gir to muligheter for bistand fra Forsvaret til det sivile samfunn. Den ene er alminnelig bistand og den andre er håndhevelsesbistand. Alminnelig bistand gis formelt gjennom Forsvarets operative hovedkvarter (FOH) (Instruks om Forsvarets bistand til politiet, 2012). Håndhevelsesbistand er den andre formen for bistand. Formell beslutningskjede er fra politiet til Justisdepartementet (JD) og deretter til Forsvarsdepartementet (Instruks om Forsvarets bistand til politiet, 2012). FD gjør en helhetlig vurdering av bistandsanmodningen, og kan fatte en beslutning som både ivaretar en generell sikkerhetsvurdering og avveining av samtidighetsproblematikk. Skal bistand ytes gir FD et formelt oppdrag til Forsvaret om å stille med bistand, samt nødvendige retningslinjer til Justis- og beredskapsdepartementet. I hovedsak gis støtte til politiet av Heimevernet og andre enheter som kan gjøre en fysisk innsats. Støtte fra Forsvaret innenfor området cybersikkerhet ble øvd på øvelse Cyber Down i 2013[36]. Forsvaret kan støtte på mange områder, men det mest aktuell er kompetanse. Forsvaret har både kompetanse til å bistå med sikring av bevis ved hendelser i cyberdomenet, og til å være rådgiver ved cyberangrep mot en sivil virksomhet.

[36] Hentet fra http://www.telenor.com/no/media/pressemeldinger/telenor-over-pa-cyberkrise/, den 15.mai 2015

I mars 2015 ble politiloven endret og godkjent i statsråd[37] (Prop. 79 L (2014-2015), 2015). Loven omhandler Forsvarets støtte til politiet, og angir yttergrensene for Forsvarets potensielle maktbruk. Cyberdomenet omtales ikke i lovteksten hverken knyttet til grensedimensjonen eller til beskyttelse av kritisk infrastruktur. Kystvakten og grensevakten mellom Norge og Russland omtales som eksempler på områder hvor Forsvaret kan bruke makt. Politiloven setter grenser for utvikling av samarbeid innenfor cybersikkerhet.

De etablerte fora dekker kun offentlig sektor. Den sivile delen av samfunnet er større. Sentralt totalforvarsforum er et forum på strategisk nivå, og som ikke er organisert for å ivareta et spesifikt fagområde. I sin tale til Oslo Militære Samfund (OMS) etterlyste sjef Cyberforsvaret reetableringen av totalforsvarets sambandsnemnd (Generalmajor Odd Egil Pedersen, 2015). Denne ble nedlagt i 1998 og han ser det som naturlig at Nasjonal Kommunikasjonsmyndighet (NKOM) tar ansvar for prosessen. Samband og Cyber er ikke identiske områder. NKOM har en naturlig rolle for oppfølging av elektroniske kommunikasjonsløsninger (EKOM). For cyberdomenet er det behov for at noen andre tar ledelsen. DSB har en rolle for nasjonal koordinering av beredskapsplaner, og er samtidig overordnet Sivilforsvaret. Sivilforsvaret har ingen kapasitet i det digitale rom. NSM er en annen aktør, men er kun faglig ansvarlig for informasjonssikkerhet. Til slutt er det Forsvaret som er ansvarlig for statlig maktutøvelse og statssikkerheten. I cyberdomenet har Forsvaret ansvar for egen infrastruktur. Et cyberråd må ledes av en av etatene eller virksomheten med ansvar innenfor cyberdomenet.

4.3 Forebygging

I denne casestudien handler forebygging om de tiltak som er iverksatt før det ble en væpnet konflikt. Hver enkelt av aktørene forbereder seg innenfor sin virksomhet. Menneskeskapte kriser som cyberangrep kan både forebygges gjennom beredskapsplaner og robuste nettverk i det digitale rom. Justis- og beredskapsdepartementet er ansvarlig for tilsyn av departementenes arbeid med samfunnssikkerhet og beredskap. DSB understøtter departementet i utøvelsen av denne rollen (Direktoratet for samfunnssikkerhet og beredskap, 2015).

Å forebygge i det digitale rom eller cyberspace er vanskeligere enn i det fysiske rom. En nasjonalstat kan bruke sympatisører eller andre tredjeparter til å gjennomføre cyberangrep, eller bruke infiserte datamaskiner i et tredjeland. Ulike grupperinger, kriminelle og terrorister kan være aktuelle globale aktører. Etterretningstjenestens årsrapport (Etterretningstjenesten, 2015) beskriver at nasjoner som Russland og Kina satser store beløp på å utvikle sine cyberkapasiteter.

[37] Tilråding fra Justis- og beredskapsdepartementet 27. mars 2015, godkjent i statsråd samme dag. (Regjeringen Solberg). Hentet fra https://www.regjeringen.no/nb/dokumenter/prop.-79-l-2014-2015/id2402973/, den 8. mai 2015

Forebygging av cyberangrep handler både om å lage et så robust forsvar som mulig og etablere informasjonsdeling mellom de ulike aktørene. Et robust forsvar forebygger cyberangrep til en viss grad. Hvis sikringen i det digitale nettverk er optimalisert og uten store svakheter skaper det utfordringer for en angriper. Robusthet er i enkleste forstand å ha oppdatert programvare og følge produsentenes råd om å gjøre sikkerhets endringer. I tillegg kommer beskyttelse som brannmurer og antivirusprogrammer. NorCERT i NSM drifter varslingssystem for digital infrastruktur (VDI). VDI bidrar til å detektere uønskede handlinger hos dem som deltar i samarbeidet. Sensorene i VDI bidrar til å øke robustheten i nettverkene, og hever terskelen for et mulig cyberangrep. Fra det fysiske domenet viser historien at festningsverk og ulike hindre er vanskeligere å passere enn åpent lende. Cyber Kill Chain® er en metode for å beskytte mot APT angrep. Ulike faser av angrepet kan påvirkes, og det mest effektive er mot rekognoseringsfasen.

Informasjonsdeling er viktig i relasjon til forebygging. Både for å ha en god evne til hendelseshåndtering (Incident Repsonse) og for å ha en mulighet for kompetanseheving og erfaringslæring (Best Practice). Informasjonsdeling for hendelseshåndtering skjer på flere nivåer og mellom ulike aktører. Det er naturlig at de ulike Computer Emergency Response Team (CERT) utvikles til å bli en tverrsektoriell og konfidensiell informasjonsgruppe sammen med nasjonal CERT. Dette er miljøer med døgnkontinuerlig drift- og overvåkningskapasitet. I et slikt samarbeid er det naturlig at Forsvarets CERT miljø inngår.

Bedrifter, etater og institusjoner i offentlig og privat sektor utgjør neste nivå på informasjonsutveksling. Disse er knyttet opp mot hver sin sektor CERT, som for eksempel KraftCERT og FinansCERT. Informasjonen som tilflyter gruppens medlemmer må være konkret og spesifikk opp mot gjeldende trussel.

På laveste nivå er små og mellomstore bedrifter, utdannings- og utviklingsmiljøer samt privatpersoner. Disse faller naturlig utenfor et informasjonsnettverk, men noen av disse har stor tillitt i samfunnet og kan dermed være et mål for noen som ønsker adgang til en tredjepart. For å beskytte nasjonale verdier er det fra et statsperspektiv viktig at flest mulig inngår i et informasjonsnettverk eller en informasjonsgruppe. Dette sikrer at informasjon og eventuelt oppdateringer på programvare kan flyte ned til de som har behovet. Deltagelse i en slik gruppe kan være frivillig eller at det reguleres med tvangsmidler fra statlig side. Utfordringen ligger i mangfoldet på dette nivået. Useriøse aktører må kunne sanksjoneres ut av gruppen basert på kriterier. Både kriminelle og utenlandske aktører kan ha interesse av å ha kontroll på noe av aktørene her. Og fra statlig side er det viktig å minske risikoen for at de kan bli en del av

trusselen. Nasjonal forebygging i cyberdomenet handler dermed om å iverksette prosesser som ivaretar både dette og informasjonsdeling.

Informasjonsdeling for erfaringer (Best Practice) gjøres av ulike aktører nasjonalt og internasjonalt. Når det gjelder forebygging og informasjonsdeling er det en del nasjonale og internasjonale aktører. I Norge er det to sentrale aktører. Den ene er Norsk senter for informasjonssikring (NORSIS) arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat (NORSIS, 2015). Center for Cyber and Information Security (CCIS) er den andre aktøren. Senteret har mandat om å styrke samfunnets kompetanse og ferdigheter til å beskytte, å oppdage, å respondere samt å etterforske uønskede og kriminelle handlinger[38]. I Europa er European Union Agency for Network and Information Security (ENISA) et nav i utveksling av informasjon, 'Best Practice' og kunnskap. Forum of Incident Response Teams (FIRST) er en global interesseorganisasjon. Denne har ti norske medlemmer inkludert NorCERT (Forum of Incident Response and Security Teams, 2015). Fi-ISAC er etablert som et offentlig-privat samarbeid i Europa. Dette er et organ hvor bankvirksomhet, nasjonale CERT miljøer og juridiske etater jobber sammen mot cyber-kriminalitet.

Forebygging mot informasjonsoperasjoner er en utfordring. Cyberangrep i informasjonsoperasjoner brukes for å påvirke mennesker. Det er derfor en teknisk og menneskelig dimensjon knyttet til forebygging. NRK reportasjen «Slik trener Norge på cyberkrig[39]» presenterte et likt cyberangrep som i casestudien. Reportasjen i NRK beskriver i detalj rekkefølgen på de ulike komponentene i angrepet. Politisk vilje til å forsvare Norge med tilstrekkelig med ressurser kan påvirkes. Erfaringer fra Ukraina konflikten viser at slike informasjonsoperasjoner gjennomføres (Franke, 2015). Hvis falske websider eller manipulerte websider er det første som møter den vanlige innbygger en morgen, så vil innholdet i nyhetene feste seg raskt. Hvis disse inneholder feilinformasjons vil det fra politisk og medias side ta lang tid å endre den oppfattelsen som har satt seg. Den falske Twitter meldingen i 2011[40] om President Obamas død spredte seg raskt, og det ble iverksatt offisielle tiltak. Til tross for dette ble det raskt store bevegelser på børsen.

Forebygging for slike sammensatte angrep handler om å inkludere større deler av samfunnet. Informasjonsoperasjoner er ikke angrep på kritisk infrastruktur eller styringssystemer. Få

[38] Hentet fra http://www.slideshare.net/GryHeleneStavseng/ccis-brosjyre-norsk-nov-2014-reducedversionnorsk, den 7. mai 2015
[39] Hentet fra http://www.nrk.no/norge/slik-trener-norge-pa-cyberkrig-1.12317682, den 21. april 2015
[40] Hentet frahttp://www.theguardian.com/news/blog/2011/jul/04/fox-news-hacked-twitter-obama-dead, den 5. mai 2015

mediekonsern eller mediehus er en del av VDI samarbeidet til NorCERT, eller inngår i andre CERT/CSIRT miljø. Dette er bedrifter med antatt lav eller ingen «verdi» for andre. Nyheter er ferskvare, og det er begrenset med bedriftshemmeligheter i slike bedrifter. Mediehus er derimot aktuelle mål som tilgangspunkt mot andre aktører. Mange av mediehusene nyter stor respekt i samfunnet generelt, og data som kommer fra serverne deres antas å være sikre. En mail med virus eller skadevare skjult i vedlegg vil sannsynligvis bli åpnet av mottager. Slik trenger det ikke være. I tillegg er det en del mediehus som forvalter en sannhet som befolkningen har tiltro til. Dette er tradisjonelt sett NRK som tidligere statskanal på TV siden, samt aviser som blant annet Aftenposten, Dagbladet og VG. Cyberoperasjoner mot disse for å presentere manipulert informasjon eller anti-nasjonal informasjon vil være meget sannsynlig i en konflikt. Skadeomfanget vil være stort ut fra hvilken tiltro befolkningen har til disse aktørene.

I Norge er det kun NRK som er tilknyttet cybersikkerhetsmiljøet, og er nå en del av VDI samarbeidet. NRK kunne ikke ta risikoen for at deres servere blir brukt som videreformidler av et cyberangrep. I diskusjonen forut ønsket ikke journalistene dette samarbeidet, og argumenterte med beskyttelse av sine kilder[41]. På en annen side bør medier ha sikkerhet for å utøve sin uavhengige rolle (Matlary, 2015).

Norge og andre nasjoner må forvente en viss grad av pågående informasjonsoperasjoner til enhver tid, også i fredstid. Ved sikkerhetspolitisk krise og væpnet konflikt må det forventes at antall angrep øker. Erfaring fra konflikter de siste 10-årene viser dette (McMahon, 2014). Det må derfor iverksettes vel koordinerte anti-informasjonsoperasjoner og anti-subversjons tiltak. Disse tiltakene må være forhåndplanlagt, og ansvar må tillegges en nasjonal aktør.

Konsekvensene av et slikt cyberangrep er store. Medier som virksomhet har sitt beskyttelsesnivå, men er ikke en aktiv part i nasjonalt cybersikkerhetsmiljø. Fiendtlig påvirkning gjennom slike cyberangrep kan skape usikkerhet i befolkningen, påvirke beslutningstakere og bidra til nedsatt samfunnssikkerhet. Det siste ved å skape kaos ved hjelp av kommunikasjon gjennom media.

Litteraturstudien ga ingen klare svar på hvem som har nasjonalt ansvar for å øke robusthet i nettverkene. Ansvaret blir dermed liggende hos den enkelte etat eller virksomhet i offentlig og privat sektor. Noen nasjonale aktører er tillagt tverrsektorielt ansvar knyttet til forebygging. DSB utfører kontroll av beredskapsplaner, men kun hos de virksomheter og etater som er pålagt å ha slike. Nasjonal sikkerhetsmyndighet (NSM) er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser. Mens NORSIS skal bidra til å øke

[41] Hentet fra http://www.klassekampen.no/article/20150113/ARTICLE/150119981, den 5. mai 2015

bevisstheten rundt bruk av internett og IKT. Det er få eller ingen som har direkte oppdrag knyttet til forebygging. Et eksempel er politiet som ofte er ute med både informasjon og aktiviteter for å forebygge. Innenfor cyberdomenet er det liten egen aktivitet[42].

4.4 Kriseledelse

Kriseledelse handler om hurtig å etablere evne til å lede andre og fatte beslutninger i en krise. Det første handler om å etablere en ledelsesstruktur med ansvar og myndighet. Evne til å ta beslutninger underbygges av å ha et system som både ivaretar rådgiving og beslutning. Den som tar beslutninger må ha informasjon eller rådgivning.

I denne casestudien tar Forsvarsdepartementet ansvar som lederdepartement og støttes av regjeringens krisestøtteenhet (KSE). KSE støtter med infrastruktur, tekniske løsninger, møtelokaler og personell. KSE har beredskap og er hurtig på plass. Forsvarets struktur for ledelse settes på krigsfot. Først med de som er på jobb, og deretter med ekstra personell. På strategisk nivå leders Situasjonssenteret i Forsvarsstaben (SITSEN). Forsvarets operative hovedkvarter (FOH) leder på operasjonelt nivå. Militære enheter underlagt sjef FOH representerer det taktiske nivået i Forsvarets operative struktur (Forsvarsstaben, 2014, s. 168). Politiet kan ved ekstraordinære hendelser endre ledelsesstruktur slik at en stabssjef overtar ledelsen på operativt nivå. Andre aktører etablerer kriseledelse som beskrevet i beredskapsplaner. Dette er bedrifter, virksomheter og etater som ikke får tilgang på økt bemanning ved krise.

De tre cyberangrepene håndteres mellom ulike aktører. Telenor er en nasjonal aktør med landsdekkende tjenester. Forsvaret samarbeider med Telenor og iverksetter tiltak på cyberangrepet mot elektroniske kommunikasjonsløsninger (EKOM). Telenor CERT og NorCERT samarbeider om hendelseshåndtering av cyberangrepet. De forsøker å finne hva slags cyberangrep som er gjennomført eller som er pågående.

Det andre cyberangrepet krever samarbeid mellom Forsvaret og Avinor. Cyberangrepet mot luftkontrollsystemer eller radarsystemer er sabotasje. Et slikt cyberangrep ble brukt av Israel mot Syria i 2007 under operasjon Orchard[43] (Rid, 2011, s. 16). Cyberangrepet mot syrisk radarsystem gjorde at israelske jagerfly kunne operere uten å bli detektert, og målet for luftangrepet var en antatt syrisk atomreaktor. Hvis en operasjon er viktig nok for en aktør vil han kunne legge ned tilstrekkelig med ressurser for å utvikle et slikt cyberangrep. Angrepet er mot både sivile og militære systemer. Sivil luftaktivitet i dette området er nesten fraværende og Forsvaret utøver

[42] Bekreftet på intervju Kripos 20. april 2015

luftromskontroll. Det sivile systemet kan tas ned i området eller prioriteres lavt. Forsvaret har begrenset med resurser, og BKI settes inn mot egne systemer. Disse er mest kritisk for den militære operasjonen i Finnmark.

Det siste cyberangrepet med mot blir håndtert av virksomheten selv. Hvis de ønsker det kan de anmelde forholdet til politiet. Konsekvensen er at politisk og strategisk ledelse må lage en strategisk kommunikasjonsplan. Denne må søke å dempe konsekvensene av falske og manglende nyhetsmeldinger.

Teori om kriseledelse i Norge beskriver ansvaret til lederdepartement og etablering av regjeringens kriseråd. Alvorlige kriser fører til at regjeringens kriseråd samles for å koordinere mellom sektorene. Beslutninger fattes av departementene i henhold til konstitusjonelt ansvar (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2015). Et militært angrep på Norge medfører at FD settes som lederdepartement. Forsvarets ledelsesstruktur leder sine underlagte enheter og koordinerer sin virksomhet mot relevante aktører. Kommandokjeden til Forsvaret er fast etablert fra fredstid.

Denne casestudien inneholder flere cyberangrep som det må iverksettes tiltak mot. De tiltak som iverksettes må ses i sammenheng med at Norge er utsatt for et pågående strategisk overfall med politiske overtoner. Cyberangrepene må møtes med både krisehåndtering og hendelseshåndtering. Det siste er oppgaver knyttet til taktisk nivå og utføres av de ulike CERT/CSIRT miljøene, samt BKI i Forsvaret.

Krisehåndtering er kriseledelse i organisasjonen innenfor ansvarsområdet, samt rådgivning til beslutningstakerne. Øvelser er en god metode for å forberede seg på kriser og for å trene på samhandling (Fimreite, 2011, s. 160).

4.4.1 Ansvar

Forsvarets rolle og ansvar innenfor krisehåndtering defineres ut fra det strategiske rammeverket. Det strategiske rammeverket er strategier og de oppdragene som gis til etaten. Strategier gir føringer på områder som skal vektlegges i tiden fremover. Norge har i dag[44] ingen nasjonal cybersikkerhetsstrategi. I forordet på Nasjonal strategi for IKT sikkerhet (Departementene, 2012) henvises det til høringsrunden på denne strategien. Av EU nasjonene har 20 av de 28 medlemslandene cybersikkerhetsstrategier på plass (ENISA, 2015). En strategi for cybersikkerhet adresserer sivilt-militært samarbeid i mer detalj.

[43] http://en.wikipedia.org/wiki/Operation_Orchard, hentet 8. mai 2015
[44] April 2015

En cybersikkerhetsstrategi som er overordnet og langsiktig, gir rolleavklaring mellom de ulike aktørene. Dette gjelder både forholdet mellom de offentlige aktørene, mellom offentlig og privat virksomhet, samt mellom sivil og militær sektor. Sivilt-militært samarbeid har to dimensjoner. Den ene er tversektoriell i offentlig sektor, og den andre er mot sivil sektor. Totalforsvarskonseptet beskriver det sivil-militær samarbeidet, og strategien gir føringer på hvordan samarbeidet skal utvikles. Forsvaret er en etat i forsvarssektoren, og er sidestilt med Nasjonal sikkerhetsmyndighet. Forsvarsdepartementet er toppnivå. Andre offentlige aktører innenfor cybersikkerhet er Samferdselsdepartementet med Nasjonal kommunikasjonsmyndighet (NKOM), Justis- og beredskapsdepartementet med Politidirektoratet, Kripos og Direktoratet for sivil beredskap (DSB). I tillegg kommer private virksomheter med ansvar for kritisk infrastruktur. Dette er blant annet Telenor, Statoil og Statnett. Kritisk infrastruktur i Norge er nesten bare eid av private virksomheter (Friis, 2015). Disse virksomhetene er i varierende grad under nasjonal kontroll. Flere har en kritisk rolle ved en væpnet konflikt. Staten er medeier i flere, men det er en politisk diskusjon om staten skal selge seg ned. Selv om den politiske diskusjonen fokuserer på statlig eierskap generelt, er det kritiske røster til å selge seg ned (Lindeberg, 2015). Det argumenteres med at mulighet for nasjonal styring og koordinering kan svekkes ved en annen eierstruktur. En strategi vil beskrive hvordan alle disse skal samarbeide. Både internt i offentlig sektor og eksternt.

I mangel av en egen cybersikkerhets strategi må deler av området ivaretas av Nasjonal strategi for informasjonssikkerhet (Departementene, 2012). Dokumentet er utgitt av fem departementer i fellesskap. Disse er Fornyings- administrasjons- og kirkedepartementet, Forsvarsdepartementet, Justis og beredskapsdepartementet og Samferdselsdepartementet. Cyberangrep som spionasje mot private og offentlige interesser dekkes av en nasjonal strategi for informasjonssikkerhet. Spionasje fremheves av både E-tj og PST sine rapporter for 2014 (Etterretningstjenesten, 2015; Politiets sikkerhetstjeneste, 2015). Begge disse beskriver pågående og avanserte etterretningsoperasjoner mot norske interesser fra blant annet Russland og Kina.

Etablering av en strategi for informasjonssikkerhet uten å ta hensyn til cybersikkerhet gir noen konsekvenser. Strategien beskriver at tiltak på identifisert kritisk infrastruktur skal gjennomføres, men disse tiltakene er ikke sett opp mot tiltak på annen kritisk infrastruktur. Strategien er et steg i riktig retning. Men den etterlater spørsmål om hvilken prioritering andre deler av cybersikkerhet har.

Den største utfordringen ved ikke å ha en cybersikkerhetsstrategi, er den manglende sammenhengen mellom all kritisk infrastruktur. Strategi for informasjonssikkerhet ivaretar kun

kritisk infrastruktur som håndterer digital informasjon i cyberdomenet. Kritisk infrastruktur som består av industrielle styringssystemer (SCADA-systemer[45]) er utelatt. Cyberangrepene Dragonfly/HAVEX mot energisektoren i Norge sommeren 2014, var rettet mot SCADA-systemer. Sabotasje mot SCADA-systemer kan gi materielle ødeleggelser som konsekvens. Både spionasje og skadevare som Dragonfly/HAVEX kan detekteres av VDI-samarbeidet til NorCERT, og av andre CSIRT/CSERT kapasiteter i Norge.

Oppdragene påvirker også evnen til å utføre kriseledelse. Forsvarets ansvar for kriseledelse er sterkt knyttet til de tildelte oppgavene. Oppgavene til Forsvaret består av noen overordnede og relativt varige oppgaver utledet av norske sikkerhetspolitiske målsettinger[46], samt noen mer konkrete oppgaver med kortere varighet.

De ni relativt varige oppgavene til er listet både hos FD[47] og beskrevet i gjeldene Forsvarets fellesoperative doktrine (FFOD) (Forsvarsstaben, 2014, s. 31). Disse oppgavene er:

1. *Utgjøre en krigsforebyggende terskel med basis i NATO-medlemskapet*
2. *Forsvare Norge og allierte mot alvorlige trusler, anslag og angrep, innenfor rammen av NATOs kollektive forsvar*
3. *Avverge og håndtere episoder og sikkerhetspolitiske kriser med nasjonale ressurser, herunder å legge til rette for alliert engasjement om nødvendig*
4. *Sikre et nasjonalt beslutningsgrunnlag gjennom tidsmessig overvåking og etterretning*
5. *Hevde norsk suverenitet og suverene rettigheter*
6. *Ivareta myndighetsutøvelse på avgrensede områder*
7. *Delta i flernasjonal krisehåndtering, herunder fredsstøttende operasjoner*
8. *Bidra til internasjonalt samarbeid på det forsvars- og sikkerhetspolitiske området*
9. *Bidra til ivaretakelse av samfunnssikkerhet og andre sentrale samfunnsoppgaver*

Noen av disse er rene nasjonale oppgaver som må løses internt, mens andre er oppgaver som løses sammen med våre allierte innenfor NATO rammen. Eksempel på det siste er oppgaven om deltagelse i flernasjonal krisehåndtering. Den niende oppgaven er å bidra nasjonalt, men under ledelse av en annen sektor enn forsvarssektoren.

[45] SCADA er forkortelsen for Supervisory Control and Data Acquisition
[46] Ekspertgruppen for forsvaret av Norge, side 60
[47] Hentet fra https://www.regjeringen.no/nb/tema/forsvar/innsikt/mal-og-oppgaver-i-forsvarssektoren/id2009096/ den 5. april 2015

I gjeldende langtidsplan er Forsvaret gitt i konkret oppdrag å drifte en forsvarbar infrastruktur (Forsvarsdepartementet, 2012). FDs Cyberretningslinjer[48] gir oppdrag til Forsvaret som skal løses av Cyberforsvaret. Disse er gjeldende i fred og i væpnet konflikt (FDs cyberretningslinjer, 2014, s. 4). Cyberforsvaret (CYFOR) har fått oppgaven med å beskytte militær kritisk infrastruktur. I Prop. 73S *Et forsvar for vår tid* er avdeling for beskyttelse av kritisk infrastruktur (BKI) oppført som en av Cyberforsvarets kapasiteter. Avdelingen har i oppdrag å overvåke og detektere cyberangrep mot Forsvarets systemer. Den skal også inneha analysekapasitet, og evne til å sende ut underenheter. I tillegg skal den kunne bidra med rådgivning og liaisonering ved angrep på norsk infrastruktur ute og hjemme (Prop. 73 S (2011-2012), 2012, s. 103). Når det gjelder ambisjon for samvirke skal CYFOR koordinere sin eksterne virksomhet med NorCERT (Forsvarsdepartementet, 2012). Dette gjelder både nasjonalt og internasjonalt. Koordinere som begrep erstattet ordet samarbeid i PET 7 til LTP, når det gjelder bistand til sivil sektor ved digitale angrep (Forsvarsdepartementet, 2012, s. 127).

Oppdraget til Forsvaret og Cyberforsvaret er meget klart, men samtidig veldig begrenset i omfang. Omfanget er begrenset til intern virksomhet og egne nettverk. Hverken luft-, sjø- eller landstyrker har samme binding på sin virksomhet. Disse gjennomfører aktivitet og operasjoner i hovedsak på eller i norsk territorium. NSM er den den andre etaten i forsvarssektoren, og den er gitt i oppdrag å varsle og koordinere håndtering av alvorlige dataangrep. Oppdraget, slik teksten kan leses, er ikke et mandat til å opprette et miljø for kriseledelse under cyberangrep. Når det gjelder rådgivning skal både NSM og Forsvaret på forespørsel støtte FDs koordineringsgruppe for informasjonssikkerhet og cyberoperasjoner (KG Cyber) (Forsvarsdepartementet, 2012, s. 49).

Oppdragene til Forsvaret, og NSM, i denne sammenheng sier lite om hvilken myndighet som kan utøves i væpnet konflikt. Omfattende og pliktmessig sivil støtte til Forsvaret ved alvorlig krise og krig hjemles i beredskapslovgivningen (Forsvarsdepartementet, 2009, s. 72). *FDs Cyberretningslinjer* er gjeldende i fred, krise og krig, men dette temaet tas ikke opp. På sikt reduserer dette evnen til å utøve kriseledelse ved cyberangrep som del av en væpnet konflikt. Så lenge dette forholdet er uavklart vil både planer og øvelser være ukomplette med tanke på ledelse og prioritering. For å utøve effektiv bruk av tvangsmidler, som hjemlet i beredskapsloven, må disse øves av riktig enhet på riktig nivå. Når det gjelder sivilt-militært samarbeid beskriver FDs cyberretningslinjer at kommersielle ordninger kan være hensiktsmessig også i krise (FDs cyberretningslinjer, 2014, s. 12). Retningslinjene sier ikke hvem som skal ta initiativet og bidra til slike avtaler. Kommersielle avtaler som erstatning for tiltak hjemlet i beredskapsloven gir

[48] Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren

Forsvaret støtte, men avtalen bør utformes slik at den også beskriver arenaer for samarbeid. Forvaret har skrevet en lignende avtale med Wilhelmsen gruppen på strategisk transport (Sveinung Berg Bentzrød, 2015).

I dette casestudiet må Forsvaret ta et større ansvar for helheten enn det de kortsiktige oppgavene tilsier. Fra kun å være herre i eget hus innenfor cybersikkerhet, så skal Forsvaret ivareta kriseledelse og bidra til rådgivning overfor politisk nivå.

4.4.2 Øvelser

Fastsatte organiseringer for krise må øves. Øvelser er viktige for å forberede kriseledelse på de utfordringer den kan møte (Dyndal, 2010, s. 318). Kriseorganiseringen i Norge ligger fast. Regjeringens kriseråd etableres på politisk nivå. Forsvaret har en fast kommandostruktur med situasjonssenteret (SITEN) på strategisk nivå og Forvarets operative hovedkvarter på operasjonelt nivå. I Forsvarets struktur er det både avdelinger med spesifikke fagoppdrag, og fagoffiserer i kommandostrukturen. Beredskapsplaner for etatene må testes ut, og rollene avklares gjennom gjennomføring av øvelser. Under sikkerhetskonferansen 2015 varslet justisminister Anundsen en større tverrsektoriell cyberøvelse i 2016. NRK rapporterte dette som en stor nasjonal sikkerhetsøvelse med fokus på respons og samarbeid (Hotvedt, 2015). Digi.no på sin side rapporterte dette som en stor IKT-øvelse, der målet blir å trene håndteringsapparatet (Jørgenrud, 2015). Utfordringen her er hvem som skal øves. DSB kan planlegge og gjennomføre en øvelse som treffer alle sektorene innenfor cybersikkerhet. Brukes scenario fra nasjonalt risikobilde kan samarbeidet og beredskapsplaner til sektorene samøves. Hvis dette er en øvelse i regi av Justis- og beredskapsdepartementet kan øvelsen være en krise hvor Politiet øves støttet av Forsvaret.

Forsvaret øver jevnlig for å opprettholde status på sine avdelinger og sin kommandostruktur. Enkelte av øvelsen involverer både andre nasjoner og nasjonale nødetater. Grunnlaget for øvelsen er de oppdragene og de kapasitetene Forsvaret er gitt i oppdrag om å ha.

4.4.3 Rådgivning

Cyberangrep og andre tversektorielle kriser setter kan sette kriseledelse på prøve. Kriser kan sette press på tid, og beslutninger må fattes hurtig. Tversektorielle kriser utfordrer sektorprinsippet. Beslutningsgrunnlag må hentes inn fra nivåene under og fra sideordnede etater. Med bruk av lederdepartement kan krisen involvere flere departementer, samt ulike etater og virksomheter. Krisehåndtering må være like god i egen sektor som overfor andre departementer med underliggende enheter (Dyndal, 2010, s. 232).

Rådgivere til regjeringens kriseråd er de ulike departementers etater og virksomheter. Samferdselsdepartementet med NKOM og Jernbaneverket, Justisdepartementet med PD, PST, DSB og NSM, samt Forsvarsdepartementet med NSM. Dette er noen av de mest aktuelle for å gi faglige råd ved en større krise. DSB vet mest om beredskapsplaner. NSM skal gi råd både til JD og FD. Alle etatene følger faglinjer opp til regjeringens kriseråd. Erfaringen fra USA under Cuba krisen i oktober 1962 viser at selv i krise vil lederen, i dette tilfellet president Kennedy, få ulike forslag fra sine departementer. Av de to som ble fremlagt valgte han et tredje (G. Allison, 2012, s. 12; G. T. Allison, 1971).

Ansvar fragmenteres i en hierarkisk struktur ved delegering (Fimreite, 2011, s. 161).

Ved cyberangrep er det viktig å ha forståelse av hva som er kritisk infrastruktur og hvordan den gjensidige avhengigheten er. Kapittel 5 i stortingsmelding 22 (St. meld. 22 (2007-2008), 2008) lister opp kritisk infrastruktur som: elektronisk kommunikasjon, satellittbasert kommunikasjon og navigasjon, kraft, vann og avløp, olje og gass, transport, bank, finans, matforsyning samt kulturminner og symboler. Kulturminner og symboler er ikke kritisk infrastruktur, men har stor betydning for vår kollektive hukommelse. Derfor inngår dette i beredskapsplanleggingen (St. meld. 22 (2007-2008), 2008, s. 52). Alle kritisk infrastrukturer kan ikke være like kritisk, men de forskjellige infrastrukturene ligger under ulike fagdepartementer. Rådene til kriserådet er dekkende for eget fagdepartements ansvarsområde, og de er ikke prioritert mellom fagdepartementene. Hvis kriserådet mangler informasjon for å koordinere, så må det iverksettes en ny runde med informasjonsinnhenting. Disse informasjonssløyfene tar ekstra tid.

Ved tidskritiske hendelser som cyberterror og andre må det være etablert et system for hurtig rådgivning. For cyberangrep kan regjeringens kriseråd søke informasjon hos cyberkoordineringsgruppen (CKG), NSM og Forsvaret. CKG er en gruppe på operasjonelt nivå med bred sammensetning, men er fokusert på trender og utvikling og ikke mot krisehåndtering. NorCERT med tilhørende miljøer er fokusert mot hendelseshåndtering, og er ikke satt opp for å understøtte tidskritisk kriseledelse. Deres analyse fokuserer på tekniske forhold knyttet til cyberangrepet, og den besvarer hva som har skjedd. NorCERT er den toppnoden som mottar rapporter fra de andre, og som videreformidler informasjon. Forsvaret under FD er likt organisert i fred som i krise og har en kommandostruktur med tilstedeværende ledelseselementer. Oppdraget til forsvaret er begrenset til egen struktur og systemer, men vil ikke kunne gi gode tverssektorielle råd. Forsvaret har fokus på å skape ledere på alle nivåer fra taktisk til strategisk. Disse kan gi råd på Cyber Defence i militære systemer.

4.5 Samvirke

Samvirke er det fjerde prinsippet for nasjonal krisehåndtering. Prinsippet skal benyttes på tvers av sektorer og mot sivil virksomhet.

I casestudien er det samarbeid mellom Forsvarsdepartementet og de andre departementene. Forsvaret samarbeider med virksomheter og bedrifter som AVINOR og Telenor. Forsvarets operative hovedkvarter som er ansvarlig for den militære innsatsen i Finnmark, har samarbeid med politi, andre nødetater, fylkesmenn og flere.

Ut fra teori skal det skapes prosesser for samarbeid alle nivå. Samvirkeprinsippet sier at alle har et selvstendig ansvar for å sikre best mulig samvirke med relevante aktører i arbeidet med forebygging, beredskap og krisehåndtering (Meld. St. 29 (2011-2012), 2012, s. 39). Det samme dokumentet beskriver også erfaringer med bruk av liaisoner mellom de ulike aktørene. Liaison fra politidirektoratet (POD) hos Oslo politidistrikt, samt liaison fra Forsvaret hos POD bidro til rask etablering av samvirke (Meld. St. 29 (2011-2012), 2012, s. 27). Videre har Justis- og beredskapsdepartementet en fast samordningsrolle overfor offentlig sektor.

Ved kriser kan det oppstå noen utfordringer med samvirke. Utfordringen er at ønsket om å samordne andre er større enn viljen til å bli samordnet (Fimreite, 2011, s. 23). Spesielt kan dette oppstå ved kriser hvor fagsektorer er faglige uenige om hvilke tiltak som skal iverksettes. Ved tidspress settes også samvirke på prøve. Alle aktørene skal samvirke, men ingen er tildelt rollen som dommer hvis det er uenighet. Bruk av liaisoner kan bidra til å få beslutninger raskere. Liaisoner er fagpersoner med erfaring fra den etat eller virksomhet de kommer fra. De er godt forberedt, og de kan ha tilgang på andre kommunikasjonsmidler.

Innenfor cybersikkerhet kan EOO-tjenestene og enkelte miljøer i Forsvaret samt politiet dele informasjon ved en krise. Utfordringen ved noe av Forsvarets virksomhet er gradering på en del av informasjonen som kan deles. Liaisoner kan være en måte å redusere avstanden mellom militære og sivile virksomheter. I enkelte tilfeller kan det være vanskelig å opprette fornuftige kanaler for informasjonsdeling.

De fleste CERT og CSIRT miljøer i Norge kan samarbeide og dele informasjon. NorCERT og Forsvaret kan ha noen begrensinger på enkelte av sine systemer. Samarbeidet mellom de ulike aktørene gir grunnlag for nettverket av informasjonsdeling som tidligere er beskrevet. Ressursene hos de fleste er begrenset, og gjennom samvirke kan det oppnås synergier for flere.

Erfaringene etter 22. juli er at det kan bli for mange å samarbeide med på en krise. I hierarkiske strukturer kan ansvaret delegeres ned til neste nivå og deles mellom flere. Hvis dette

gjennomføres i flere ledd vil det bli mange som skal forholde seg til samme krise. Splitting av ansvar kan gjøres med basis i geografi. Dette er bakgrunnen for politidistriktene. Her kan det oppstå utfordringer når kriser beveger seg mellom geografiske områder eller er på grensen mellom to.

Cyberdomenet er mangfoldig. Ulik definisjon på hva den enkelte etat og virksomhet skal jobbe med utfordrer samvirke. Det kan være virksomheter som har delvis overlappende fagområde. Aftenpostens avsløring av falske basestasjoner, såkalte IMSI-catchere, i Oslo førte til debatt og ettertanke (Madsen, 2014). Her var det mange aktører som tilsynelatende ikke tok ansvaret, men det ble heller ikke noe godt samvirke mellom de samme aktørene for å løse saken.

4.6 Delkonklusjon

Totalforsvarskonseptet legger grunnlaget for sivilt-militært samarbeid. Det legger premisser for både prosesser og samarbeidsforum. Tiltak gjennomført i fredstid må ha effekt ved en alvorlig krise eller væpnet konflikt. Gjennom samvirke i fredstid og Forsvarets støtte til mindre kriser utvikles kjennskapen til hverandres kapasiteter. Dette både på ledelses- og avdelingsnivå. Sentralt totalforsvarsforum og Cyberkoordineringsgruppen er to fora for sivilt-militært samarbeid i offentlig sektor. Det ene er interdepartementalt mellom sektoren og det andre er mellom EOS tjenestene. Når det gjelder cybersikkerhet er det ikke initiert hverken prosesser eller samarbeidsfora. Det skapes dermed få forutsetninger for å etablere gjensidig samarbeid inenfor dette området.

Forebygging og forberedelser har betydning for cybersikkerhet. Robustheten i nettverkene heves ved jevnlig å oppdatere programvare og justere tekniske muligheter. Informasjonsdeling knyttet til hendelseshåndtering og 'Best Practice' hever sikkerhetsnivået hos mange. De ulike miljøene har behov for ulik informasjon. CERT miljøer må dele avansert og bred informasjon. Litteraturstudien ga ingen klare svar på hvem som har nasjonalt ansvar for å koordinere eller å lede forebyggende tiltak i cyberdomenet.

Øvelser forbereder organisasjoner på kriser. Hensikten må være å øve på de oppgavene de ulike aktørene har. Cybersikkerhet må øves av de aktørene som har ansvar i krise og væpnet konflikt.

Ved alvorlige kriser får regjerningens kriseråd informasjons gjennom fagdepartementene. Med dagens organisasjon og styring på fagdepartementer er første tversektorielle krisehåndteringsenhet regjeringens kriseråd. Kriserådet koordinerer og departementene beslutter. Cyberangrep som treffer tverrsektorielt utfordrer denne strukturen. Rådene fra de ulike fagsektorene blir fremlagt uten prioritering, og det kan bli en ny runde med

informasjonsinnhenting. Tidskritisk informasjon må i dag komme fra miljøene i de ulike fagsektorene. Miljøer som kan bli bedt om å gi råd er ikke dimensjonert til å ta en slik oppgave. Hverken periodiske fora for informasjonsutveksling eller deteksjonskapasiteter kan ta rollen som rådgiver. Rådgivere må være på plass like raskt som krisestøtteenheten.

I dette tilfellet er ikke en nasjonalt strategi cybersikkerhet på plass. Ved en alvorlig krise vil de sivile etater og virksomheter bidra, men prosessene for samarbeid er ikke etablert. Samvirke er mulig, men har utfordringer med å understøtte tidskritisk kriseledelse. Vilje til å samarbeide oppveier ikke for manglene evne. Samvirke er en utfordring med mange aktører både i offentlig og privat sektor. Forsvaret jobber med graderte systemer til daglig, og kan få utfordringer med å etablere samvirke med alle relevante aktører.

5 Væpnet cyberangrep i komparativt perspektiv

Ved å se på andre nasjoner kan det være mulig å finne alternative organisasjonsmodeller. USA er en naturlig aktør av to grunner. Det første er at de har satset mye på cyberkapasitet gjennom at det er en felles sjef for National Security Agency (NSA) og United States Cyber Command (USCYBERCOM)[49]. I tillegg har de hatt cyberangrep som de løftet til et sikkerhetspolitisk nivå. Andre land er Finland og Nederland. Begge er småstater som Norge, men den ene er NATO medlem. I tillegg kan det være noe å lære av England. England og Nederland er to av våre viktigste allierte i Europa.

USA synes å ha en sterk knyting mellom daglig hendelseshåndtering og politisk beslutningsnivå. Politisk nivå mottar god informasjon fra hendelsesmiljøene ute i strukturen. Håndteringen av situasjonen rundt cyberangrepene mot Sony Pictures i 2014 viser at hendelser kan løftes til politisk nivå hvis de er innenfor nasjonens interesseområde. Her anklaget USA Nord-Korea for å stå bak angrepene (Sanger & Perlroth, 2014).

Operasjonen mot Sony Pictures ble gjennomført i minst tre steg. Først spredning av informasjon om de ansatte, deretter sletting av servere og til slutt en fysisk trussel mot kinoer som ville vise filmen. Forutsetningen for de to første er at angriperen fikk tilgang til datasystemene i Sony Pictures.

Organiseringen og prosessene løftet denne saken ut fra de daglige hendelsene og satte den inni en sikkerhetspolisk ramme. Håndteringen deretter ble metodisk som en sikkerhetspolitisk krise. Potensialet til den fysiske trusselen var stor. Nord-Korea er en av de utpekte trusselaktørene som kan påvirke USA og gir dermed grunnlag for å løfte denne til et politisk nivå. Uten denne koblingen kunne hendelsen ha blitt sett på som en større kriminell handling med utspring i Nord-Korea.

Kortversjonen (Fact Sheet) av The Department of Defence (DoD) Cyber Strategy[50] beskriver offentlig-privat samarbeid i en annen kontekst enn flere andre nasjoner. Der de andre fokuserer mest på informasjonsdeling og samarbeidsfora i denne sammenhengen, så fokuserer USA på utvikling av faglig ekspertise. Fra offisiell side i USA jobbes det for å få på plass lover som gjør det mulig å dele informasjon mellom offentlige etater og private bedrifter[51]. Strategien beskriver også at forsvarets kapasiteter skal beskytte kritisk offentlig sektor samt forsvarets systemer. Denne oppgaven likt den som Cyberforsvaret har i Norge.

[49] The National Security Agency/Central Security Service (NSA/CSS) hentet fra www.nsa.org 29.april 2015
[50] Fact Sheet hentet fra http://www.defense.gov/home/features/2015/0415_cyber-strategy/, den 1. mai 2015

I Norge ville denne blitt håndtert som kriminalitet. Bedriften må anmelde forholdet og lokalt politi etterforsker dette som datakriminalitet. Hvis bedriften er en del av NorCERT sitt VDI samarbeid vil hendelsen bli registrert der, og informasjon tilflyter andre også de samarbeidende etterretnings- og sikkerhetstjenestene. Trusselen som følger cyberhandlingen avventes nærmere. Dette likt de forhold som medførte bevæpning av norsk politi høsten 2014[52]. Ut over ekstra overvåkenhet og fokus fra EOS-tjenestene ble det ikke iverksatt ytterligere tiltak, og ingen av krisehåndteringsmekanismene ble etablert for å starte forberedelser.

Både Finland og Nederland har organisasjoner og prosesser som underbygger en helhetlig tilnærming. Finland beskriver i sin cybersikkerhets strategi en satsning på offentlig privat samarbeid og etablering av et Cyber Security Centre (Security and Defence Committee, 2013). Til det siste skal det også utvikles et system for 24/7 informasjons sikkerhet for samfunnet. Den finske CERT funksjonen er plassert i samme etat som Cyber Security Centre. FICORA er en etat som ligner på NKOM i Norge og er underlagt Ministry of Transport and Communications[53]. På militær side har Finland en cyberkapasitet som både har angreps (CNA) og forsvars (CND) kapasitet (Security and Defence Committee, 2013, s. 8). På strategisk nivå har Finland etablert en strategisk sikkerhetskomité (Security Committee) med tverrsektoriell representasjon for å ivareta en helhetlig tilnærming til nasjonal sikkerhet[54]. Denne mangler derimot deltagere fra det private næringsliv.

Nederland beskriver i sin cybersikkerhets strategi videre satsning på offentlig-privat samarbeid i rammen av National Cyber Security Centre (NCSC)[55] (National Coordinator for Security and Counterterrorism, 2013, s. 24). Forsvaret er en av aktørene i offentlig sektor som bidrar. Fra privat side er det deltagere fra energisektoren, finanssektoren og telekommunikasjon. Videre utvikling innenfor NCSC er etablering av et Security Operations Centre (SOC) i tillegg til den eksiterende CERT funksjonen. NCSC er underlagt Ministry of Security and Justice. For å møte trusselen fra cyberspionasje er det etablert en Joint Sigint Cyber Unit (JSCU) som er et samarbeid mellom etterretningen og sikkerhetstjenestene (National Coordinator for Security and Counterterrorism, 2013, s. 24). Når det gjelder det offentlig-private samarbeidet så er det utviklet

[51] Hentet fra https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf, den5. mai 2015
[52] Pressemelding Nr: 76 – 2014 Samtykke til bevæpning hentet fra https://www.regjeringen.no/nb/aktuelt/Samtykke-til-bevapning/id2341743/, den 29. april 2015
[53] Hentet fra http://www.lvm.fi/en/communications_policy, den 29. april 2015
[54] Hentet fra http://www.defmin.fi/en/overview/ministry_of_defence/organisations_accountable_to_the_ministry_of_defence/security_and_defence_committee, den 22. april 2015
[55] Hentet fra https://www.ncsc.nl/english, den 29. april 2015

fra «partnership» til «participation» fra NCSS 1 til NCSS 2. På militær side vil Nederland etablere en Cyber Command som en del av Hæren med kapasitet for både forsvar, etterretning og angrep innenfor cyberdomenet[56].

Til slutt kan England også tas med. England har etablert et offentlig-privat samarbeid for informasjonsdeling. The Cyber security Information Sharing Partnership (CiSP) er etablert som del av deres CERT-UK (CERT-UK, 2015). Ansvarlig departement for utvikling av UK Cyber Strategy er Cabinet Office. The Office of Cyber Security and Information Assurance (OCSIA) i departementet utarbeider strategiske føringer og koordinerer cybersikkerhetsprogrammet på vegne av regjeringen[57].

Felles for flere av disse nasjonene er at de har samlet både defensiv og offensiv kapasitet i samme avdeling. På en side kan dette være fornuftig for småstater som Nederland og Norge. Miljøene blir større og mulighet for kompetanseoverføring mellom enkeltindivider øker. Forsvarets defensive kapasitet er liten i Cyberforsvaret, men vil være en del av et større miljø hvis samlet med andre elementer innenfor Computer Network Operations (NCO). I motsetning til dette står muligheten til informasjonsdeling og evne til Cyber Defence[58]. Som teorien beskriver i kapittel 2 er informasjonsdeling viktig for å ha best mulig evne til forsvar mot cyberangrep. Informasjonsdeling mellom en militær avdeling og sivile samarbeidspartnere forutsetter ugardert eller beskyttet informasjon. Hvis den militære CNO avdelingen jobber med høygardert informasjon, så kan den ikke dele denne med andre enn autoriserte enheter. EOS miljøet i Norge er en gruppe avdelinger som kan dele gradert informasjon. I en CNO avdeling kan cyber forsvar nedprioriteres til fordel for angrep. Det unike med cyberkapasiteter er at kapasiteter for angrep og utforskning (NCA og CNE) ikke kan benyttes til forsvar (CND). Thomas Rid uttaler at gode evne til offensive cyberoperasjoner ikke oppveier svakheter i defensive evner, og at kapasitetene ikke kan brukes om hverandre (NATO, 2013a).

USA, Finland, Nederland og England er organisert på en annen måte en Norge, men det er mulig å lære av disse.

Flere nasjonene satser på tverrsektorielt og sivil-militært samarbeid. Den formelle samarbeidsformen er både samlokalisert og felles enhet. Samling av resurser i et miljø har noen fordeler med tanke på krisehåndtering. Strategisk og politisk ledelse kan få beslutningsunderlag

[56] Hentet fra http://www.defensie.nl/english/topics/cyber-security/contents/cyber-command, den 29. april 2015
[57] Hentet fra https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace#background, den 3. mai 2015

som allerede er koordinert mellom aktørene, og ulike mulige aktiviteter kan være prioritert. Ved en annen løsning ville innspill til beslutninger fulgt rapporteringslinjene i sektoren. Beslutningsorgan på politisk eller strategisk nivå må vurdere innspill mot hverandre før beslutning. Et felles miljø vil også kunne respondere raskere og ha bedre samvirke. Miljøet er satt, og de ulike deltagerne har forståelse og innsikt i hverandres oppgaver. Muligheten til felles situasjonsbevissthet er også bedre nå miljøet er samlet. Ulempen ved å være samlet kan være at miljøet ubevisst siler og vurderer informasjon som politisk eller strategisk nivå burde ha tatt stilling til. For de fleste vil fordelene oppveie for ulempene, og de har etablert slike felles miljøer.

[58] Cyber forsvar (Cyber defence) er en militær oppgave innenfor området cyber sikkerhet.("Cyber defence is part of NATO's core task of collective defence" hentet fra http://www.nato.int/cps/en/natohq/topics_78170.htm den 12. Februar 2015)

6 Konklusjon

Norge har så langt ikke vært involvert i en større væpnet konflikt mot en motstander med stor bredde i sine kapasiteter. De operasjonene Norge har deltatt i internasjonalt de siste tiårene har vært mot en teknologisk og kapasitetsmessig underlegen motstander. Cybertrusselen er relativ ny, og cyberangrep er i dag et virkemiddel som kan benyttes. Fra Estland i 2007, via Georgia i 2008 til Ukraina i 2014 er det innslag av ulike cyberangrep i det som kan regnes som mellomstatlige konflikter. I tillegg har det vært brukt cyberangrep for å forhindre utvikling av kjernefysiske våpen. Stuxnet var rettet mot systemer som anriket uran, mens Israels angrep mot syrisk luftvarsling var beskyttelse for egne luftoperasjoner.

I Norge er ansvaret for cybersikkerhet fordelt mellom ulike aktører. Ved et væpnet angrep på Norge vil Forsvaret ta ledelsen, og sivil sektor må i henhold til totalforsvarskonseptet understøtte militær virksomhet.

I denne studien fant jeg at Forsvaret har begrensede rammer for ivaretagelse av cybersikkerhet. Oppdragene er knyttet til egne nettverk. Oppgavene begrenser Forsvarets mulighet til å ta ansvar for øvelser. Øvelser bidrar til å forberede kriseledelse og for å teste beredskapsplaner. Norge mangler en cybersikkerhetsstrategi. Denne skal blant annet regulere den sivil-militære samarbeidet, beskrive informasjonsdeling, beskyttelse av kritisk infrastruktur og kriseledelse. Samvirke er en utfordring med mange aktører både i offentlig og privat sektor. Totalforsvarskonseptet gir mulighet for å etablere et «cyberråd» mellom virksomhetssjefer med ansvar innenfor kritisk infrastruktur. Dette som nivå under sentral totalforsvarsnemd, og samtidig bredere sivil-militær deltagelse enn cyberkoordineringsgruppen.

Funnene vil skape store utfordringer for kriseledelse i en væpnet konflikt. Noe av manglene kan oppveies av tid til å sette prosesser og iverksette tiltak etter at krisen har oppstått. Utforingene vil være størst når tiden er knappest. Cyberangrep kommer uten forvarsel, og det må iverksettes hendelseshåndtering og kriseledelse. Cyberdomenet er globalt, og angrepet trenger ikke å være fra en nasjon med grenser mot Norge.

Oppgavens første del forklarte forhold knyttet til cybersikkerhet og grunnlaget for organisering av offentlig sektor. Empiri viser at sabotasje, spionasje og subversjon er former for cyberangrep som kan benyttes mot Norge. Disse vil være rettet mot både sivile og militære systemer. Sekundærlitteraturen beskriver mange cyberangrep mot det som defineres som sivile systemer. Dette bekreftes av E-tjenesten og PST sine rapporter for 2014 (Etterretningstjenesten, 2015; Politiets sikkerhetstjeneste, 2015). Attribusjon av angrep til stater er vanskelig. I litteraturen

pekes det ut nasjoner bak ulike angrep, men det er få eksempler på at det dermed er løftet til sikkerhetspolitisk nivå. USA sin håndtering av cyberangrepene mot Sony Pictures er et eksempel på dette. Her ble Nord-Korea både beskyldt for å stå bak, samt at det ble gjennomført motangrep. Intervju med UD bekrefter at det er ingen kjente eksempler på at attribuerte cyberangrep, enten som spionasje eller rekognosering, har ført til diplomatiske reaksjoner. I den fysiske verden er det mer vanlig å iverksette diplomatiske reaksjoner ved avdekking av spionasje. Til slutt i første del ble ministerstyre og organisering i fagdepartement vektlagt. De fire krisestyringsprinsippene skal brukes for å øke evnen til krisehåndtering i offentlig sektor. Disse er ansvar, nærhet, likhet og samvirke. Samvirke er det som skal gi tverrdepartemental samordning.

I oppgavens andre del ble cyberangrep som sikkerhetspolitisk virkemiddel og en væpnet konflikt analysert. Hvis et cyberangrep er alvorlig og medfører tap av liv eller materielle ødeleggelser kan politisk nivå velge å kreve rett til selvforsvar etter FN paktens artikkel 51 (Forsvarets høgskole/Forsvarets stabsskole, 2013, s. 190). Når det gjelder krigens folkerett bør Forsvaret harmonisere sitt begrepsapparat, og bruke cyberangrep som dekkende på all ondsinnet aktivitet, men samtidig gradere alvorlighetsgraden. Et alvorlig cyberangrep som medfører tap av liv eller fører til materielle skader, utløser rett til selvforsvar. Sammenfallende begrepsapparat er viktig med tanke på samarbeid med andre aktører. Litteratur brukt til denne oppgaven, samt workshop og intervjuer bekrefter allmenn bruk av ordet cyberangrep. Innsatsen mot cyber må være tversektoriell, samt at den må dekke offentlig og privat sektor. Felles begrepsbruk er viktig ved samarbeid. Analysen av en væpnet konflikt var formet rundt en casestudie som inneholdt både en fysisk dimensjon og flere samtidige cyberangrep. Analysen så på totalforsvarskonseptet, forebygging, kriseledelse og samvirke.

Etter 22.juli er samvirke etablert som det fjerde prinsippet i nasjonal krisehåndtering i 2012 (Meld. St. 29 (2011-2012), 2012). Hensikten er å øke koordineringen mellom fagdepartementene under kriser. Avhengig av oppstått krise velges kriseorganisering. Organiseringen påvirker håndteringen av cybersikkerhet gjennom kriseskalaen. Definerte kriser gir definerte organiseringer for krisehåndtering. Under sikkerhetskonferansen 2015 varslet justisminister Anundsen en større tverrsektoriell cyberøvelse i 2016. NRK rapporterte dette som en stor nasjonal sikkerhetsøvelse med fokus på respons og samarbeid (Hotvedt, 2015). Digi.no på sin side rapporterte dette som en stor IKT-øvelse, der målet blir å trene håndteringsapparatet (Jørgenrud, 2015). Justis- og beredskapsdepartementet har både rollen som lederdepartement ved en sivil krise, samt at det er kontrollorgan for beredskapsarbeid i offentlig sektor. Den siste oppgaven utøves av DSB. Hvis øvelsen skal teste beredskapsplanverk hos aktørene er denne

viktig for cybersikkerhet i væpnet konflikt. Deltagere på workshop beskrev også øvelser som tiltak for å redusere risiko innenfor cybersikkerhet[59].

Når det gjelder kriseledelse er Forsvaret en organisasjon som har evne til planlegging og gjennomføring av operasjoner. Dette gjelder både i fredstid, i krisesituasjoner og ved en væpnet konflikt. Som eksperter på kriseledelse vil de andre aktørene se til Forsvaret ved en væpnet konflikt. Deltagerne på workshop bekrefter denne tolkningen av totalforsvarskonseptet[60]. Dette forutsetter derimot at Forsvaret har vært synlig på alle nivåer. Forutsetning for samarbeid og koordinering ligger i gjensidig forståelse hos hverandre på styrker og svakheter. Det bør etterstrebes å ha like oppgaver i fred, krise og væpnet konflikt. Hvis Forsvaret forventes å ha en ledende rolle innenfor cybersikkerhet i væpnet konflikt, så må ansvarsområdet utvides fra hendelseshåndtering i egen infrastruktur til kriseledelse innenfor nasjonal cybersikkerhet. Hvis ikke forblir fokus på taktisk nivå i samarbeid med andre nasjonale CERT miljøer.

Totalforsvarskonseptet gir det overordnede tankegodset på sivilt-militært samarbeid i kriser. Strategi utdyper hvordan samarbeidet utvikles og oppdrag til virksomheter og etater fordeler ansvaret. Risiko og sårbarhet reduseres ved å revitalisere totalforsvarskonseptet, formalisere en nasjonal cybersikkerhetsstrategi, etablere et offentlig-privat samarbeidsforum og satse på forebygging. Totalforsvarskonseptet er ikke avviklet, og Forsvaret må ha støtte fra det sivile ved en væpnet konflikt. Det bør etableres et «Cyberråd» på strategisk nivå som favner ledere for virksomheter og etater i offentlig og privat sektor. Cyberrådet bør etableres med samme type mandat som det totalforsvarets sambandsnemd hadde frem til 1999. Lederposisjonen bør ivaretas av den sivile delen av statsforvaltningen. Forsvaret skal lede i en væpnet konflikt, men har ikke mandat til myndighetsutøvelse i fredstid.

En nasjonal cybersikkerhetsstrategi mangler. Andre småstater som Norge kan sammenligne seg har utgitt sin strategi (ENISA, 2015). Det meste av kritisk infrastruktur er i privat eie (Friis, 2015), og strategien bør si noe om innretning på offentlig-privat samarbeid. De nasjonale prinsippene for krisehåndtering gjelder også for privat sektor. Prinsippet om samvirke medfører en koordinering av innsatsen også mot sivil sektor.

Analysen av en væpnet konflikt med cyberangrep viser at det er utfordringer knyttet til tidskritisk rådgivning til strategisk og politisk nivå. Regjeringens kriseråd er representanter for fagdepartementene, og faglige råd til rådet følger tjenestevei i departementene. Cyberangrep mot kritisk infrastruktur har konsekvenser ut over ansvaret til hvert enkelt fagdepartement.

[59] Oppsummering etter tverrsektoriell workshop15. april 2015

Regjeringens kriseråd koordinerer mellom departementene, og har behov for tversektorielle anbefalinger. Faglige råd fra departementene som ikke er sammenfallende kan medføre en ny informasjonssløyfe. Det mangler et operativt samarbeidsforum for krisehåndtering på operasjonelt nivå. Dette bør være tverrsektorielt og basert på offentlig-privat samarbeid, likt det som andre nasjoner har etablert. Med dagens regime settes regjeringens kriseråd på politisk nivå først etter en alvorlig hendelse. Hvis ekspertutvalgets anbefaling tas til følge vil det bli etablert en fast tilpasset kriseenhet ved Statsministerens kontor[61]. Et felles forum på operasjonelt nivå med både tverrsektoriell og privat representasjon vil kunne se hendelser i en større helhet, og vil kunne løfte de riktige hendelsene til politisk nivå. Et minimum ambisjonsnivå bør være en samlokalisering av aktørene. En utfordring med sektorprinsippet i dag er at alle skal koordinere, men ingen ønsker å bli koordinert. Samvirke som krisestyringsprinsipp kan tolkes som å koordinere egen aktivitet med andre. Ambisjonen bør være samarbeid som Nederland har skissert i sin nyeste cybersikkerhetsstrategi (National Coordinator for Security and Counterterrorism, 2013). Her er ambisjonen for offentlig-privat samarbeid hevet fra å koordinere (coordinate) til å samarbeide (cooperate) i siste versjon. Et slikt samarbeid vil kunne utøve kontroll på tiltak i nasjonal kritisk infrastruktur, ha mulighet til å se denne i sammenheng samt sette prioritet mellom dem i tid og rom. I motsetning til USA har ikke Norge noen juridiske bindinger på offentlig-privat samarbeid. Dette felles miljøet bør ha evne til å se på hvorfor cyberangrepene gjennomføres basert på deteksjonsrapporter fra CERT miljøene. Organisatorisk gir dette miljøet anbefalinger om tiltak innenfor nasjonal cybersikkerhet til både regjeringens kriseråd og til operativ kommandokjede i Forsvaret. I tillegg vil et slikt miljø kunne anbefale tverrsektorielle prioriteringer når det gjelder reetablering etter cyberangrep. Cybersikkerhetsstrategien bør si hvem som gis hovedansvar for etablering av et slikt miljø. Daværende stortingsrepresentant Ine Marie Eriksen Søreide med flere la frem et forslag om målrettet og forsterket innsats for informasjons- og cybersikkerhet i 2012. Her uttales at samarbeid mellom offentlig og privat sektor burde organiseres i et samspill basert på felles interesser og med et gjensidig forpliktende samarbeid (Dokument 8:147S (2011-2012), 2012). Formen på dette bør være et miljø som er samlokalisert og som har kapasitet for å vurdere tidskritiske hendelser. Denne enheten samler inn informasjon, bearbeider informasjonen tverrsektorielt og mot privat sektor samt gir råd til regjeringen kriseråd. Terrortrusselen mot Norge høsten 2014 førte kun til bevæpning av operativt politi, og ikke forberedelser til

[60] Oppsummering etter tverrsektoriell workshop15. april 2015
[61]Ekspertgruppen for forsvaret av Norge: Et felles løft, side 75

kriseledelse. Kriseledelse bør bli dynamisk og ikke hendelsesbasert som i dag. Et tverrsektorielt samarbeid i form av et tilgjengelig «Krisesenter» kan starte tversektorielle forberedelser.

Rammen for samarbeid bør være basert på frivillighet. Formalisering av et offentlig-privat samarbeid vil kunne være et alternativ til de tvangsmidler som beredskapslovgivningen gir. Det norske forsvaret er lite og det er i liten stand til å ta kontroll over andre virksomheter selv ved en væpnet konflikt.. Det bør ses på om det innenfor cybersikkerhet kan lages avtaler lik den som Forsvarets Logistikkorganisasjon (FLO) har fremforhandlet med Wilhelmsen-gruppen (Sveinung Berg Bentzrød, 2015). En samarbeids- eller intensjonsavtale med vitale leverandører av kritisk infrastruktur kan gi rom for samvirke, forberedelser og øvelser i fredstid.

Ingen er gitt konkrete oppdrag om ledelse eller koordinering av forebyggende tiltak knyttet til cybersikkerhet. Forebygging i cyberdomenet handler om å gjøre cyberdomenet mer robust, og heve beskyttelsesnivået. Målsettingen bør være å etablere og vedlikeholde en forsvarbar infrastruktur i Norge. Her må alle typer virksomheter inngå, både i offentlig og privat sektor. Her inngår statlig virksomhet, forsknings- og utviklingsmiljøer, media, akademiske institusjoner, små og mellomstore bedrifter samt enkeltindivider. Sammenlignet med den fysiske verden må det koste en del ressurser for å komme forbi ringmuren. Det bør bli vanskeligere enn i dag, men det handler om å binde opp motstanderen ressurser selv om han er tallmessig overlegen. Av mulige aktører påstås det at Nord-Korea har 6000 cyberkrigere i sitt Byrå 121[62]. Kina og Russland har også store offentlige miljøer. Erfaring fra Cyber Kill Chain tilsier at innsatsen bør flyttes fra hendelseshåndtering og til forebygging. Alle bør med for å bygge sterk sikkerhet i «Cyber festningsverk Norge». Statlige virksomheter og de største bedriftene i Norge har både forståelse for og evne til å følge opp den tekniske dimensjonen av cybersikkerhet. Akademiske institusjoner og forsknings- og utviklingsmiljøer har stor tillitt i samfunnet, og er store brukere av informasjonsteknologi i utøvelsen av sine oppgaver. Lav bevissthet om cybersikkerhet hos disse kan gjør dem til utgangspunkt for cyberangrep mot andre virksomheter. Små og mellomstore bedrifter og enkeltindivider utgjør det største volumet. Hos de fleste av disse er kompetansen og bevisstheten liten, og de evner ikke å sette et tilstrekkelig forebyggende nivå på sikkerhet. Forsvaret må bli synlig på alle nivåer og være en pådriver for utvikling av nasjonal cybersikkerhet, hvis ikke kan det bli vanskelig å overta kriseledelse ved en væpnet konflikt.

For å lykkes med å bygge en normalsituasjon med en robust og forsvarbar infrastruktur må det deles informasjon mellom aktørene. Ulike aktører har ulike informasjonsbehov. CERT-miljøene

[62] Hentet fra http://www.dw.de/north-korea-cyber-army-double-the-size-previously-thought/a-18173646, den 6. mai 2015

kan dele informasjon som er både detaljert og gradert. Til dette finnes det egne beskyttede datasystemer. Det store volumet av brukere bør få enkel og lettfattelig informasjon på tiltak de kan iverksette. De få og store aktørene er fokusert på cybersikkerhet, setter av ressurser til dette og er tilknyttet et CERT-miljø. Inntil videre er ikke slike tjenester kommersialisert enda, men det er enkelte produkter på vei inn på markedet. Fujitsu sin Software Systemwalker Security Control er en online tjeneste for bedrifter[63]. Gjennom et abonnement ivaretas sikkerhet for bedriften. Inntil videre bør alle inviteres til å delta i informasjonsnettverkene. Alternativet ville vært en lov eller bestemmelse som regulerer et minimum sikkerhetsnivå, og virksomheter må ha dette på plass på lik linje som med godkjent regnskap for å kunne drive virksomheten på lovlig vis. Over tid må det tas opp til diskusjon om noen få (evt mange) skal få tillatelse til å ta risikoen på vegne av nasjonen hver dag når de ikke har sikkerhet på plass. Cyberspionasje mot industrien reduserer nasjonal verdiskapning på sikt. Tidligere sjef for NSA General Keith B. Alexander beskriver dette som "death by a thousand cuts[64]". Advokaten for 'Cyber Pearl Harbor' beskriver dette som den største trusselen i 2012 (Rosenbaum, 2012). Skadevare med utspring i usikrede nasjonale systemer kan få store ringvirkninger. Den offentlige debatt i Norge fokuserer ofte på ivaretagelse av informasjonssikkerhet eller håndtering av digital informasjon. STUXNET og HAVEX er ikke trusler som håndteres innenfor informasjonssikkerhet. Utvidet kommunikasjonskontroll fra PST og de andre EOS tjenestene vil ikke kunne forhindre eller oppdage slike cyberangrep. Informasjonsdeling er en utfordring for en etat som Forsvaret hvor «Need to know» er et fremtredende prinsipp. Forsvaret bør etablere løsninger hvor det blir mulig å inngå i et ugradert informasjonsnettverk. Dette bygger tillitt og synlighet i fredstid, og er med på å skape forutsetninger for fremtidig kriseledelse.

Utviklingen videre må også være innenfor det som Norge har forpliktet seg til i NATO sammenheng. I nasjonalt krisespekter fra fred til væpnet konflikt skal de evner som er beskrevet i det strategiske konseptet etter toppmøtet i Lisboa, videreutvikles (NATO, 2010, s. 5 pkt 19). Det står her at NATO og nasjonene skal videreutvikle sin evne til å forebygge, oppdage, forsvare seg mot og reetablere etter cyberangrep[65]. Oppdage er knyttet til hendelseshåndtering (Incident Response) er tidskritisk og bør holdes til miljøer som er på døgndrift. Denne kapasiteten har NorCERT og det nasjonale nettverket av CERTer og CSIRTer. Information Sharing and Analyst

[63] FUJITSU Software Systemwalker Security Control. Hentet fra http://www.fujitsu.com/global/about/resources/news/press-releases/2014/0507-02.html, den 3. mai 2015

[64] Sitat "Alexander referred to the growing number of hacking incidents targeting US technology and corporate trade secrets as "death by a thousand cuts."" Hentet fra http://www.hstoday.us/focused-topics/cybersecurity/single-article-page/us-facing-death-by-a-thousand-cuts-in-cyberspace/4ac6f26957f17cafb8611b6fa5899622.html, den 7. mai 2015

[65] Oversatt fra engelsk Cyber-Attack

Centre (ISAC) er analyse, oppfølging av trender og deling av Best Practice. Prosessen er ikke tidskritisk. Dette er en oppgave som CERT miljøene har, men i tillegg bør andre institusjoner og virksomheter inngå i et slikt nettverk.

Forsvaret skal lede i væpnet konflikt. Etaten kan slite med tillit i andre deler av krisespekteret. Det etaten har av informasjon er gradert, og det vil være noen hinder for å dele med andre. Årsrapporten fra E-tjenesten har en side knytet til Cyber, og denne informasjonen er vanskelig å omsette i konkrete tiltak for de som leser denne. Tillitsforholdet kan dermed være vanskelig å bygge opp i fredstid. Politi har lokale tilstedeværelse, og har en rolle i bekjempelse av cyberkriminalitet. De og andre sivile aktører har ikke denne bindingen på deling av informasjon.

Organisering etter kriseskalaen egner seg ikke for cybertrusselen. Organiseringen bør være mer trusselfokusert. Hendelser i fredstid kan være forberedelser for sabotasje i væpnet konflikt eller spionasje mot kritisk infrastruktur. Forsvaret bør ha en mer integrert rolle og synlighet i hele konfliktspekteret for å stå bedre rustet til å overta ansvar fra politiet i dagens skisserte overgang mellom krise og væpnet konflikt.

Ekspertgruppen (Ekspertgruppen for forsvaret av Norge, 2015) anbefaler at det etableres en ny «normaltilstand». I normalsituasjonen inngår blant annet cyberangrep som del av pågående informasjonsoperasjoner og cyberspionasje mot norske interesser. Normalsituasjonen bør ha mulighet til å følge trusler mer dynamisk. Derigjennom bør det fastslås hvilke cyberangrep som skal sikkerhetiseres, og bli en del av nasjonens sikkerhetspolitikk. Beredskapsplaner må ta høyde for at en normalsituasjon med flere typer trusler ikke vil være konstant, men mer dynamisk over tid. Trusselen i cyber er menneskeskapt, og i hvilken form den vil materialisere seg er uvisst. Noen cybervåpen er «One Shot Gun»[66]. Når de er benyttet og kompromittert må de endres. Dette fører til at det stadig kommer nye metoder og avarter av gjennomførte cyberangrep. Det viktigste vil ikke være detaljeringsgraden i planen i seg selv men den prosessen og det nettverket som skapte planen er det (Fimreite et al., 2012).

Andre nasjoner har etablert en militær enhet for Computer Network Operations (CNO) som har både offensive og defensive kapasiteter. Et mulig rasjonale for en felles avdeling er å få et større teknisk miljø. Småstater som Norge bør samle sammenfallende ressurser i et miljø. Individer med god kompetanse innenfor cyberdomenet kan benyttes både til offensive og defensive oppgaver. Utfordringen ligger på kapasitetene. Militære kapasiteter kan generelt benyttes både til angreps- og forsvarsformål. Dette er ikke gjeldende for cyberkapasiteter. Offensive

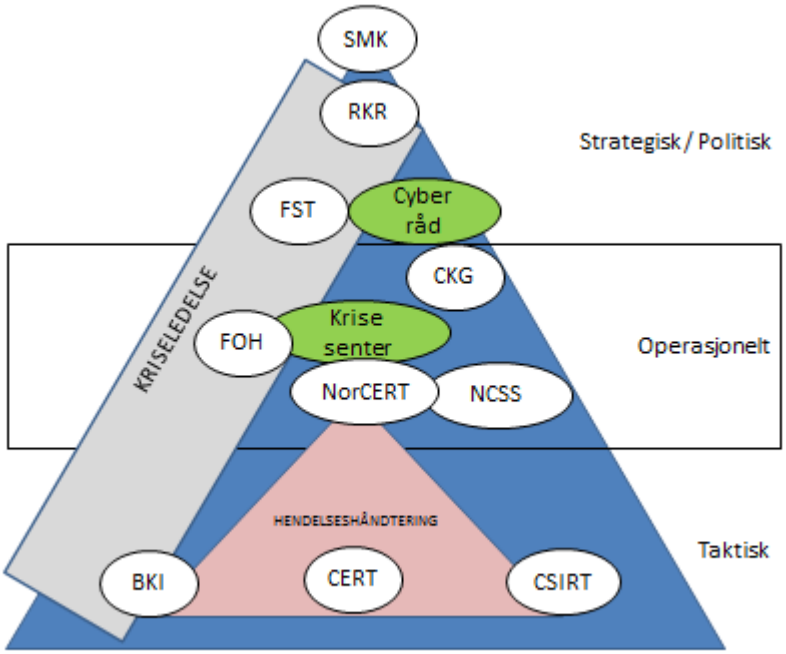
[66] General (R) Sverre Diesen foredrag FSTS høsten 2014

cyberkapasiteter gir ingen overførbarhet til defensive cyberkapasiteter (NATO, 2013a). Dette gjelder på strukturelt nivå og med hensyn på maktmidlene (tools of power) som er forskjellige. USA med stor offensiv kapasitet er svakt rustet innenfor cybersikkerhet (R. Clarke, 2009).

Dette viser at nasjonal organisering for håndtering av cybersikkerhet i væpnet konflikt ikke er optimal. Dette begrunnes i at det ut fra denne studien er det flere utfordringer som har negative konsekvenser for nasjonalt samarbeid. Det skapes ikke tilstrekkelig med forutsetninger for å lykkes på en bedre måte. Selv innenfor etablert sektorprinsipp og nasjonale krisestyringsprinsipper er det muligheter for å ivareta cybersikkerhet på en bedre måte. Cyberangrep treffer samfunnet bredt og totalforsvarskonseptet legger sivilt-militært til grunn. Men samarbeidet defineres ikke videre i strategi og oppgaver til Forsvaret. Forsvarets evne til krisehåndtering er dermed begrenset innenfor området cybersikkerhet.

6.1 Mulige utviklingstrekk og fremtidig forskning

Denne skissen oppsummerer nasjonal krisehåndtering på taktisk, operasjonelt og strategisk nivå. En del fokuserer på kriseledelse, en del på hendelseshåndtering og en del på koordinering av aktivitet. For kriseledelse har Forsvaret en kommandolinje og tjenestevei som er lik i fred, krise og i væpnet konflikt. Ved alvorlig krise og væpnet konflikt samles Regjerings kriseråd og Statsministerens kontor på politisk nivå. For å komplettere evne til kriseledelse etableres et «krisesenter» miljø på operasjonelt nivå. Dette miljøet kan gi tversektorielle og prioriterte anbefalinger til regjeringens kriseråd. Miljøer for hendelseshåndtering er på taktisk nivå, med NorCERT som nav plassert på operasjonelt nivå. Cyberråd er totalforsvarets forum for koordinering mellom offentlig og privat sektor på lang sikt.



Det bør i tillegg forskes på hvordan teknologi og prosesser kan bidra til bedre cybersikkerhet. Cyberdomenet er menneskeskapt, og det må ses på muligheter for å gjøre forberedelser i domenet eller muligheter for å endre på domenet. Både cyberspionasje og cyberrekognosering ser etter muligheter i cyberdomenet, og hendelsen kan repeteres såfremt domenet er likt fra forrige gjennomføring. Hvis ikke må utførende legge ressurser i å oppdatere veien frem til kilden eller målet.

Vedlegg A Informasjonsskriv

Forespørsel om deltakelse i forskningsprosjektet

"Cybersikkerhet i væpnet konflikt"

Bakgrunn og formål
Jeg gjennomfører for tiden en masterstudie ved Forsvarets høgskole.

Nasjonale resurser for håndtering av cybersikkerhet er fragmentert. I tillegg til aktørene i statlig sektor er det viktige aktører i privat sektor.

Hensikten med oppgaven er å se på hvordan de nasjonale aktørene innenfor cybersikkerhet samvirker i krisespekteret og se på overgangen til væpnet konflikt.

Hva innebærer deltakelse i studien?
Det legges opp til et delvis strukturert intervju. Som intervjuobjekt vil du bidra til å besvare deler av studien. Du er utvalgt som intervjukilde i kraft av din kompetanse og stilling. All informasjon som skal benyttes i oppgaven vil være ugradert for å ha størst mulig tilgjengelighet. Hvis det forekommer gradert informasjon i intervjuet må jeg gjøres oppmerksom på det. Du vil få tilsendt spørsmålene i forkant av intervjuet, men du står fritt for å ta opp andre forhold som har betydning for problemstillingen. Intervjuet vil bli tatt opp.

Hva skjer med informasjonen om deg?
Alle personopplysninger vil bli behandlet konfidensielt. Datamateriale vil kun være tilgjengelig for meg som prosjektleder og veileder.

Intervjuobjekter vil gjenkjennes med navn og funksjon i oppgaven når den publiseres.

Prosjektet skal etter planen avsluttes 1. juli 2015. Datamateriale anonymiseres og behandlingen av personopplysninger vil være i samsvar med retningslinjene ved Forsvarets høgskole. Evt gradert informasjon vil bli oppbevart iht Forsvarets bestemmelser for gradert informasjon.

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 ønsker å delta eller har spørsmål til studien, ta kontakt med meg på telefon: 48994971 eller e-mail: nprestmo@fhs.mil.no.
Du kan også kontakte min veileder Professor Janne Haaland Matlary på epost: j.h.matlary@stv.uio.no

Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste AS.

Med vennlig hilsen

Nils Gaute Prestmo
Oblt/Masterstudent
Forsvarets Høyskole

Samtykke til deltakelse i studien

Jeg har mottatt informasjon om studien, og er villig til å delta

---------- ----------

(Sted og dato) (Signatur)

Vedlegg B Intervjuguide

Teoretisk ståsted

Hvordan vil du definere et cyberangrep?

Er det sannsynlig at vi kan oppleve et «Cyber Pearl Harbor» eller «Cyber 9/11» mot Norge de nærmeste 10 årene?

Hvilke tre utviklingstrekk vil du fremheve innenfor Cybersikkerhet de neste 10 årene?

Nåtidsbetraktninger

Hvordan bidrar dere i dag til å redusere nasjonal risiko i forhold til cybertrusselen?

Hvilke nasjonale fora er med på å koordinere aktiviteter mellom aktørene innenfor cybersikkerhet?

Hva vil være kjennetegn på en cyberkrise?

Hvem bør lede innsatsen i forbindelse med en cyberkrise?

Hva slags cyber hendelser vil utløse en diplomatisk reaksjon mot en annen nasjon?

Fremtid

Hvordan bør nasjonal robusthet utvikles de neste 10 årene? Er det akseptabelt at enkelte aktører i statlig og privat sektor tar større risiko på vegne av fellesskapet?

Hvilke intensiver bør benyttes for å redusere risiko innenfor cybersikkerhet de neste 10 årene?

Hvem bør koordinere og prioritere fysiske maktmidler og digitale ressurser ved en væpnet konflikt i Norge?

Bør nasjonale CERT inkluderes i krigens folkerett som objekt med generell eller spesiell beskyttelse? Objekter med spesiell beskyttelse er av spesiell viktighet for sivilbefolkningen eller objekter som, dersom de blir angrepet, vil medføre spesielt stor risiko for sivile tap.

Litteraturliste

Admiral Haakon Bruun-Hanssen (2015, 12. januar). [Forsvarssjefens statusoppdatering].

Allison, G. (2012). The Cuban Missile Crisis at 50. [Article]. *Foreign Affairs, 91*(4), 11-16.

Allison, G. T. (1971). *Essence of decision: explaining the Cuban missile crisis*. Boston: Little, Brown.

Arquilla, J., & Ronfeldt, D. (1997). Cyberwar Is Comming! *In Athena's camp: preparing for conflict in the information age* (s. XXIV, 501 s. : ill.). Santa Monica, Calif.: Rand.

Bakken, J. B., & Aarseth, M. B. (2014, 29. august). Laget for sabotasje, *Dagens Næringsliv*, s. 2.

Bakken, J. B., Christensen, I. S., & Ånestad, M. (2014, 27. august). Tidenes hackerangrep i Norge, *Dagens Næringsliv*, s. 2.

Beredskapsloven. (1950). *Lov om særlige rådgjerder under krig, krigsfare og liknende forhold* Hentet fra https://lovdata.no/dokument/NL/lov/1950-12-15-7.

Boin, A. (2008). *Crisis management*. Los Angeles: Sage.

Boin, A., & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. [Article]. *Journal of Contingencies & Crisis Management, 15*(1), 50-59. doi: 10.1111/j.1468-5973.2007.00504.x

Buzan, B., & Waever, O. (2003). *Regions and powers: the structure of international security* (Vol. 91): Cambridge University Press.

CERT-UK. (2015). Cyber-security Information Sharing Partnership (CiSP). Hentet 3. mai, 2015, fra https://www.cert.gov.uk/cisp/

Clapper, J. R. (2013). US Intelligence Community Worldwide Threat Assessment. *US Senate Select Committee on Intelligence*.

Clarke, R. (2009). War From cyberspace. *National Interest*.

Clarke, R. A., & Knake, R. (2010). *Cyber war: the next threat to national security and what to do about it*. New York: Ecco.

Colbjørnsen, T. (2004). *Ledere og lederskap: AFFs lederundersøkelser*. Bergen: Fagbokforl.

Departementene. (2012). *Nasjonal strategi for informasjonssikkerhet*. Oslo: Hentet fra https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf.

Direktoratet for forvaltning og IKT. (2014). *Mot Alle odds? Veier til samordning i norsk forvaltning*. Difi Hentet fra http://www.difi.no/sites/difino/files/mot-alle-odds.-veier-til-samordning-i-norsk-forvaltning-difi-rapport-2014-7.pdf.

Direktoratet for samfunnssikkerhet og beredskap. (2014). *Nasjonalt risikobilde 2014*. Tønsberg: Direktoratet for samfunnssikkerhet og beredskap.

Direktoratet for samfunnssikkerhet og beredskap. (2015). Tilsyn. Hentet 21. mai, 2015, fra http://www.dsb.no/no/Ansvarsomrader/Nasjonal-beredskap/Tilsyn/

Dokument 8:147S (2011-2012). (2012). *Representantforslag 147S*. Oslo: Stortinget Hentet fra https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Representantforslag/2011-2012/dok8-201112-147/.

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

Ekspertgruppen for forsvaret av Norge. (2015). *Et felles løft*. Hentet fra https://blogg.regjeringen.no/annedivi/files/2015/03/2015-04-27-Et-Felles-L%C3%B8ft-webversjon.pdf.

ENISA. (2015). National Cyber Security Strategies in the World Hentet 18. april, 2015, fra https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

Etterretningstjenesten. (2015). *Fokus 2015. Etterretningstjenstens vurdering*. Hentet fra https://forsvaret.no/ForsvaretDocuments/FOKUS2015-endelig.pdf.

Fackler, M. (2014, Dec 28). North Korea Accuses U.S. of Staging Internet Failure, *New York Times*. Hentet fra http://search.proquest.com/docview/1640597714?accountid=8017

FDs cyberretningslinjer. (2014). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i Forsvaret*.

Fimreite, A. L. (2011). *Organisering, samfunnssikkerhet og krisehåndtering*. Oslo: Universitetsforl.

Fimreite, A. L., Lango, P., Lægreid, P., & Rykkja, L. H. (2012, 23. august). Uklart frå kommisjonen, Kronikk, *Dagens Næringsliv*.

Forsvarets høgskole/Forsvarets stabsskole. (2013). *Manual i krigens folkerett*. Oslo: Forsvarssjefen.

Forsvarsdepartementet. (2009). *Evne til innsats: strategisk konsept for Forsvaret*. Oslo: Forsvarsdepartementet.

Forsvarsdepartementet. (2012). *Et forsvar for vår tid - Iverksettingsbrev til forsvarssektoren for langtidsperioden 2013–2016*. Hentet fra https://www.regjeringen.no/globalassets/upload/fd/ivbltp.pdf.

Forsvarsdepartementet, & Justis- og beredskapsdepartementet. (2015). *Støtte og samarbeid - En beskrivelse av totalforsvaret i dag*. Oslo: Hentet fra https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/rapporter-og-regelverk/fd_stotte-samarbeid_web_april.pdf.

Forsvarsstaben. (2014). *Forsvarets fellesoperative doktrine*. Oslo: Forsvarets stabsskole (FSTS), Forsvarets høgskole (FHS).

Forum of Incident Response and Security Teams. (2015). FIRST Members around the world. Hentet 19. april, 2015, fra https://www.first.org/members/map#NO

Foss, A. B., Johansen, P. A., & Hager-Thoresen, F. (2014, 15. desember). Spionutstyr plassert i Norges fremste finansmiljø *Aftenposten*, s. 1.

Franke, U. (2015). War by non-military means.

Friis, K. (2015, 6. mai). Tamt ekspertutvalg om Forsvaret, Kronikk. Hentet fra http://www.nrk.no/ytring/tamt-ekspertutvalg-om-forsvaret-1.12345243

Generalmajor Odd Egil Pedersen (2015, 2. februar). [Gir IKT-satsingen til Forsvaret en forsvarbar informasjonsinfrastruktur og et fundament for moderne militære operasjoner?].

Goncharov, K. (2015). Mothership unlocked: The Equation APT. Hentet 8. mai, 2015, fra https://business.kaspersky.com/mothership-unlocked-the-equation-apt/3608

Grunnloven. (1814). Kongeriket Norges Grunnlov.

Gustavsen, I. H. (2014). *Sivilit-militært samarbeid i en cyberkrise.* Masteroppgave, Forsvarets høgskole, Ingunn Harildstad Gustavsen, Oslo.

Hagen, J. M., Fridheim, H., & Grunnan, T. (2010). *(U) Sikkerheitspolitisk krise, nasjonal kriseleiing og sivilmilitært samarbeid*. Kjeller: Forsvarets forskningsinstitutt (FFI).

Hotvedt, S. K. (2015, 17. mars). Advarer 800 norske sjefer im digitale trusler og dataspionasje, *NRK.no*. Hentet fra http://www.nrk.no/norge/advarer-800-norske-sjefer-om-dataspionasje-1.12263945

Instruks for dep.arbeid med samfunnssikkerhet mv. (2012). *Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering*.

Instruks om Forsvarets bistand til politiet. (2012). *Instruks om Forsvarets bistand til politiet*.

Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser?: innføring i samfunnsvitenskapelig metode* (Vol. 2): Høyskoleforlaget Kristiansand.

Johansen, I. (2010). *Scenarioklasser - Forvsarsstudien 2007*. (FFI Rapport 2006/02664). Kjeller: Forsvarets forskningsinstitutt.

Jørgenrud, M. (2015, 18. mars). PST ber om skadevare og Snowden ødela, *Digi.no*. Hentet fra http://www.digi.no/sikkerhet/2015/03/18/pst-ber-om-skadevare-og-snowden-odela

Kenney, M. (2015). Cyber-Terrorism in a Post-Stuxnet World. *Orbis, 59*(1), 111-128.

Klimburg, A. (2012). *National cyber security framework manual*: NATO Cooperative Cyber Defense Center of Excellence.

Krepinevich, A. F. (2012). *Cyber Warfare: A «Nuclear Option»?* Washington D.C.: Center for Strategic and Budgetary Assessments.

Krigsskueplass. (2009). Store norske leksikon Hentet fra https://snl.no/krigsskueplass

Krise. (2009). Store norske leksikon Hentet fra https://snl.no/krise

Langberg, Ø. K. (2014, 16. desember). Dette har de forskjellige sikkerhetsorganene ansvar for, *Aftenposten*. Hentet fra http://www.aftenposten.no/nyheter/iriks/Dette-har-de-forskjellige-sikkerhetsorganene-ansvar-for-7829402.html

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *Security & Privacy, IEEE, 9*(3), 49-51.

Langø, H.-I. (2013). Den akademiske debatten om cybersikkerhet: Hans-Inge Langø. *Internasjonal politikk, 71(2013)nr. 2*, S. 229-240.

Lee, D. (2014, 5. mars). Russia and Ukraine in cyber 'stand-off', *BBC*. Hentet fra http://www.bbc.com/news/technology-26447200

Lindeberg, A. (2015, 27. januar). Frykter annen storeier i Telenor. Hentet fra http://www.dn.no/nyheter/politikkSamfunn/2015/01/27/2114/Telenor/frykter-annen-storeier-i-telenor

Madsen, P. A. (2014, 17 desember). Når ansvar pulveriseres, Kommentar, *Aftenposten*, s. 1.

Matlary, J. H. (2015, 14. januar). Uten sikkerhet, ingen frihet, Kronikk, *Dagens Næringsliv*.

McMahon, J. (2014). An Analysis of the Characteristics of Cyber Attacks. *Discovery, Invention & Application*(1).

Meld. St. 24 (2010-2011). (2011). *Samarbeidet i NATO i 2010: Tilråding frå Utanriksdepartementet av 27. mai 2011, godkjend i statsråd same dagen. (Regjeringa Stoltenberg II).* Hentet fra http://www.regjeringen.no/nb/dep/ud/dok/regpubl/stmeld/2010-2011/meld-st-24-20102011.html?id=644588.

Meld. St. 29 (2011-2012). (2012). *Samfunnssikkerhet: Tilråding fra Justis- og beredskapsdepartementet 15. juni 2012, godkjent i statsråd samme dag. (Regjeringen Stoltenberg II).*

Nasjonal sikkerhetsmyndighet. (2014). Rapport om sikkerhetstilstanden 2014.

National Coordinator for Security and Counterterrorism. (2013). *National Cyber Security Strategy 2 - From awareness to capability*. NCSC Hentet fra https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf.

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

NATO. (2013a). Cyberwar - does it exist? Hentet 18. februar, 2015, fra http://www.nato.int/docu/review/2013/Cyber/Cyberwar-does-it-exist/EN/index.htm

NATO. (2013b). NATO Cyber Defence *Media Backgrounder* (s. 2).

NOU 2000:24. (2000). *Et sårbart samfunn - Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Oslo.

NOU 2006:6. (2006). *Når sikkerheten er viktigst - Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner: Innstilling fra utvalg oppnevnt ved kongelig resolusjon 29. oktober 2004.*

NOU 2012:14. (2012). *Rapport fra 22. juli-kommisjonen*. Oslo: Hentet fra http://www.regjeringen.no/nb/dep/smk/dok/nou-er/2012/nou-2012-14.html?id=697260.

Petersson, M. (2013). Just an Internal Exercise? NATO and the "New" Security Challenges. I E. Hallams, L. Ratti & B. Zyla (Red.), *NATO beyond 9/11: the transformation of the Atlantic Alliance* (s. X, 347 s.). Basingstoke: Palgrave Macmillan.

Politiets sikkerhetstjeneste. (2015). *Åpen trusselvurdering 2015*. Hentet fra http://www.pst.no/media/75480/PSTs_tv2015.pdf.

Prop. 1 S (2014-2015). (2014). *FOR BUDSJETTÅRET 2015: Tilråding fra Forsvarsdepartementet 12. september 2014, godkjent i statsråd samme dag. (Regjeringen Solberg)*.

Prop. 73 S (2011-2012). (2012). *Et forsvar for vår tid: Tilråding fra Forsvarsdepartementet 23. mars 2012, godkjent i statsråd samme dag. (Regjeringen Stoltenberg II)*.

Prop. 79 L (2014-2015). (2015). *Endringer i politiloven (bistand fra Forsvaret)*. Oslo.

Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies, 35*(1), 5-32.

Rosenbaum, R. (2012). Richard Clarke on Who Was Behind the Stuxnet Attack. *Smithsonian Magazine*.

Sanger, D. E., & Perlroth, N. (2014, 2014 Dec 18). U.S. Is Said to Find North Korea Behind Cyberattack on Sony, *New York Times*. Hentet fra http://search.proquest.com/docview/1637440629?accountid=8017

Security and Defence Committee. (2013). *Finland's Cyber Security Strategy*. Secretariat of the Security and Defence Committee Hentet fra https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf.

Senel, E., Hirsti, K., & Bruland, R. S. (2015). Strømmen tilbake i Istanbul, *NRK.no*.

Senter for cyber- og informasjonssikkerhet (2014). Informasjonssikkerhet, cybersikkerhet, datasikkerhet – hva er forskjellen? Hentet 13. januar, 2015, fra https://ccis.no/nb/informasjonssikkerhet-cybersikkerhet-datasikkerhet-hva-er-forskjellen/

Sikkerhet. (2013). Store norske leksikon Hentet fra https://snl.no/sikkerhet

Skillingshaug, A. (2011). *Fortsatt ansvarsprinsipp eller helhetlig tilnærming til cybersecurity i Norge?* Masteroppgave, Forsvarets høgskole, Arild Skillingshaug, Oslo.

Skogan, J. K. (2011). Sikkerhetspolitiske mål og virkemidler. I J. Hovi & R. Malnes (Red.), *Anarki, makt og normer: innføring i internasjonal politikk* (s. 423 s. : ill.). Oslo: Abstrakt forl.

St. meld. 22 (2007-2008). (2008). *Samfunnssikkerhet - Samvirke og samordning*.

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

St.meld. nr. 37 (2004–2005). (2005). *Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering*. Oslo: Hentet fra https://www.regjeringen.no/contentassets/4867117e76b94e948426aa25d895cbde/no/pdfs/stm200420050037000dddpdfs.pdf.

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

Sveinung Berg Bentzrød. (2015, 20. mars). Wilhelmsen-gruppen blir en del av det norske forsvaret, *Aftenposten*. Hentet fra http://www.aftenposten.no/nyheter/iriks/Wilhelmsen-gruppen-blir-en-del-av-det-norske-forsvaret-7949688.html

The Washington Treaty. (1949). *The North Atlantic Treaty*. NATO Hentet fra http://www.nato.int/cps/en/natohq/topics_67656.htm?

The White House Office. (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked Worldr*: White House.

Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A.-M., & Vihul, L. (2008). Cyber attacks against Georgia: Legal lessons identified. *Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, at http://www. carlisle. army. mil/DIME/documents/Georgia, 201*, 200.

Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and their Classification. *IJ Network Security, 15*(5), 390-396.

Yost, D. S. (2010). NATO's evolving purposes and the next Strategic Concept. *International affairs*, *86*(2), 489-522.

Zetter, K. (2015, 22. februar). How the NSA's Firmware Works and Why It's so Unsettling. Hentet 8. mai, 2015, fra http://www.wired.com/2015/02/nsa-firmware-hacking/