MILITÆRE STUDIER
FORSVARETS STABSSKOLE
2
2015

Når samfunnet lammes

Militær bistand ved et dataangrep

Ingunn Harildstad Gustavsen

Forsvarets stabsskole (FSTS)

Akershus festning, bygning 10, Postboks 1550 Sentrum, 0015 Oslo, Norge

Forsvarets stabsskole er en del av Forsvarets høgskole (FHS). Som faglig uavhengig høgskole utøver FHS sin virksomhet i overensstemmelse med anerkjente vitenskapelige, pedagogiske og etiske prinsipper (jf. Lov om universiteter og høgskoler § 1—5).

Sjef Forsvarets stabsskole: flaggkommandør Jan Østensen Berglund

Militære studier er en militærfaglig tidsskriftserie innenfor Forsvarets stabsskoles ulike fagområder. Alle synspunkter, vurderinger og konklusjoner som fremkommer i denne publikasjonen står for forfatterens egen regning. Hel eller delvis gjengivelse av innholdet kan bare skje med forfatterens samtykke.

Ansvarlig redaktør: oberstløytnant Tormod Heier (PhD)
Ass. redaktør: Yngvild Sørbye

Norwegian Defence Command and Staff College

Akershus festning, bygning 10, Postboks 1550 Sentrum, 0015 Oslo, Norway

The Norwegian Defence Command and Staff College is part of the Norwegian Defence University College (FHS). As an independent university college, FHS conducts its professional activities in accordance with recognized scientific, pedagogical and ethical principles (pursuant to the Act pertaining to Universities and University Colleges, section 1—5).

Chief Norwegian Defence Command and Staff College: Commodore Jan Østensen Berglund

Militære studier is an independent military journal attached to the Norwegian Defence Command and Staff College's broad portfolio of professional interests. All views, assessments and conclusions which appear in this publication are the author's own. The author's permission is required for any reproduction, wholly or in part, of the contents.

Editor-in-chief: Lieutenant Colonel Tormod Heier (PhD)
Assistant editor: Yngvild Sørbye

hogskolene.forsvaret.no/forsvarets-hogskole/avdelinger/fsts/Sider/fsts.aspx

Når samfunnet lammes
Militær bistand ved et dataangrep

Ingunn Harildstad Gustavsen

Utgiver
Forsvarets stabsskole/FHS
Redaksjon
Oberstløytnant Tormod Heier (ansv.)
Yngvild Sørbye
Grafisk design
commandogroup.no
ISSN
1894-2547

Forsidebilde
Vinterøvelse ved Forsvarets Ingeniørhøgskole 2015.
Foto
Daniel Nordby, Forsvarets mediesenter
Trykk
07 Media – 07.no
Henvendelser om skriftserien kan rettes til
Forsvarets stabsskole/Forsvarets høgskole
post.fhs@mil.no

Forfatteren

Ingunn Harildstad Gustavsen har bakgrunn fra Hærens tekniske fagskole/elektronikk og har mange års erfaring med drift og forvaltning av IKT-materiell, både nasjonalt og innen NATO. Hun har tjenestegjort ved Sambandsbataljonen i Indre Troms, Joint Headquarter North/Forsvarskommando Sør-Norge og Forsvarets logistikkorganisasjon i Stavanger. I 2009 ble Gustavsen sivilt ansatt ved FLO IKT-kapasiteter på Kolsås. Hun gjennomførte sin toårige masterutdanning ved Forsvarets høgskole i 2012—2014.

Summary

This study examines the role of military support to civil authorities in the event of a national cyber crisis in Norway, with special emphasis on the Norwegian Cyber Force.

In later years, Norway's nationwide mobile network has collapsed at several occasions. In March 2013, it was revealed that the Norwegian telecom corporation, Telenor, was itself exposed to industrial espionage. The ensuing investigation unveiled a sophisticated Indian cyber attack infrastructure compromising corporations and governments worldwide.

In principle, Norway's military should defend the nation against external threats, whereas the police should handle domestic threats. The police, however, have neither sufficient resources nor the competence to handle large-scale cyber terrorism. The Norwegian Cyber Force, on the other hand, has technology, expertise and experience from operating, monitoring and defending its own nationwide infrastructure.

In the event of a cyber crisis, coordinating expert organs such as the Norwegian National Security Authority with its CERT will step in (the NSA reporting both to the Minister of Defence and the Minister of Justice). Regular civil-military cooperation and exercise is vital to preventing security threats, as was shown in the autumn of 2013, when Telenor initiated a large-scale exercise together with NorCERT, the police, several banks, private computer security companies, and the Norwegian Cyber Force. If civilian e-com infrastructure is targeted by an attack that puts vital social interests, life or health in danger, the Norwegian Cyber Force will be able to support the civil authorities with various special competencies, ranging from smaller teams of advisors to large military units.

Keywords: civil-military cooperation, cyber attack, cyber crisis, telecommunications, civilian infrastructure, Norwegian Cyber Force, Telenor, NorCERT, military support, cyber terrorism

Innhold

Redaktørens forord

Kjære leser!

I denne utgaven av *Militære studier* ser vi nærmere på selve sentralnervesystemet i den norske forsvarsevnen: IKT-infrastrukturen. Dersom dette systemet bryter sammen, vil ikke bare Norges forsvarsevne forvitre. Også samfunnet slik vi kjenner det i dag vil gå i stå. Strømforsyning til de tusen hjem, innkjøp og bankoverføringer, telekommunikasjon, trafikkstyring av fly, tog og båter, trygde- og lønnsutbetalinger, mat- og medisintilførsler, olje- og gassleveranser til utlandet og en uendelig rekke andre forhold vil også bli påvirket. Siden dette berører din og min sikkerhet direkte, ligger det et stort ansvar på våre politiske og militære myndigheter om å ta grep.

Men handling viser seg vanskelig. Fragmentering av roller og ansvar, mellom hvem som gjør hva, på tvers av sivil-militære, sektorbestemte og profesjonsbaserte skillelinjer, gjør moderne stater sendrektige og sårbare i forhold til trusselen rundt oss. Det er et paradoks at den største trusselen mot norsk sikkerhet i cyberdomenet ikke kommer utenfra, men innenfra. Et utall av sivile og militære leverandører av IKT jobber hver for seg ut fra de beste hensikter, men i sum skaper de dysfunksjonelle organisasjoner som ikke kan kommunisere med hverandre. Bare innad i Forsvaret finnes det nærmere 200 forskjellige IKT-systemer som ikke kan «snakke sammen». I Forsvarets øverste ledelse sitter mange generaler som alle har en aksje i IKT-ansvaret, men som hver for seg opererer med konkurrerende mål og sprikende prioriteringer. Lignende forhold preger etter all sannsynlighet statsforvaltningen for øvrig.

Sivil-militær samordning på IKT-feltet er derfor av strategisk betydning — ikke bare for Forsvarets operative evne isolert sett, men for politikernes evne til å ivareta innbyggernes grunnleggende behov for trygghet dersom Norge angripes i cyberdomenet. Derfor er også uttalelsene fra vår nåværende sjef i Cyberforsvaret, generalmajor Odd Egil Pedersen, urovekkende: Forsvaret klarer ikke å utnytte cyberdomenet til beste for landets sikkerhet. Og verre kan det bli med budsjettreduksjoner på IKT-siden på mellom 50 og 70 prosent i årene som kommer.

Tormod Heier
Redaktør/oberstløytnant
Forsvarets stabsskole/Forsvarets høgskole

Kapittel 1
Innledning

Spørsmålet er ikke lenger *om* vi vil rammes av en cyberkrise, men *når* krisen inntreffer. Det er inntrykket man sitter igjen med etter Dagbladets artikkelserie «Null CTRL» høsten 2013. I løpet av serien, som omhandlet IKT-sikkerhet i Norge, avslørte avisen at over 2500 styringssystemer var koblet til internett med minimal eller ingen sikkerhet (Karlsen, 2013). 500 av disse systemene kontrollerte industriell eller samfunnskritisk infrastruktur.

I forbindelse med artikkelserien ble daværende sjef for Cyberforsvaret, generalmajor Roar Sundseth, intervjuet. Sundseth uttalte at angrep mot norsk infrastruktur ikke kan utelukkes. Han påpekte at verken Norge eller særlig mange andre land har sett omfattende angrep ennå, men at muligheten er der: «Trusselen er stor, og den er økende» (Hillestad og Sandli, 2013).

Sundseths vurdering samsvarer godt med rapporter fra Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets etterretningstjeneste (E-tjenesten). NSM rapporterer om et økende antall detekterte forsøk på dataangrep og datainnbrudd i kritisk infrastruktur. I 2013 håndterte sikkerhetsmyndigheten 50 alvorlige digitale infiltrasjonsforsøk (NSM, 2014b, s. 4).

E-tjenesten beskriver trusler i det digitale rom som «særlig relevant» for norsk sikkerhet og nasjonale interesser: «Digitale operasjoner kan rettes mot infrastruktur eller styringssystemer og forårsake forstyrrelser, fysisk skade eller ødeleggelse» (Etterretningstjenesten, 2014, s. 59).

Temaet for denne studien er sivil-militært samarbeid i en cyberkrise. Oppgaven fokuserer på Cyberforsvarets rolle dersom sivil elektronisk kommunikasjonsinfrastruktur (ekom-infrastruktur) rammes av et cyberangrep[1]. Når kan Cyberforsvaret bistå, og hva kan det bistå med?

Nasjonal krisehåndtering og regulering av sivil-militært samarbeid er i utgangspunktet uavhengig av domenet krisen oppstår i. Det etablerte systemet utgjør følgelig det teoretiske grunnlaget for å kunne drøfte Cyberforsvarets rolle i en cyberkrise.

Cyberangrep er vanskelige å definere. Slike angrep kan ligge i en gråsone mellom kriminell virksomhet og krigshandlinger, mellom politiets og Forsvarets ansvarsområder. Hovedregelen er at cyberangrep mot sivil infrastruktur håndteres av sivile myndigheter inntil Regjeringen beslutter noe annet. Samtidig vil politiet ofte ha begrenset kompetanse og ressurser til å kunne håndtere pågående cyberangrep.

Det moderne velferdssamfunnet vårt avhenger av elektronisk kommunikasjonsinfrastruktur (ekom-infrastruktur) for å fungere. IKT utgjør grunnmuren for samhandling nasjonalt og internasjonalt. I Norge ble erkjennelsen av samfunnets teknologiske avhengighet og begrepet *et sårbart samfunn* for alvor etablert med utgivelsen av Sårbarhetsutvalgets rapport i 2000 (NOU 2000: 24). Utvalget ble oppnevnt av Bondevik-regjeringen og ledet av Kåre Willoch. Sårbarhetsutvalget slo fast at kritiske samfunnsfunksjoner vil bryte sammen uten elektronisk kommunikasjon. Utfordringene knyttet til et *sårbart samfunn* er like aktuelle i dag som i 2000.

En av de kritiske samfunnsfunksjonene er informasjons- og ledelsesapparatet som trer i kraft ved kriser. Kriseapparatets behov for ekom-tjenester ble særlig bekreftet av to hendelser i 2011. I juni 2011 førte en logisk feil i en server til at Telenors mobilnett falt ut i 18 timer, samtidig som Østlandet var rammet av storflom. I romjulen samme år førte orkanen «Dagmar» til at omkring 20 000 husstander ble uten fasttelefon og 7500 uten internett/bredbånd.

[1] I denne oppgaven skal cyberangrep forstås som målrettede angrep med ulike formål, herunder både spionasje og sabotasje, se kapittel 1.2. Begrepsbruken er imidlertid stadig under utvikling, oppgaven kommer nærmere inn på dette i kapittel 4.

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

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

Ingen av de nevnte hendelsene var tilsiktet. Samtidig tilsier dagens trusselbilde at det finnes aktører som vil ønske å ramme kritisk infrastruktur digitalt. Et slikt cyberangrep kan skje i form av spionasje eller sabotasje via nett. Det er kriminelle aktører som står bak de fleste ulovlige aktivitetene på nett i dag, men Forsvaret hevder at det er nasjonalstater som utgjør den største trusselen (Etterretningstjenesten, 2014; Hillestad og Sandli, 2013). Statene driver etterretningsaktivitet for å ivareta egen nasjonal sikkerhet, samtidig som det også foregår spionasje for å fremme kommersielle mål. Denne typen spionasje skiller seg fra øvrig kriminalitet i cyberdomenet ved å være både mer målrettet og langt mer avansert (Johnsen og Kveberg, 2014, s. 36).

Et eksempel på avansert spionasje er kjent fra den britiske etterretningstjenesten. En artikkel i *Der Spiegel* i september 2013[2] indikerer at det nasjonale byrået Government Communications Headquarters (GCHQ) skal ha stått bak et omfattende hacker-angrep[3] mot Belgacom. Belgacom er Belgias svar på Telenor — landets største telekommunikasjonsselskap og delvis statlig eid (Knudsen, 2013). Belgacoms ansatte ble lurt til et nettsted hvor de fikk installert ondsinnet programvare på datamaskinene sine. Datamaskinene ble så brukt som utgangspunkt for videre spionasje mot de delene av infrastrukturen de hadde tilgang til. Målet var tilsynelatende å få tilgang til en sentral nettverkskomponent som håndterte internasjonal trafikk. GCHQ skal ha vært ute etter å kartlegge Belgacoms infrastruktur og legge til rette for avansert utnyttelse av mobiltelefonbrukere (Spiegel, 2013).

Johnsen og Kveberg stiller i rapporten *Cyberdomenet, cybermakt og norske interesser* spørsmål om hvorvidt stater risikerer å påvirke stabiliteten i andre staters infrastruktur ved slike etterretningsoperasjoner (Johnsen og Kveberg, 2014, s. 26). Hvem vil ha ansvar, myndighet og virkemidler til å håndtere situasjonen i Norge, dersom digitale operasjoner rettes mot norsk kommunikasjonsinfrastruktur?

Problemstilling

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

Nasjonal beredskaps- og krisehåndtering har fått stor oppmerksomhet etter terroranslagene 22. juli 2011. «Aldri mer 22/7» er nærmest blitt et mantra.

[2] Basert på dokumenter lekket fra NSA-varsleren Edward Snowden.
[3] Å *hacke* vil si å bryte seg inn i datasystemer og -nettverk som man ikke har lovlig tilgang til.

Utfordringen relatert til «ressursene som ikke fant hverandre» var knyttet til det fysiske domenet i juli 2011 (NOU 2012: 14). Ville ressursene ha funnet hverandre i dag dersom krisen oppsto i det digitale domenet? Tar dagens regulering av det sivil-militære samarbeidet høyde for cybertrusselen?

Gjennom *Nasjonal strategi for informasjonssikkerhet* (2012) ga regjeringen sin beskrivelse av sikkerhetsutfordringene og hvilke områder den ville vektlegge. I dokumentet påpekes det at dagens utfordringer krever en helhetlig tilnærming og grenseoverskridende tiltak. Den nye regjeringen støtter dette og sier at den ønsker å stille Forsvarets ressurser til disposisjon for nasjonal krisehåndtering — og «koble Cyberforsvaret inn i sivil cybersikkerhet hvor dette er hensiktsmessig» (Høyre-Frp-regjeringen, 2013, s. 40).

Men hva ligger det egentlig i å «koble inn» Cyberforsvaret, og når vil det kunne være hensiktsmessig? Spørsmålene leder frem til følgende problemstilling:

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

For å kunne besvare denne problemstillingen er det nødvendig å ha kunnskap om hvordan kriser prinsipielt håndteres i Norge og hva som regulerer bruken av militære ressurser i fredstid. Utgangspunktet er at nasjonal krisehåndtering og regulering av sivil-militært samarbeid er uavhengig av domenet krisen oppstår i. Blant de bestemmelser som regulerer sivil-militært samarbeid, står *bistandsinstruksen*[4] særlig sentralt. Det er ikke gitt at dette systemet er tilpasset cyberhendelser, men håndteringen av cyberhendelsene må likevel forholde seg til etablerte prinsipper og gjeldende bestemmelser. Forståelse for dette systemet er viktig; det utgjør det teoretiske grunnlaget for å kunne drøfte Cyberforsvarets rolle i en cyberkrise og vil derfor vies relativt stor plass i studien.

[4] *Instruks om Forsvarets bistand til politiet* regulerer det operative samarbeidet mellom Forsvaret og politiet. «Det er oppgåva til politiet å hindre allmenn kriminalitet, her under terrorhandlingar. For Forsvarsdepartementet (FD) er det viktig at det er og skal vera eit skarpt skilje mellom sivile og militære oppgåver. Når det er sagt, finst det årsakar til at Forsvaret likevel i enkelte høve kan hjelpe politiet i dette arbeidet. Dette er regulert i den nemnde instruksen» (Regjeringen, 2013b).

Oppgaven er løst som en kvalitativ studie, en kombinasjon av innholdsanalyse, casestudier og intervjuer. Selve undersøkelsen vil gjennomføres i tre deler (tilsvarende kapittel 4—6). Den første skal bidra til økt kunnskap om ekom-infrastruktur og cyberdomenet. Jeg vil se på hva ekom-infrastruktur er og hvorfor forstyrrelser i, eller ødeleggelse av, sivil ekom-infrastruktur kan forårsake en nasjonal krise — en cyberkrise. Videre vil jeg se nærmere på hva et cyberangrep innebærer og de utfordringer samfunnet vil stå overfor i håndteringen av alvorlige cyberangrep.

For å kunne drøfte Cyberforsvarets rolle er det viktig å ha kjennskap til hvilke andre aktører som innehar roller. Studiens del to vil derfor kartlegge aktører og diskutere ansvar, oppgaver og myndighet knyttet til ekom-infrastruktur og håndtering av cyberangrep. De sivile aktørenes kapasitet vil indikere om de vil få behov for bistand fra Forsvaret eller ei. På samme måte vil Cyberforsvarets oppdrag og kapasiteter gi en god indikasjon på hva det vil kunne bistå med.

Tredje og siste del vil ta for seg to caser som innebar cyberangrep mot sivil infrastruktur, analysere hvordan disse ble håndtert og hvilken støtte det viste seg å være behov for. Caseanalysen vil ha fokus på de oppgavene som er vektlagt i *Nasjonal strategi for informasjonssikkerhet*, herunder å oppdage, analysere, koordinere og håndtere. De oppgaver hvor det viste seg å være behov for støtte vil så drøftes fortløpende. Har Cyberforsvaret kunnskap og verktøy til å kunne støtte, og kan Cyberforsvaret bistå gitt dagens prinsipper for krisehåndtering og regulering av Forsvarets bistand til det sivile samfunn?

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

Definisjoner

I studien brukes en del begreper som det vil være nyttig å definere.

Cyberdomenet, også kalt det digitale rom, forstås som fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data. *Cyber* er et prefiks som indikerer at en aktivitet foregår i cyberdomenet.

Cyberangrep skal i denne studien forstås som målrettede angrep med ulike formål, herunder både spionasje og sabotasje. Cyberangrep som rammer samfunnskritisk infrastruktur, samfunnskritisk informasjon eller samfunnskritiske funksjoner på en slik måte at det får betydning for samfunnets og befolkningens trygghet, defineres som *alvorlige cyberhendelser*. Begrepsbruken er under stadig utvikling, og jeg har valgt å basere meg på Forsvarsdepartementets definisjoner slik de er gitt i FDs cyberretningslinjer: Med cyberangrep forstås handlinger i eller gjennom cyberdomenet som har til hensikt å skade eller påvirke personell, materiell eller konfidensialiteten, integriteten, tilgjengeligheten eller autentisiteten til et informasjonssystem (FD, 2014, s. 5). Dette utdypes i kapittel 4.

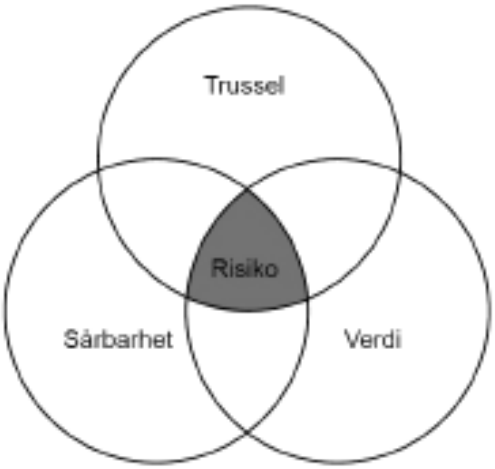
Begrepene *elektronisk kommunikasjon* (ekom) og *telekommunikasjon* brukes gjerne om hverandre. EKOM ble først tatt i omfattende bruk i forbindelse med utarbeidelse av Ekomloven, som erstattet den tidligere Teleloven. Telekommunikasjon er fremdeles et mye brukt begrep, men oppfattes likevel ofte snevrere og mer opphengt i tidligere systemer og tjenester.[5] Ekom-nett defineres i Ekomloven til å være et «system for signaltransport som muliggjør overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel der radioutstyr, svitsjer, annet koblings- og dirigeringsutstyr, tilhørende utstyr eller funksjoner inngår, herunder nettverkselementer som ikke er aktive» (Ekomloven, 2003: § 1—5).

Trussel, sårbarhet, verdi og risiko:

Trussel er sannsynligheten for å bli utsatt for et angrep. Sannsynligheten for å bli utsatt for en tilsiktet uønsket handling kan ikke vurderes på samme måte som sannsynligheten for naturhendelser og ulykker. Sannsynligheten for et cyberangrep vil avhenge av de til enhver tid aktive trusselaktører, deres intensjoner og kapasitet som antas å foreligge for å gjennomføre uønskede

[5] I en historisk beskrivelse er det imidlertid mest korrekt å benytte begrepet tele/telekommunikasjon (Nystuen og Fridheim, 2007, s. 9).

handlinger og oppnå bestemte mål. Trusselnivået er ingen statisk størrelse, men kan endres fra dag til dag (DSB, 2013a, s. 7). Trusselaktørene er globale og spenner fra statlige etterretnings- og sikkerhetstjenester via tradisjonelle militære motstandere, globale næringsbedrifter, terrorist- og ekstremistgrupper til organiserte hackergrupper og enkeltpersoner (E-tjenesten, NSM og PST, 2013, s. 9).



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

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

Verdier er størrelser vi av ulike hensyn ønsker å beskytte. Dette kan være alt fra liv og helse til fysiske objekter og infrastruktur, eller også abstrakte verdier som omdømme og operativ evne. Da de fleste samfunnssektorer er avhengige av kraft og telekommunikasjon, har noen samfunnskritiske virksomheter verdier som er viktige for hele samfunnet. Bortfall av disse verdiene vil ha konsekvenser for hele samfunnet, direkte eller indirekte.

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

Forskningsstatus

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

I forbindelse med BAS5 gjennomførte fire forskere ved FFI i 2007 en grundig analyse og beskrivelse av sårbarhetene i internettinfrastrukturen. I denne rapporten, *Sårbarheter i Internett*, deles sårbarhetene inn i fire kategorier: fysiske[6], logiske og sosiale[7] sårbarheter samt avhengigheter[8] (Windvik et al., 2007, s. 23). Som påpekt i rapporten vil et angrep kunne utnytte og ha effekter i flere av disse dimensjonene.

Logiske sårbarheter omfatter sårbarheter realisert i programvare, herunder protokoller og tjenester samt logisk redundans. Angrepsmidler mot logiske sårbarheter kan være «alt fra utnyttelse og bruk av allmenn tilgjengelig infrastruktur og kode som publiserte nettverksverktøy på Internett, til angrepskode og mer spesialskrevne verktøy» (Windvik et al., 2007, s. 23). Det presiseres at alle komponenter som kjører programvare, og alle systemer som helt eller delvis styres via programvare, kan være sårbare. Det er angrepsmidler mot logiske sårbarheter som har fokus i denne studien.

I tilknytning til det samme BAS-prosjektet forsket Lene Borgen og Kristin Mørkestøl på hvilke aktører som kan bli involvert i en IKT-krise på nasjonalt

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

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

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

nivå i Norge, samt hvilke ansvar, myndighet og virkemidler de forskjellige aktørene har (Bogen og Mørkestøl, 2005). Forfatterne erfarte at selv om konsekvensene på mange måter er de samme om hendelsen skyldes ekstremvær eller angrep, vil årsaken til krisen kunne påvirke hvilke virkemidler som tas i bruk og Forsvarets rolle i håndteringen (Bogen og Mørkestøl, 2005, s. 11). Etter deres vurdering var det høy terskel for å sette inn Forsvaret i krisehåndteringen. Det nærmer seg ti år siden dette arbeidet ble utført, og siden da har avhengigheten til IKT økt. Maskinvare og programvare er blitt mer avansert, mer tilgjengelig og i større grad integrert i folks dagligliv. Terskelen for å bruke Forsvarets ressurser i krisehåndtering kan ha endret seg, og tillegg har Cyberforsvaret blitt etablert. Forsvaret vil derfor kunne få en annen rolle dersom nasjonen rammes av en IKT-krise[9] i dag.

Denne studien vil drøfte Cyberforsvarets rolle dersom sivil infrastruktur skulle bli utsatt for et cyberangrep i dag.

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

I 2010 publiserte FFI en studie av nasjonal kriseledelse og sivil-militært samarbeid. Forskerne påpekte utfordringer knyttet til ansvar og roller i kriseledelsen, og hevdet at Norge manglet en god strategi for hvordan vi skal håndtere et omfattende IKT-angrep (Fridheim, Grunnan og Hagen, 2010). Regjeringen har i ettertid gitt ut *Nasjonal strategi for informasjonssikkerhet*. Den foreliggende studiens ambisjon var opprinnelig å undersøke om strategien har bidratt til å avklare hvordan et alvorlig cyberangrep mot sivil ekom-infrastruktur skal håndteres. Ansvarsforholdene mellom de forskjellige instanser er imidlertid fortsatt noe uklare. Det finnes også ellers lite offentlig tilgjengelig forskningsmateriale som sier noe om studiens tema, men det pågår flere interessante forskningsprosjekter som vil berøre samme problemstilling.

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

Parallelt med BAS-prosjektene har Forskningsrådet kjørt et program for samfunnssikkerhet og risiko — *SAMRISK.* SAMRISK ble sluttført i juni 2011, men Forskningsrådet uttalte senere at terrorangrepene 22. juli bidro til å anskueliggjøre at det stadig er behov for oppdatert forskning. Rådet påpekte samtidig at den fremtidige forskningen på samfunnssikkerhet ikke må ha for stor fokus på forrige krise: «Neste gang en krise rammer kan det være på et helt annet område som krever en helt annen type kunnskap, andre reaksjoner eller tiltak» (Forskningsrådet, 2013).

Cybertrusler er et av Forskningsrådets nye prioriterte forskningstemaer. Med rådets ord er det «behov for mer kunnskap om aktører, operasjonsmodus, konsekvenser, scenarier og muligheter for forebygging gjennom beskyttelse, avverging og andre former for bekjempelse» (Bjørgo et al., 2013).

FFI etablerte i 2012 prosjektet *Cybermakt.* Prosjektet er en studie av cyberdomenets egenskaper og potensial som et nytt krigføringsdomene. Studien er bestilt av Cyberforsvaret og har som mål å fremme en anbefaling om hvilke kapabiliteter Norge og Forsvaret bør ha i cyberdomenet, og videre hvordan cyberdomenet skal forsvares og utnyttes i fred, krise, væpnet konflikt og krig. Prosjektet ble avsluttet i november 2014.

Avgrensning og presisering

Dersom samfunnskritisk ekom-infrastruktur i Norge skulle rammes av et cyberangrep, er det flere avdelinger i Forsvaret som vil kunne få en rolle i krisehåndteringen. Jeg har valgt å fokusere på Cyberforsvaret ettersom det ble nevnt spesifikt i regjeringserklæringen. Samtidig er denne studiens hovedtema håndteringen av selve cyberangrepet, herunder å oppdage, varsle, analysere, koordinere og håndtere. I en slik kontekst er Cyberforsvaret en av de mest relevante avdelingene i Forsvaret.

Et cyberangrep mot sivil ekom-infrastruktur vil i første rekke kunne true samfunnssikkerheten ved at kritiske funksjoner settes ut av spill. Avhengig av angrepets omfang og mål kan det også true statssikkerheten (Prop. 73

S (2011—2012), s. 24). Denne studien avgrenses til kriser som eies og ledes av sivile myndigheter, fordi Cyberforsvarets rolle er mye tydeligere dersom angrepet er av en slik art at Forsvaret leder håndteringen. Studien vil derfor ikke i særlig grad[10] berøre juridiske betraktninger om hva som skal til for at angrepet passerer grensen for *angrep på Norge*[11].

Oppbygning

Dette første kapitlet har presentert bakgrunn, rammer, tidligere forskning og valg av problemstilling: *Hva er Cyberforsvarets rolle dersom sivil elektronisk kommunikasjonsinfrastruktur rammes av et cyberangrep? Når kan Cyberforsvaret bistå, og hva kan det bistå med?*

Kapittel 2 redegjør for valgt metode og kilder.

Kapittel 3 skal etablere det teoretiske grunnlaget for problemstillingen. Utgangspunktet er at nasjonal krisehåndtering og regulering av sivil-militært samarbeid er uavhengig av domenet krisen oppstår i. Håndteringen av et cyberangrep mot ekom-infrastrukturen og en eventuell cyberkrise må forholde seg til det etablerte systemet.

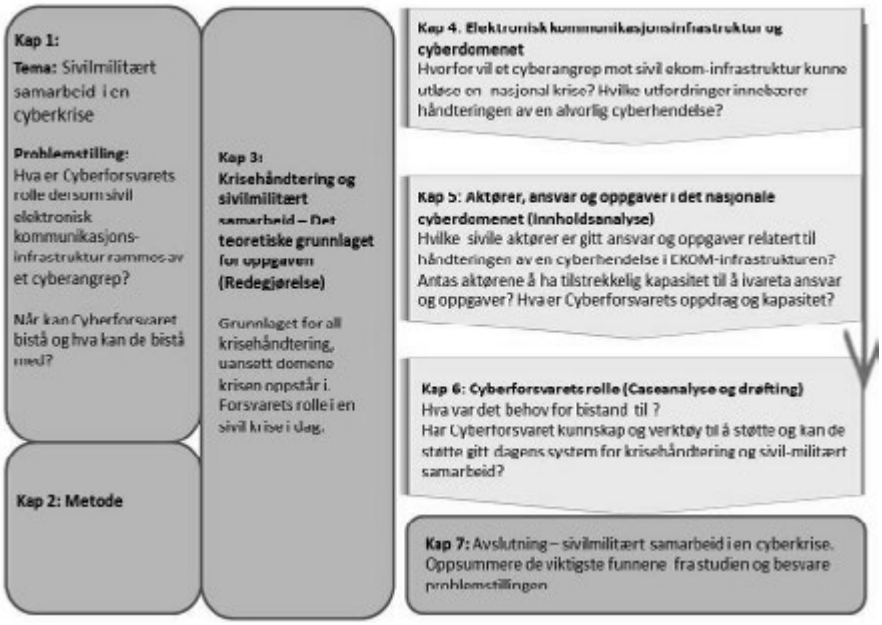
Kapittel 4 vil sette søkelyset på ekom-infrastruktur og cyberdomenet. Hensikten er å bidra til økt forståelse for hva ekom-infrastruktur er. Hvordan kan forstyrrelser i eller ødeleggelse av sivil ekom-infrastruktur kan forårsake en nasjonal krise — en cyberkrise? Hva innebærer et cyberangrep, og hvilke utfordringer vil vi stå overfor i håndteringen av alvorlige cyberangrep?

[10] Dette berøres kort i kapittel 4.
[11] Det er regjeringen som må beslutte om en situasjon er et «væpnet angrep på Norge». En slik vurdering vil omfatte en rekke faktorer, herunder hvem som står bak terroranslaget, omfang og kompleksitet, betydningen for rikets sikkerhet og folkerettslige rammer: «Når et væpnet angrep først er konstatert, vil en nærmere vurdering av den konkrete situasjonen være avgjørende for hvilke deler av krigens folkerett som får anvendelse» (Meld. St. 29 (2011—2012), s. 98).

Kapittel 5 tar utgangspunkt i *Nasjonal strategi for informasjonssikkerhet* (2012). Her vil jeg kartlegge sentrale aktører, diskutere deres ansvar og drøfte deres oppgaver knyttet til ekom-infrastruktur og håndtering av cyberangrep. Hensikten er å indikere bistandsbehovet i sivil sektor, samt redegjøre for hva Cyberforsvaret vil kunne bistå med.

Kapittel 6 vil analysere to caser (fra 2013) som innebar cyberangrep mot sivil infrastruktur. Caseanalysen vil ha fokus på de aktørene og oppgavene som ble kartlagt og diskutert i innholdsanalysen. Hvordan ble disse oppgavene håndtert? Hadde ansvarlig aktør behov for støtte? De oppgaver hvor det viser seg å være behov for støtte vil så drøftes fortløpende. Har Cyberforsvaret kunnskap og verktøy til å kunne støtte? Kan Cyberforsvaret bistå gitt dagens prinsipper for krisehåndtering og regulering av det sivil-militære samarbeidet?

Kapittel 7 inneholder konklusjoner og svar på hva som er Cyberforsvarets rolle dersom sivil ekom-infrastruktur rammes av et cyberangrep — herunder *når* det skal bistå og *hva* det kan bistå med.



Figur 2: Oppgaveskisse

Kapittel 2
Metode og kilder

Problemstillingen i denne studien er uklar på den måten at vi har lite forhåndskunnskaper om det som skal undersøkes. Det er knapt to år siden generalmajor Roar Sundseth, daværende sjef for Cyberforsvaret, selv etterlyste nærmere avklaringer om Cyberforsvarets samfunnsrolle (Kirknes, 2013). Som Sundseth påpekte, eksisterer det ikke noen nasjonal cyberstrategi, og bistand fra Forsvaret til det sivile samfunn i forbindelse med reelle cyberhendelser er så langt uprøvd. Problemstillingen blir dermed *utforskende* eller *eksplorerende* (Jacobsen, 2005, s. 67—84).

Studien har søkt å kombinere flere metoder for å samle tilstrekkelig empiri til å kunne drøfte Cyberforsvarets rolle dersom sivil ekom-infrastruktur skulle bli rammet et av cyberangrep. Det er brukt en kvalitativ metode som er gjennomført ved en kombinasjon av innholdsanalyse, casestudier og intervjuer.

Innholdsanalyse, casestudie og intervju

Innholdsanalyse er en systematisk analyse av dokumenter og tekster (Ringdal, 2013), hvor data deles inn i temaer eller kategorier med henblikk på å finne en sammenheng (Jacobsen, 2005, s. 187). Denne studien fokuserer på håndtering av selve cyberhendelsen, herunder oppdagelse, varsling, analyse,

koordinering og håndtering. I *Nasjonal strategi for informasjonssikkerhet* vises ansvarsdelingen på et overordnet nivå. Ved å lese dette dokumentet opp mot andre dokumenter og tekster har det vært mulig å kartlegge og diskutere hvilke aktører som er gitt ansvar, oppgaver og myndighet knyttet til ekom-infrastruktur og håndtering av cyberangrep, samtidig som jeg har forsøkt å belyse aktørenes antatte kapasitet.

Dokumentene gir likevel ikke klare svar på problemstillingen. Innholdsanalysen er derfor kombinert med en *casestudie,* som avgrenser selve studieobjektet i tid og rom (Cresswell, 2013; Jacobsen, 2005; Ringdal, 2013). Ifølge Ringdal kan en case utgjøres av såvel individer, bedrifter og organisasjoner som hendelser og beslutninger, og data kan samles inn blant annet ved samtaleintervjuer. Jacobsens tolkning av casestudier er ikke så ulik Ringdals forståelse: en case kan være en spesiell situasjon, noe spesielt som har skjedd (Jacobsen, 2005, s. 87—101).

I denne studien har jeg valgt å se på to caser. Kriteriene var at de mest sentrale aktørene på feltet skulle være involvert i begge casene; casene måtte være av nyere dato, og de skulle omhandle håndtering av et cyberangrep mot sivil infrastruktur. Samtidig ønsket jeg at Cyberforsvaret skulle ha ulike roller i de to hendelsene.

Det har vært mange reelle cyberhendelser de senere år, men få av disse er tilgjengelige for forskning, da de fleste virksomheter ønsker å holde informasjon om slike hendelser for seg selv. Valget falt på den reelle cyberhendelsen hos Telenor vinteren 2013, kjent som *Industrispionasjesaken,* og øvelse *CyberDawn* høsten 2013, som ble initiert av Telenor. Bakgrunnen for valget av førstnevnte hendelse er at Telenor gikk til media og informerte om angrepet de ble utsatt for, noe som gjorde det tilgjengelig for forskning. Når det gjelder CyberDawn, er dette den eneste kjente norske cyberøvelsen hvor Forsvaret har hatt en aktiv rolle og støttet en sivil virksomhet gjennom bistand til politiet.

Intervjuene ble gjennomført som samtaleintervjuer med basis i en intervjuguide (Ringdal, 2013, s. 102—103). Intervjuguiden ble tilpasset det enkelte intervju og sendt respondenten i forkant. Spørsmålene varierte fra informant til informant. Det er gjort intervjuer med åtte sentrale ressurspersoner, som

fikk tilsendt et informasjonsskriv i forkant.[12] Intervjuene ble tatt opp digitalt, lagret som lydfiler og transkribert i ettertid.

Om kriseledelse, samfunnssikkerhet og beredskap

Studien har brukt et bredt utvalg av kilder, herunder faglitteratur, utredninger, stortingsproposisjoner, stortingsmeldinger, strategier, høringsnotat, lover, instrukser, interne dokumenter, rapporter, medieoppslag og egne intervjuer.

I antologien *Mellom fred og krig: Norsk militær krisehåndtering* (Heier og Kjølberg, 2013) drøftes Forsvarets rolle i nasjonal krisehåndtering ut fra ulike perspektiver. Cyberforsvaret, cyberdomenet og cyberkriser er ikke omtalt, men boken bidrar med nyttig kunnskap om kriser og krisehåndtering i de andre domenene. Nasjonal krisehåndtering er også et hovedtema i artikkelsamlingen *Strategisk ledelse i krise og krig* (Dyndal (red.), 2010). Heller ikke i denne boken står cyber på dagsordenen, men Bjørn Olav Heieraas bidrar, blant mange andre, med kunnskap om utfordringer knyttet til sivil-militært samarbeid både før og nå.

Andre viktige bidrag kommer fra generalmajor Roar Sundseth, tidligere sjef i Cyberforsvaret (2013), Kristin Bergtora Sandvik (2013) og Morten Irgens (2013). Alle bidrar med kunnskap direkte relatert til problemstillingen, henholdsvis om cybertrusler, juridiske utfordringer og cybersikkerhet.

Ansatte ved FFI har, som omtalt i kapittel 1, bidratt med forskning på kritiske infrastrukturer og ekom. Disse rapportene er primært blitt brukt til å etablere en kunnskapsplattform og til å definere og avgrense studien.

Flere offentlige utredninger har synliggjort samfunnets avhengighet av kritisk infrastruktur og sårbarhet overfor svikt i denne. To nasjonale utvalg som må fremheves i denne sammenheng er det såkalte *Sårbarhetsutvalget* (NOU 2000:24, *Et sårbart samfunn*) og *Infrastrukturutvalget* (NOU 2006: 6, *Når sikkerheten er viktigst*). Sårbarhetsutvalget bidro med vurderinger knyttet til felles

[12] Se respondentoversikt og skriv bakerst i denne studien.

sivil-militær ressursbruk og utvikling av forholdet mellom politi og forsvar, mens Infrastrukturutvalget gjorde rede for kritisk infrastruktur og kritiske samfunnsfunksjoner. En tredje NOU som er relevant for studien er *Rapport fra 22. juli-kommisjonen* (NOU 2012: 14). Rapporten om terroranslagene 22. juli 2011 fokuserer på trusler i det fysiske domenet, men gir også tungtveiende bidrag om sentrale sider ved beredskapen og nasjonens evne til å beskytte seg mot angrep. Ved siden av disse tre offentlige utredningene har DSB og Post- og teletilsynet (PT) gjennomført flere utredninger som gir viktig kunnskap om infrastrukturens sårbarhet, samfunnets sårbarhet overfor brudd i offentlige ekom-nett, og kunnskap om dagens ekom-marked.

Stortinget har siden Sårbarhetsutvalgets rapport behandlet flere stortingsmeldinger om samfunnssikkerhet og beredskap. De mest relevante for denne studien er:

St. meld. nr. 17 (2001—2002), *Samfunnssikkerhet. Veien til et mindre sårbart samfunn,* beskriver hva som ligger i begrepet samfunnssikkerhet. Forsøksprosjektet *Varslingssystem for digital infrastruktur* (VDI) er omtalt, og robusthet i teleinfrastruktur og beredskap er nevnt i meldingen.

St. meld. nr. 39 (2003—2004), *Samfunnssikkerhet og sivilt-militært samarbeid,* omhandler det nye totalforsvaret og det sivil-militære samarbeidet.

St. meld. nr. 22 (2007—2008), *Samfunnssikkerhet. Samvirke og samordning,* fokuserer på betydningen av samvirke og samarbeid både nasjonalt og internasjonalt i møte med fremtidens risiko-, trussel- og sårbarhetsbilder.

Meld. St. 29 (2011—2012), *Samfunnssikkerhet,* gjennomgår samfunnets beredskap, læringspunkter og tiltak etter 22/7, samt flom kombinert med svikt i telenettene, ekstremvær og andre alvorlige utfordringer de siste årene. Samvirkeprinsippet introduseres, og ansvarsforholdene rundt kritisk infrastruktur presiseres.

Meld. St. 21 (2012—2013), *Terrorberedskap,* presenterer en overordnet strategi for å forebygge og håndtere terror i Norge. Fokus er videreutvikling av de områder hvor Forsvarets ressurser kan supplere og utfylle sivil beredskaps- og krisehåndtering.

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

Industrispionasjesaken i Telenor fikk mye omtale i media. Sikkerhetsdirektør Rune Dyrlie i Telenor informerte utførlig om hendelsen og håndteringen av den på NSMs sikkerhetskonferanse samme år (Dyrlie, 2013b), og sikkerhetsselskapet Norman Shark har skrevet en omfattende rapport om hendelsen, *Operation Hangover: Unveiling an Indian cyberattack infrastructure* (Fagerland et al., 2013).

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

I tillegg til disse bidragene bygger studien på muntlige kilder i form av åtte intervjuer. Respondentene er valgt ut fra sin stilling og kunnskap. Alle har tilknytning til virksomheter som vil inneha sentrale roller dersom Norge skulle bli rammet av et alvorlig cyberangrep, herunder Telenor, NSM, Politidirektoratet, Forsvarsdepartementet, Forsvarets Operative Hovedkvarter og Cyberforsvaret. De utvalgte respondentene representerer høyt spesialisert kompetanse og er dermed helt sentrale for oppgaven.[13]

[13] Se oversikt over respondentene bak i studien.

Vurdering av metoden

Industrispionasjesaken og øvelse CyberDawn viste seg å være to svært relevante caser for studiens problemstilling. Det faktum at den ene casen var en krisehåndteringsøvelse på initiativ av en privat aktør (Telenor), kunne i utgangspunktet ha svekket studien. For eksempel deltok ikke Forsvarets Operative Hovedkvarter (FOH), FD eller JD under øvelsen. Disse aktørene ville alle hatt svært sentrale roller ved et reelt cyberangrep. Imidlertid er det håndteringen på taktisk nivå som er kjernen i denne undersøkelsen, ikke strategisk krisehåndtering, så dette svekket ikke studien i vesentlig grad. For å kompensere intervjuet jeg dessuten representanter fra FOH og JD som kjente til øvelsen, og en inspektør i Politidirektoratet som deltok.

Bruk av intervju som metode er ikke uten svakheter. Det kan ikke utelukkes at andre respondenter ville ha gitt andre svar, men jeg har tatt høyde for dette ved å intervjue så mange som jeg hadde kapasitet til, og intervjuene er i all hovedsak brukt til å forsterke og utdype det som andre kilder allerede har indikert. Ved å kombinere intervjuene med casestudier og innholdsanalyse av andre kilder, ta høyde for eventuelle svakheter og sammenstille funnene fikk jeg et godt grunnlag for å kunne drøfte problemstillingen.

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

Kapittel 3
Kriser og sivil-militært samarbeid

Det vil alltid være delte oppfatninger om hvordan kriser og terrorhendelser bør bli eller burde ha blitt håndtert. Det nasjonale systemet for krisehåndtering skal gi rammene for hvordan kriser prinsipielt skal håndteres i Norge. Både dette systemet og regelverket for bruken av militære ressurser i fredstid er uavhengig av hvilket domene krisen oppstår i. Det er ikke gitt at systemet har tatt høyde for eller passer til alle hendelser, men håndteringen av dem må likevel forholde seg til det etablerte systemet. For å kunne drøfte Cyberforsvarets rolle i en sivilt ledet krise, er det derfor en forutsetning å ha kjennskap til og forståelse for dette systemet.

Hva definerer en krise?

Situasjoner som oppleves kritisk på taktisk nivå kan håndteres som en daglig operasjon på strategisk nivå — og motsatt. 27 % av norske virksomheter sier at de «opplever det kritisk» når IT-systemene er nede i én time. Ytterligere 35 % av svarer at det er «kritisk for virksomheten» når viktige IT-systemer er nede en dag (Næringslivets sikkerhetsråd, 2012, s. 10). Dette oppleves alvorlig

for den enkelte virksomhet, men det er ikke nødvendigvis en nasjonal krise av den grunn.

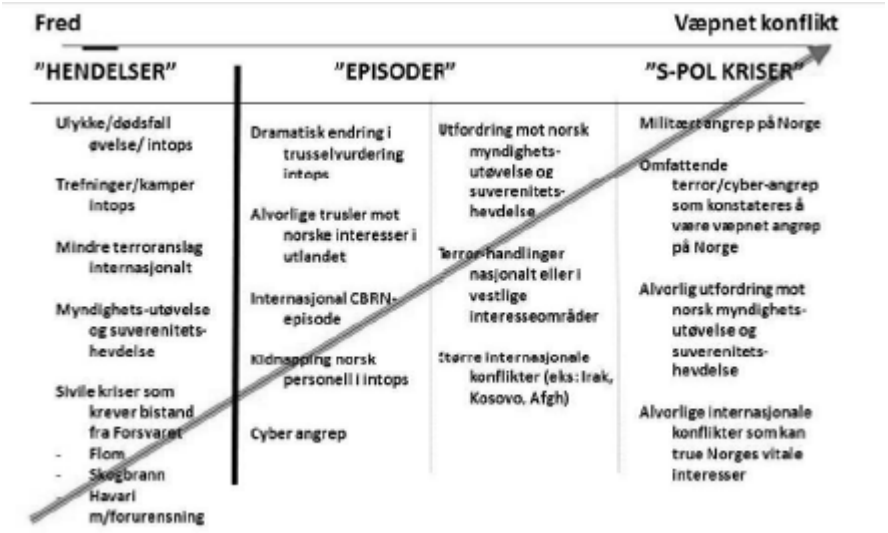
Ifølge Sårbarhetsutvalgets definisjon er en krise «en hendelse som har potensial til å true viktige verdier og svekke en organisasjons evne til å utføre viktige funksjoner» (NOU 2000: 24, s. 19). Politiet har utdypet Willoch-utvalgets definisjon av krisebegrepet ved å si at krise er en «tilstand som kjennetegnes av at samfunnssikkerheten eller andre viktige verdier er truet, og at håndteringen utfordrer eller overskrider kapasiteten og/eller kompetansen til den aktøren som i utgangspunktet har ansvaret» (Politiet, 2011, s. 25).

Politiets definisjon inneholder et annet begrep som også har manglet en tydelig definisjon, nemlig *samfunnssikkerhet*. Samfunnssikkerhet er blitt definert som «den evne samfunnet som sådan har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger» (St. meld. nr. 17 (2001—2002), s. 4). Slik begrepet ble beskrevet i meldingen skulle det dekke et bredt spekter av utfordringer, fra begrensede, naturskapte hendelser, via større krisesituasjoner som representerer omfattende fare for liv, helse, miljø og materielle verdier, til sikkerhetsutfordringer som truer nasjonens selvstendighet eller eksistens. Begrepet samfunnssikkerhet ble senere avgrenset til «angrep og annen skade i situasjoner der statens grunnleggende interesser ikke er truet» (St. meld. nr. 37 (2004—2005), s. 50). Kort fortalt dreier samfunnssikkerhet seg om vern mot hendelser som truer, og primæransvaret for samfunnssikkerhet ligger hos de sivile myndigheter.

Det er JD som har hovedansvaret for å ivareta helheten i regjeringens politikk for samfunnssikkerhet, men Forsvaret kan bistå. Samarbeidet mellom sivile og militære myndigheter for å støtte opp under samfunnssikkerheten omtales som *sivil-militært samarbeid*. Forsvaret sier i siste langtidsplan at det vil gjøre sitt ytterste for å bistå når det anmodes om bistand (Prop. 73 S (2011—2012).

I sin tolkning av krisebegrepet vektlegger Forsvaret tilgangen på ressurser: en krise «kan føre til at én myndighet eller etat alene ikke har ressurser til å håndtere krisen. I stedet vil det være nødvendig å konsentrere deler eller samtlige av statens tilgjengelige ressurser» (Forsvarsstaben, 2014, pkt. 03 026). Forsvarets bistand vil eventuelt være et supplement til sivile myndigheters krisehåndtering, og støtten skal primært være innenfor områder der etaten

har kompetanse eller ressurser som andre ikke har. Forsvaret plasserer situasjoner ut fra intensitet, geografisk omfang og varighet på en *konfliktskala* som vist i figur 3.



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

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

Sentrale prinsipper for beredskap og krisehåndtering

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

Ansvarsprinsippet innebærer at den virksomhet, myndighet eller etat som har ansvar for et fagområde til daglig også har ansvar for å håndtere ekstraordinære hendelser på området (Meld. St. 29 (2011—2012), s. 39). Kritisk infrastruktur er ikke noe unntak: «Ansvar for beskyttelse av kritisk infrastruktur ligger til eier eller operatør av infrastrukturen og følger sektoransvaret» (St. meld. nr. 22 (2007—2008), s. 40).

I praksis innebærer ansvarsprinsippet at eier av infrastrukturen må sørge for de nødvendige beredskapsforberedelser, herunder å planlegge hvordan funksjoner innenfor eget ansvarsområde skal kunne opprettholdes og videreføres dersom det inntreffer en ekstraordinær hendelse, eksempelvis et cyberangrep. For å ivareta sitt ansvar må virksomheten sørge for å ha tilstrekkelige avtaler med sine underleverandører og andre for å sikre seg hjelp i tilfelle kriser (Brattekås, Hagen og Sandrup, 2011, s. 43).

Det er ministeren som sitter med det overordnede ansvaret for sin sektor. Det overordnede ansvaret innebærer å peke ut og sikre kritisk infrastruktur i egen sektor, iverksette nødvendige forebyggende tiltak, forberede beredskapstiltak og krisehåndtering samt føre tilsyn med informasjonssikkerheten i egne underliggende etater (Meld. St. 29 (2011—2012).

En krise som oppstår på bakgrunn av et cyberangrep mot en teleoperatør, vil innledningsvis høre inn under samferdselsministerens ansvarsområde. Dersom angrepet i stedet rammet prosesskontrollsystemet i et oljeselskap, ville krisen ha sortert under Olje- og energidepartementet (Brattekås et al., 2011, s. 19). Dersom ansvarlig minister ikke har nødvendig kompetanse eller ressurser i sin sektor for å håndtere situasjonen, vil det være nødvendig å koordinere med andre departementer og etater, men det konstitusjonelle ansvaret for å løse oppgavene i en sektor ligger like fullt hos den enkelte fagstatsråd (NOU 2006: 6, s. 150).

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

Nærhetsprinsippet innebærer at situasjonen skal håndteres på så lavt nivå som mulig. Også dette prinsippet er tett knyttet til ansvarsprinsippet. En krise innenfor en virksomhets ansvarsområde er det virksomhetens ansvar å håndtere: «Departementenes hovedfunksjon i det daglige er å være sekretariat for den politiske ledelsen, og det er viktig at departementene i krisesituasjoner ikke overtar oppgaver som best kan utføres av de operative nivåene underlagt departementet» (St. meld. nr. 37 (2004—2005), s. 32). De som står nærmest krisen, vil dessuten ha best kjennskap til de lokale forhold og normalt kunne yte den raskeste og mest målrettede assistansen (NOU 2006: 6, s. 150).

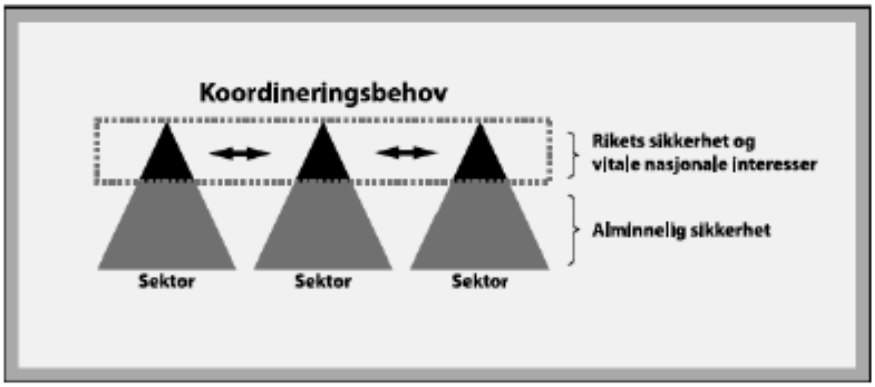
Nærhetsprinsippet innebærer at kriseledelse må kunne ivaretas like godt på lokalt nivå som på sentralt nivå. Det ideelle er at beslutninger fattes så lavt som mulig, men likevel på tilstrekkelig høyt nivå til at de overordnede nasjonale målsettinger blir ivaretatt. Jo større krisen er desto mer sentralisert krisehåndtering vil det være behov for. Av den grunn gjelder ikke nærhetsprinsippet ved sikkerhetspolitiske kriser (Meld. St. 29 (2011—2012), s. 39).

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

overordnet og styrende, særlig ved større sektorovergripende kriser (Høyre-Frp-regjeringen, 2013).

Det strategiske lederapparatet

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



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

I 2005 besluttet Stortinget, i kjølvannet av flodbølgekatastrofen i romjulen 2004, å basere strategisk krisehåndtering på tre hovedelementer: lederdepartementet,

Kriserådet[14] og Krisestøtteenheten. Hvilket departement som skulle ha rollen som lederdepartement, skulle besluttes ut fra faktorer som krisens karakter, hvem som hadde mest og best tilgang til informasjon om krisen, samt hvem som hadde de riktige virkemidlene for å håndtere krisen (St. meld. nr. 37 (2004—2005), s. 31). Senere er det imidlertid blitt besluttet at Justis- og beredskapsdepartementet «skal være fast lederdepartement for sivile nasjonale kriser med mindre noe annet er bestemt» (Meld. St. 29 (2011—2012), s. 7). Det er lederdepartementet som skal ivareta samordningen mellom departementene i mindre alvorlige kriser, mens Kriserådet skal sørge for samordningen i komplekse kriser.

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

[14] I 2005 kalt Regjeringens kriseråd. Regjeringen besluttet i 2012 å endre navnet til Kriserådet for å unngå *«usikkerhet utad om når møter finner sted på politisk nivå og om når møter finner sted på administrativt nivå»* (Meld. St. nr. 29 (2011—2012), s. 69). Kriserådet har fem faste medlemmer: regjeringsråden ved Statsministerens kontor, utenriksråden i UD og departementsrådene i Helse- og omsorgsdepartementet, JD og FD. I tillegg til disse faste medlemmene kan andre delta ved behov.

Hvem eier krisen?

I de fleste tilfeller er det krisens årsak som definerer krisen, skriver Bjerga og Håkenstad. Hvem som *eier* krisen og følgelig har ansvar for å lede håndteringen av den, avhenger av hva slags krise vi står overfor. Avhengig av om det er en *militær* eller en *sivil krise* vi står overfor, skal den håndteres av henholdsvis militære eller sivile myndigheter.

De militære krisene består av krig og sikkerhetspolitiske kriser for øvrig (Bjerga og Håkenstad, 2013, s. 58). Krig innebærer et væpnet angrep på Norge, mens en sikkerhetspolitisk krise er en situasjon hvor Norges territorielle integritet, politiske suverenitet eller økonomiske livsgrunnlag utfordres av en fremmed makt eller andre internasjonale aktører, uten at det nødvendigvis dreier seg om et militært angrep i tradisjonell forstand (NOU 2012: 14, s. 209).

I praksis vil det ofte være vanskelig å umiddelbart fastslå hvilken type krise man står overfor. I FFOD bemerkes det at Forsvaret har et selvstendig ansvar i det de kaller *nasjonale kaossituasjoner*, herunder omfattende cyberangrep, hvor det kan være uklart om Norge står overfor en krise eller væpnet konflikt (Forsvarsstaben, 2014, pkt. 03 032).

I Politiets beredskapssystem (Politiet, 2011) eller NOU 2006: 6, *Når sikkerheten er viktigst*, eksisterer ikke begrepet *kaossituasjoner*, men begge publikasjoner fremhever politiets ansvar for den operative håndteringen i terror og sabotasjesituasjoner: «Politiet skal lokalisere og pågripe gjerningsperson(er) som har iverksatt eller truer med å iverksette slike handlinger i fred, krise eller krig, såfremt det åpenbart ikke er stridshandlinger utført av militære stridskrefter tilhørende en fremmed makt» (NOU 2006: 6, s. 151).

Stridshandlinger med opprinnelse utenfor Norges grenser er et grunnvilkår for å kunne konstatere et væpnet angrep på Norge. Bjerga og Håkenstad påpeker at det i lys av hendelsene 22. juli og regjeringens umiddelbare vurdering av at det handlet om en sivil krise, er grunn til å stille spørsmål ved hva som skal til for at et anslag vurderes som en sikkerhetspolitisk krise. Kanskje er det slik at alle kriser «som ikke innebærer en eksplisitt fiendtlig, militær inntrengning på norsk territorium vil defineres som sivile kriser og håndteres deretter», også i fremtiden (Bjerga og Håkenstad, 2013, s. 74).

Sivil-militært samarbeid før og nå

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

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

Etterkrigstidens totalforsvar ble etablert som følge av erfaringer fra 1940 og faren for en ny storkrig. Beredskapsloven trådte i kraft 15. desember 1950. Loven ga konge (regjering) og militære myndigheter vide fullmakter til å disponere samfunnets sivile ressurser i tilfelle krig. Totalforsvarskonseptet skulle sørge for at alle landets ressurser skulle kunne tas i bruk for å verne om nasjonale interesser, verdier, territorium, samfunn og befolkning. Heieraas mener at muligheten for bruk av militærmakt i fredstid likevel var svært begrenset i flere tiår. Dette ble endret med etableringen av 200-milssonen i 1976. Med opprettelsen av Kystvakten i 1977, Forsvarets spesialkommando (FSK) i 1982 og Indre Kystvakt i 1996 ble Forsvaret gradvis en aktør på områder som tidligere hadde vært forbeholdt politiet. Heieraas beskriver denne utviklingen som *økt bruk av militær støtte til løsning av sivile samfunnsoppgaver* (Heieraas, 2010, s. 102).

I samme periode ble faren for ny storkrig gradvis mindre. Etter at den kalde krigen tok slutt, har beredskapsarbeidet mye dreid seg om å kunne forebygge og håndtere kriser i fredssituasjoner. Imidlertid har planverket igjen fått stort fokus de siste årene. Det er ennå for tidlig å si hvilke konsekvenser utfordringene i Ukraina og andre konfliktområder vil få. Kanskje tradisjonell sikkerhetspolitikk og krisehåndtering igjen blir mer sentralt?

Bruk av militære ressurser i fredstid

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

Regjeringen har altså i utgangspunktet ikke anledning til å anvende militærmakt mot statens borgere uten at maktbruken er formelt hjemlet i lovverket. Unntaket er dersom en forsamling forstyrrer den offentlige ro og orden og ikke oppløser seg selv etter at straffelovens opprørsparagrafer er blitt opplest av politiet. Dette innebærer at Forsvarets bistand til politiet i utgangspunktet skal begrunnes i en lovhjemmel. Så langt har imidlertid Forsvarets bistand til politiet vært regulert i kongelige resolusjoner, resolusjoner av henholdsvis 1965, 1998, 2003 og senest 22. juni 2012.

I 2013 foreslo Forsvarsdepartementet å lovfeste Forsvarets bistand til politiet i en egen lov (Regjeringen, 2013a). I høringsnotatet *Om lov om Forsvarets ansvar for å avverge luftbårne terroranslag og Forsvarets bistand til politiet* påpeker departementet at det imidlertid er en «lang og fast praksis for at dagens former for bistand, slik disse er regulert i bistandsinstruksen — alminnelig bistand og håndhevelsesbistand — faller utenfor det alminnelige grunnlovforbudet.

For dagens typer bistand er derfor lovforankring ikke ansett påkrevet» (Forsvarsdepartementet[15], 2013).

Hvorvidt det er behov for lovforankring eller ikke, har likevel vært og er fortsatt svært omdiskutert. Juristen Jon Petter Rui har konkludert med at «lovgivning er nødvendig» når det gjelder politiets behov for støtte fra Forsvaret. Rui beskriver Forsvarets bistand i forbindelse med naturkatastrofer, større ulykker eller søk etter savnede personer som ukontroversielt. Forsvarets bistand til politiet ved forebygging og bekjemping av straffbare forhold er derimot ikke like greit. Rui mener det må «anses som sikkert at Forsvaret uten hjemmel i formell lov ikke kan gi støtte til politiet hvis formålet med operasjonen er at Forsvarets personell skal utøve fysisk makt overfor sivile borgere» (Rui, 2011, s. 445). Han avslutter med å si at tiden er moden for at Stortinget tar stilling til om og eventuelt i hvilken utstrekning Forsvaret skal kunne bruke makt mot sivile borgere når det ytes støtte til politiet, samt at det lovfestes klare prosedyrer for bistand og ansvarsforhold.

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

Det nye totalforsvarskonseptet

Sårbarhetsutvalget tok for seg problemstillinger knyttet til felles sivil-militær ressursbruk og utvikling av forholdet mellom politi og forsvar. Utvalget hevdet at rutinene for bistand til politiet var for byråkratiske og kunne bidra til langtrukne beslutningsprosesser. Samfunnet sto overfor en voksende og vanskelig definerbar risiko som følge av bevisste handlinger i en gråsone mellom fred og krig.

Utvalget argumenterte for at det var viktig å utvikle samarbeidet mellom politiet og Forsvaret, fordi politiet hadde begrenset kapasitet til å møte de nye utfordringene samfunnet sto overfor. Forsvaret skulle gi støtte til det

[15] Heretter (i referansene) FD.

sivile samfunn i fredstid, så fremt det var forenlig med Forsvarets primære oppgaver. Fare for anslag av omfattende skadevoldende karakter rettet mot vesentlige samfunnsinteresser ble oppgitt som en situasjon hvor det kunne være aktuelt med bistand fra Forsvaret (NOU 2000: 24, s. 55).

Utvalget etterlyste en avklaring av hvordan samvirket mellom politi og militære styrker skulle kunne etableres i det som ble vurdert som særlig kritiske situasjoner uten at det krevde medvirkning fra vedkommende departementer. De fryktet at beslutningsprosessene skulle ta for lang tid, og at tapene derfor kunne blir større enn nødvendig. Fleksibel holdning til bruk av militære styrker ble vurdert som avgjørende for landets beredskapsmessige slagkraft. Samtidig ble det poengtert at det ikke skulle bety en utvisking av skillet mellom sivilt og militært ansvar.

Utvalget kunne ikke vise til klare eksempler på hvorfor det skulle være behov for å justere instruksverket på området, siden det ikke hadde vært noe omfattende tilfelle av slik terror, som man ønsket sterkere beskyttelse mot. Utvalget anbefalte likevel en gjennomgang av regelverk og prosedyrer (NOU 2000: 24, s. 54—59).

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

I 2003 kom en ny instruks for Forsvarets bistand til politiet. I kgl. res. av 28. februar 2003 ble støtte fra Forsvaret inndelt i tre kategorier: administrativ bistand, operativ bistand og håndhevelsesbistand. Den

militære innsatsen skulle fortrinnsvis konsentreres om vakthold, sikring og dekning. Stortingsmeldingen *Samfunnssikkerhet og sivilt-militært samarbeid* kom ut året etter og ga totalforsvarssamarbeidet et mer helhetlig innhold. Totalforsvarssamarbeidet skulle som før omfatte krig og sikkerhetspolitiske kriser, men det ble nå påpekt at kriser også skulle omfatte alvorlige og omfattende terrorhandlinger. *Det nye totalforsvarskonseptet* skulle bestå av «gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn om både forebygging, beredskapsplanlegging og operative forhold» (St. meld nr. 39 (2003—2004), s. 15).

Samarbeidet mellom FD og JD om etatsstyringen av NSM ble presentert som et eksempel på sivil-militært samarbeid innenfor det nye totalforsvarskonseptet (St. meld nr. 39 (2003—2004), s. 17). Forsvaret skulle kunne bidra til samfunnssikkerhet med tilgjengelige kapasiteter, kompetanse og ressurser. Den videre moderniseringen av Forsvaret skulle legge til rette for at Forsvarets ressurser i større grad kunne tas i bruk til støtte for politiet og sivile myndigheter. Det ble imidlertid fastslått at bistand bare skulle gis under den forutsetning at politiets personell og materielle ressurser ikke strakk til, og den militære innsatsen skulle fortrinnsvis konsentreres om vakthold, sikring og dekning (St. meld nr. 39 (2003—2004), s. 23). Det ble gjort oppmerksom på at det var sterkt begrenset adgang for militært personell til å gi håndhevelsesbistand. Bakgrunnen til denne restriktive holdningen var at håndhevelsesbistand kunne ha politiske implikasjoner, og spørsmålet om slik bistand skulle derfor behandles i JD i samråd med FD (St. meld nr. 39 (2003—2004), s. 23).

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

si for deltakerne, hvilke handlingsalternativer som kan og bør iverksettes, samt oppfølgingen av iverksatte tiltak» (NOU 2006: 6, s. 20).

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

Regjeringen påpekte at Forsvaret har et vidt spekter av ressurser som kan stilles til rådighet for det sivile samfunn i krisesituasjoner, men samtidig har Forsvaret færre mannskaps- og materiellressurser til å yte bistand nå enn før. Utgangspunktet er at sivile kriser håndteres med sivile ressurser, og dersom det er behov for bistand må Forsvaret involveres tidlig i krisen «slik at relevante ressurser kan identifiseres og stilles til rådighet til rett tid» (St. meld. nr. 22 (2007— 2008), s. 71).

Da det norske samfunnet ble satt på prøve 22. juli 2011, var nettopp rådigheten over relevante ressurser noe av det som manglet. Forsvarets fokus var fra første øyeblikk rettet mot å kunne bistå politiet med relevante støttekapasiteter. Forsvarsminister Faremo ga tidlig klar beskjed om å «støtte politiet med det de anmoder om» (NOU 2012: 14, s. 242). Forsvaret var derfor proaktivt, kalte inn mannskaper og startet å klargjøre materiell i påvente av bistandsanmodninger. Det kom i alt fem bistandsanmodninger, hvorav samtlige omhandlet en eller annen form for håndhevelsesbistand (NOU 2012: 14, s. 243).

22. juli-kommisjonens vurdering var at samarbeidet mellom etatene i dette tilfellet hadde fungert godt og at anmodningene hadde blitt ekspedert raskt (NOU 2012: 14, s. 160). Konklusjonen var at Forsvaret evnet å klargjøre de kapasiteter som ble etterspurt og løste sitt oppdrag på en tilfredsstillende måte. Oppdraget kunne imidlertid ha vært større. Kommisjonen indikerte at politiet burde ha tatt i bruk bistandsinstruksen langt tidligere og mer proaktivt (NOU 2012: 14, s. 245). Kommisjonen påpekte også at det var nødvendig å videreutvikle samhandlingen mellom politiet og Forsvaret (NOU 2012: 14, s. 146).

Ny instruks om Forsvarets bistand til politiet

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

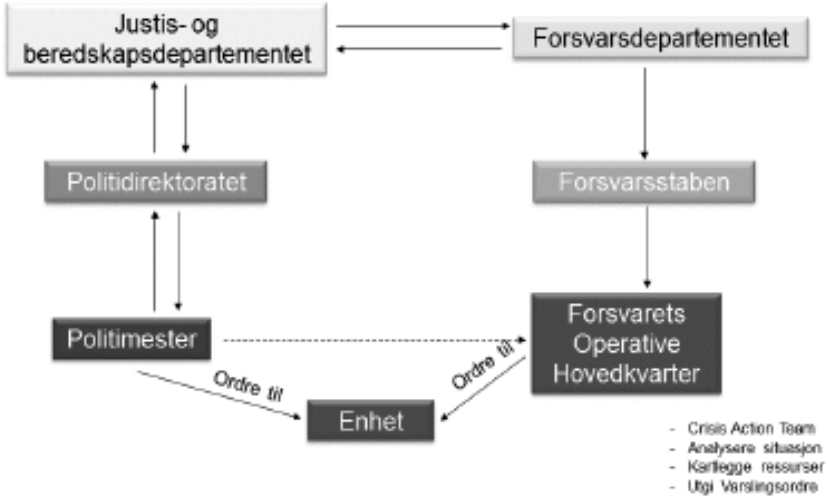
Et forsvar for vår tid påpeker at angrep i det digitale rom er en av de raskest voksende truslene. Det forventes at truslene vil fortsette å øke og bli mer komplekse, og at det vil kunne skape utfordringer for kritisk infrastruktur, som telekommunikasjon. Selv om de fleste hendelsene så langt har vært spionasjeangrep, kan utviklingen gå i retning av å sabotere kritisk infrastruktur: «Stans i kommunikasjonslinjene kan være en trussel både mot samfunns- og statssikkerheten» (Prop. 73 S (2011—2012), s. 22). Det understrekes at Forsvaret skal kunne bistå sivile myndigheter ved hendelser i cyberdomenet etter de samme prinsipper og regler som for annen militær bistand til samfunnssikkerhet. Det er imidlertid bare Forsvarets bistand til politiet som hittil er regulert i en egen instruks. I tilfeller hvor Forsvaret skal yte bistand til andre sivile myndigheter enn politiet, er det «viktig å unngå at Forsvaret påtar seg oppgaver som bør, kan eller skal ivaretas av sivile aktører» (Prop. 73 S (2011—2012), s. 54).[16]

[16] Allerede før 22. juli 2011 var det igangsatt et arbeid med å utarbeide en egen instruks om Forsvarets bistand til andre sivilie myndigheter enn politiet, men denne er ennå [2015] ikke ferdigstilt.

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

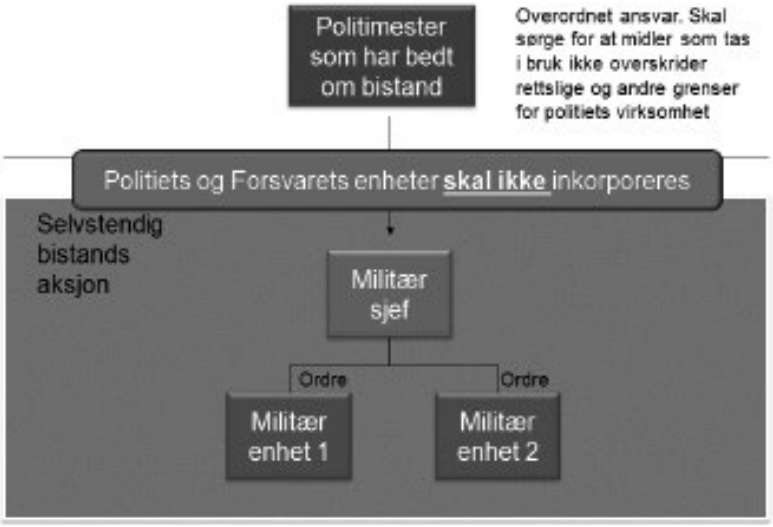
22. juni 2012 ble den nye bistandsinstruksen vedtatt. Instruksen gjelder for Forsvarets bistand til politiet i fred, krise og krig. Med bistand menes all form for støtte, herunder både personell og materiell. Den nye instruksen slår sammen de tidligere tre bistandsformer til to: alminnelig bistand og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

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



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

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



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

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

sjeldent tilstrekkelige, mens Forsvaret besitter et overskudd av ressurser som er relevant i nasjonal beredskap og krisehåndtering, også i fredstid.

Oppsummering

En krise omfatter situasjoner som kommer uventet, utvikler seg raskt og uforutsigbart og har potensial til å true samfunnssikkerheten, samtidig som håndteringen utfordrer eller overskride kapasiteten og/eller kompetansen til den aktøren, myndighet, eller etat som i utgangspunktet har ansvaret. Dagens modell for beredskap og krisehåndtering er tuftet på fire prinsipper: *ansvar, likhet, nærhet og samvirke*. Regjeringen sier at ansvar og samvirke skal være overordnet og styrende ved større sektorovergripende kriser.

Sivile kriser skal håndteres av sivile myndigheter, og JD er fast lederdepartement for nasjonale kriser med mindre noe annet blir bestemt. *Det nye totalforsvarskonseptet* innebærer gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn om både forebygging, beredskapsplanlegging og operative forhold. Forsvaret skal gi bistand til det sivile samfunn når viktige samfunnsinteresser og liv og helse står på spill. Dette dreier seg om bistand både til politiet og til det øvrige sivile samfunn.

Forsvaret har et vidt spekter av ressurser som kan stilles til rådighet for det sivile samfunn i krisesituasjoner, men samtidig færre mannskaps- og materiellressurser til å yte bistand nå enn før. Utgangspunktet er at sivile kriser håndteres med sivile ressurser, men terskelen for å be om bistand fra Forsvaret skal ha blitt lavere med den nye bistandsinstruksen, og i fremtiden vil Forsvaret kunne få en større rolle i nasjonal beredskap. Prop. 73 S fastslår at Forsvaret kan bistå sivile myndigheter ved hendelser i cyberdomenet etter de samme prinsipper og regler som for annen militær bistand til samfunnssikkerhet.

Det nasjonale systemet for krisehåndtering og reguleringen av det sivil-militære samarbeidet definerer i stor grad *når* og med *hva* Cyberforsvaret[17] vil kunne bistå. Cyberforsvaret kan bistå sivile myndigheter ved et cyberangrep mot ekom-infrastrukturen dersom viktige samfunnsinteresser, liv og helse står på spill, — og under forutsetning av at politiets personell og materielle ressurser ikke strekker til. Cyberforsvaret vil i så fall kunne bistå med all tilgjengelig kompetanse og ressurser. For å besvare problemstillingen må derfor den videre studien vise hva som skal til for at et cyberangrep får konsekvenser for samfunnssikkerheten. Videre må studien se på hvilke cyberressurser politiet har, og hva som skal til for at deres personell og materiell eventuelt ikke strekker til. Sist, men ikke minst, må studien gjøre rede for hvilken kompetanse og ressurser Cyberforsvaret besitter.

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

Kapittel 4
Ekom og cyberdomenet

Forsvaret skal gi bistand til sivilsamfunnet når viktige samfunnsinteresser, liv og helse står på spill. NSM håndterte nær 4000 sikkerhetshendelser på internett i 2013, altså gjennomsnittlig over 10 per dag. Disse hendelsene rammet sentrale norske virksomheter som myndighetsorganer, forsvarsindustri og teknologibedrifter. 50 av angrepene ble kategorisert som alvorlige (NSM, 2014b). Det var likevel ikke behov for bistand fra Forsvaret ved noen av disse hendelsene.

Dersom et cyberangrep mot ekom-infrastrukturen forårsaker en nasjonal krise, kan Forsvaret kan bli bedt om å bistå. Å forstå gangen i dette krever kjennskap til infrastrukturen. Dette kapitlet vil gjøre nærmere rede for hva ekom-infrastruktur er og forhåpentlig begrunne hvordan cyberangrep mot denne infrastrukturen kan true samfunnssikkerheten. Alvorlige cyberangrep kan kreve en annen håndtering enn de andre, daglige, sikkerhetshendelsene på internett.

Hva er kritisk infrastruktur?

Infrastrukturutvalget definerte kritisk infrastruktur til å være «de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens

trygghetsfølelse» (NOU 2006: 6, s. 16). Utvalget definerte elkraft, vann og avløp, transport, olje og gass, satellittbasert infrastruktur og ekom som kritiske infrastrukturer.

Utvalget fant tre generiske trekk eller kriterier for utvelgelse av kritisk infrastruktur, som vist i figur 7: *avhengighet, manglende alternativer og tett kobling.*

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

Det første kriteriet var kritisk *avhengighet* av infrastrukturen med tanke på å kunne opprettholde et tjenestetilbud til befolkningen. Bortfall av infrastrukturen vil få alvorlige konsekvenser dersom et stort antall mennesker er avhengige av den. Det andre kriteriet var *manglende alternativer*: få eller ingen alternativer som kan erstatte infrastrukturen indikerer at infrastrukturen er kritisk. Det tredje kriteriet var *tett kobling*. Slik kobling kan gjelde mellom ulike komponenter innenfor ett og samme system, slik at svikt i én komponent fører til at hele systemet bryter sammen. En annen variant av tett kobling «kan skyldes avhengighet mellom systemer slik at svikt i ett system, har negative virkninger for funksjonaliteten i andre systemer og at det dermed får sektorovergripende konsekvenser» (NOU 2006: 6, s. 21).

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

Fra telemonopol til fri konkurranse

Etter andre verdenskrig var beskyttelse av teletjenester en viktig del av totalforsvarskonseptet. Offentlige telekommunikasjonstjenester ble levert av en offentlig forvaltningsbedrift, nemlig Televerket. Til tross for at man hadde egne telenett med høye krav til robusthet innen jernbanen, Forsvaret og kraftforsyningen, var offentlige teletjenester likevel en svært viktig del av datidens totalforsvar (DSB, 2012).

På slutten av 1980-tallet startet en gradvis omorganisering av sektoren. I 1988 ble Televerkets monopol på terminalutstyr opphevet, i 1991 ble det innført konkurranse innen mobiltelefoni, og i 1995 ble Televerket omdannet til et statlig aksjeselskap, Telenor. Da det norske telemarkedet ble åpnet for fri konkurranse 1. januar 1998, økte antall tilbydere av ekom-tjenester

hurtig. Ti år etter fantes det nær 200 aktører innenfor områdene fasttelefoni, mobiltelefoni, internett og leide linjer (PT, 2013).

Et telemarked med fri konkurranse krevde et nytt konsept for telesikkerhet og -beredskap. Disse rammene ble beskrevet i St. meld. nr. 47 (2000—2001), *Telesikkerhet og -beredskap i et telemarked med fri konkurranse,* og innebar at alle teleoperatører, ikke bare Telenor, skulle pålegges en del beredskapsforpliktelser. PT skulle følge utviklingen og gjennom pålegg og ulike samarbeidstiltak sørge for økt robusthet (St. meld. nr. 17 (2001—2002), s. 44—45).

Bruksmønsteret innen teletjenester har gradvis endret seg det siste tiåret. Ekom-tjenestene har blitt stadig mer avanserte, mer tilgjengelige og mer integrert i folks dagligliv. For telefoni har trenden vært nedgang i andelen fasttelefoniabonnementer til fordel for mobil. Ved utgangen av første halvår 2013 var det 1,32 millioner fasttelefoniabonnementer og om lag 5,9 millioner mobilabonnementer i Norge. Trafikken fra mobiltelefoner utgjorde nesten 75 prosent av den totale trafikken.

Samtidig har internettbruken eksplodert. Ved utgangen av 2002 lå antallet abonnementer for fast (kablet) bredbånd på 200 000, mens man i 2013 nærmet seg 1,9 millioner. Mobilt bredbånd ble introdusert i 2006, og ved utgangen av første halvår 2013 nærmet man seg 812 000 abonnementer. Dette tilsvarer om lag 43 prosent av antall abonnementer for fast bredbånd (PT, 2013).

Mobiltelefonen brukes stadig mer og dekker et større mangfold av behov. Endringer i bruksmønsteret er en medvirkende årsak til det pågående teknologiskiftet i Telenor. Telenor vil avvikle den linjesvitsjede telefoniplattformen og erstatte det med IP-teknologi og/eller mobile løsninger (DSB, 2013b, s. 5). Ifølge DSB vil denne omleggingen få negativ betydning for samfunnets robusthet og sårbarhet: «Overgangen til en felles plattform for nesten all elektronisk kommunikasjon i Telenors nett medfører en endring i sårbarhetsbildet for ekom-nett og ekom-tjenester. Redundansen vil bli redusert, og ekom-nettene vil i større grad enn før bli eksponert for cyberangrep av ulike slag» (DSB, 2013b, s. 6).

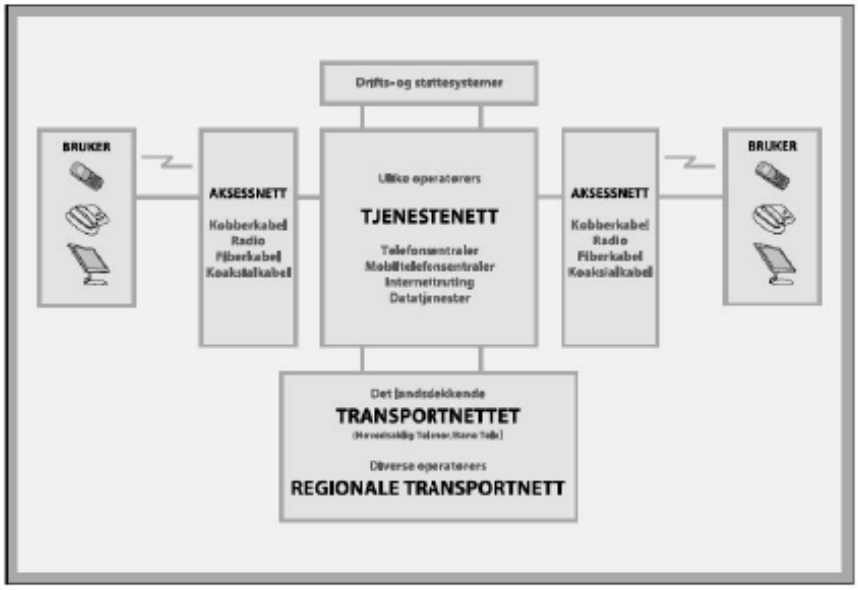
Telenor er fortsatt den dominerende leverandør av teletjenester i Norge både innenfor fasttelefoni, mobiltelefoni og internett (PT, 2013):

- Fasttelefoni: Telenor har, målt i omsetning, 68,1 % av markedsandelen.

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

Ekom-infrastruktur – oppbygning og status

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

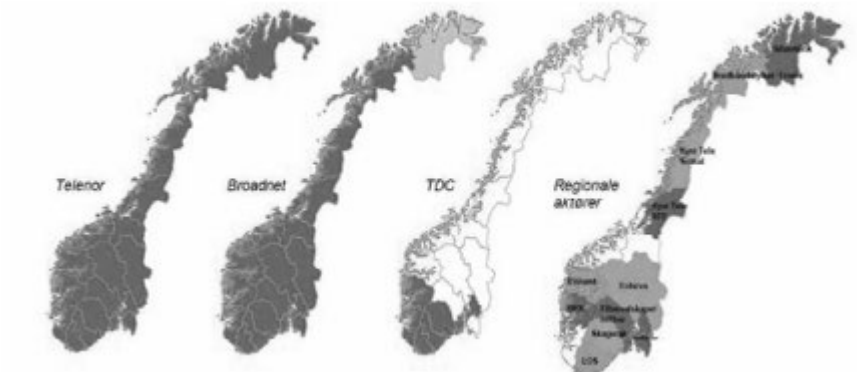


Figur 8: Prinsippskisse ekom-infrastruktur (NOU 2006: 6, s. 100: Figur 10.1)

Stamnett, også kalt *transportnett,* er den landsdekkende motorveien for tele- og datakommunikasjon. Transportnettene består av overføringssystemer med stor kapasitet, fiberkabel og i noen tilfeller radiolinje. Det er flere virksomheter som eier fiberinfrastruktur som kan inngå i andre tilbyderes transportnett,

men nær samtlige aktører er fortsatt avhengige av å leie kapasitet av Telenor for å sy sammen egne nett.

Telenor og Broadnet[18] er, som illustrert i figur 9, de to eneste som tilbyr nasjonal transportkapasitet basert på fiberoptiske kabler. Telenor har i dag to landsdekkende og fysisk adskilte transportnett (Svendsen, 2014). Jernbaneverket har et digitalt nett som brukes til jernbaneformål, men det tilbys ikke andre. Også Statnett har egen infrastruktur, men kjøper fortrinnsvis overføringskapasitet fra andre aktører der det er mulig (DSB, 2013b, s. 14).



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

Transportnettene er en del av det PT regner som kritisk infrastruktur (DSB, 2012, s. 15). To av Venstres stortingsrepresentanter fremmet i 2014 et krav om å etablere en nasjonal plan for utbygging av bredbåndsinfrastruktur. De mente at dagens situasjon ikke er holdbar sett fra et sårbarhets- og sikkerhetsperspektiv, ettersom alle samfunnskritiske ekomtjenester, mobil- og nødnettstjenester til syvende og sist hviler på Telenors stamnett (Breivik og Kjenseth, 2014).

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

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

Transportnettet knytter sammen regionalnettene. Regionalnettene er riksveiene for tele- og datakommunikasjon. I regionalnettene står det flere sentraler som samler opp trafikk fra såkalte *aksessnett.* Under brannen i Lærdal var det en slik sentral i regionalnettet som brant ned (Svendsen, 2014).

Aksessnettene knytter forbindelse mellom den enkelte sluttbruker og transport- og tjenestenettene. De faste aksessnettene kan være fiber, hybridfiber eller kobber, og disse nettene sender trafikk mellom sluttbruker og nærmeste sentral i regionalnettet. Mobilnettene er en type aksessnett hvor det er trådløs forbindelse mellom basestasjoner og brukernes mobiltelefoner.

Den enkelte basestasjon dekker et lite geografisk område, og hver basestasjon er knyttet til kjernenettet med en fast linje eller en radiolinje. For at en tilbyder av mobilnett skal kunne dekke hele landet kreves det et aksessnett med flere tusen basestasjoner. Telenor hadde i 2012 omkring 10.000 basestasjoner, plassert på 6.500 lokasjoner (PT, 2012b, s. 8). Andre mobiltilbydere er avhengig av Telenors infrastruktur for å levere sine tjenester (DSB, 2012, s. 15). Innfasing av fjerde generasjon mobiltelefoni (4G) medfører også at IP-teknologi blir tatt i bruk på dette området.[19]

Tjenestenett er ikke et selvstendig fysisk overføringsnett, men kan benytte ulike typer infrastruktur som også anvendes til andre typer tjenester. Fasttelefon og mobiltelefon er eksempler på tjenestenett. Tjenestenettene består av diverse systemer og utstyr som er nødvendig for å levere de ulike tjenestene.

[19] 2G og 3G vil ikke fases ut, men fortsatt eksistere ved siden av 4G (DSB, 2013b, s. 23).

Drifts- og støttesystemene er IT-systemer som overvåker og styrer ekom-nett og tjenestenett. DSB påpeker at drifts- og støttesystemene kan utgjøre en kritisk del av infrastrukturen (DSB, 2012, s. 15—16). Funksjonene er gjerne sentralisert og er derfor selv avhengige av ekom for å overvåke og styre komponentene i nettene.

Cyberdomenet

Omtrent 40 prosent av verdens befolkning er i dag på internett (Johnsen og Kveberg, 2014). Det er internett mange tenker på når de hører begrepet *cyberdomenet.* Etter Forsvarsdepartementets definisjon består cyberdomenet av fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data (FD, 2014, s. 4). Cyberdomenet omfatter altså både de nett som er tilgjengelig fra internett (åpne nett) og de som ikke er det (lukkede nett), både infrastrukturen og dataene som er lagret der.

I den seneste langtidsplanen, *Et forsvar for vår tid* (2013—2016) ble cyberdomenet for første gang beskrevet som *det femte krigføringsdomenet.* Sjefen for det da ganske nyetablerte Cyberforsvaret (tidligere Forsvarets Informasjonsinfrastruktur), generalmajor Roar Sundseth, beskrev dette som en erkjennelse av fundamental betydning. Selv om det ikke var en ny forsvarsgren, ble det menneskeskapte cyberdomenet gitt en status på linje med de tradisjonelle krigføringsarenaene på land, sjø, i luften og rommet (Sundseth, 2013). I denne erkjennelsen, sa Sundseth, ligger en rekke vesentlige konsekvenser for ansatte i Forsvaret:

> *Alle våre operasjoner, all vår øving og all vår trening har fått en ny dimensjon. Vår forvaltning og fredstidsdrift har også fått en ekstra dimensjon å forholde seg til. All vår planlegging, fra skarpe operasjoner til Forsvarets nye IKT-strategi må ta inn over seg og inkludere konsekvensene av denne erkjennelsen. Informasjonssikkerheten og integriteten til Forsvarets kommando- og kontrollsystemer ligger ikke til oss i Cyberforsvaret alene. Hele*

Forsvarets organisasjon, ned til den enkelte ansatte, må flette dette perspektivet inn i sin daglige aktivitet og sitt daglige virke. Ellers kan konsekvensene bli store.

Cyberangrep

Cyberbegrepene er abstrakte, relativt nye, og de brukes forskjellig. For å kunne drøfte Cyberforsvarets rolle ved et *cyberangrep* er det nødvendig å ta en begrepsgjennomgang.

Prefikset c*yber* indikerer at en aktivitet foregår i cyberdomenet (FD, 2014). Aktiviteten i seg selv har gjerne en definisjon fra før. En *cyberkrise* er altså en krise som har oppstått i eller gjennom cyberdomenet. Imidlertid er det ikke slik at alle aktiviteter har en klar definisjon fra før, og nettopp *angrep* er en slik aktivitet.[20]

Manual i krigens folkerett beskriver den folkerettslige betydningen av begrepet *cyberangrep* på denne måten: «Med cyberangrep menes en cyberoperasjon som er forventet å forårsake død eller skade på personell eller skade eller ødeleggelse på objekter»[21] (Forsvaret, 2013, s. 190).

I media og blant folk flest brukes begrepene cyberangrep, dataangrep og IKT-angrep om hverandre, og de betegner hendelser av forskjellig alvorlighetsgrad (Utheim, 2013). I Cyberforsvaret har man, i tråd med krigens folkerett, vært restriktiv med bruk av begrepet. Generalmajor Sundseth har begrunnet dette slik: «For oss fagmilitære er det slik at begrepet *angrep* veier tungt. Det å bli angrepet er ikke noe vi tar lett på, og det er en handling som hos oss møtes med klar respons. Det er, med andre ord, et tyngre vektet begrep i den fagmilitære verden enn det er i resten av samfunnet» (Sundseth, 2013).

[20] *Krise* er også et begrep uten en klar definisjon, men dette begrepet ble drøftet i kapittel 3.
[21] Den generelle definisjonen av angrep gis i punkt 2.2. i manualen.

Forsvarsdepartementet har i ettertid definert cyberangrep som «handlinger i eller gjennom cyberdomenet med hensikt å skade eller påvirke personell, materiell eller konfidensialiteten[22], integriteten[23], tilgjengeligheten[24] eller autentisiteten[25] til et informasjonssystem» (FD, 2014, s. 5).

Et angrep innbefatter en villet handling fra en aktør som har til hensikt å påvirke informasjonssystemet eller informasjonen som ligger lagret der. Effekten av angrepet kan ramme selve informasjonssystemet eller infrastruktur som styres av informasjonssystemet (FD, 2014, s. 5). Forsvarsdepartementets definisjon av angrep omfatter målrettede angrep med ulike formål, herunder både spionasje og sabotasje. Angrep er ikke avgrenset til de hendelser som går ut over overlevelsesevnen, men omfatter også hendelser som påfører ulempe eller påvirker livskvaliteten. Denne studien baseres på departementets terminologi.

Begrepet *cyberhendelse* brukes av Forsvarsdepartementet både om situasjoner der IKT-systemer blir utsatt for cyberangrep og ved utilsiktet svikt. Alvorlige cyberhendelser er «cyberhendelser som rammer samfunnskritisk infrastruktur, samfunnskritisk informasjon eller samfunnskritiske funksjoner på en slik måte at det får betydning for samfunnets og befolkningens trygghet» (FD, 2014, s. 5).

Hva innebærer cybersikkerhet?

Regjeringen sier at den vil koble Cyberforsvaret inn i sivil cybersikkerhet, men hva innebærer cybersikkerhet? Informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet er begreper som brukes om hverandre, og folk legger

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

tilsynelatende litt forskjellig i begrepene. En som har forsøkt å skape klarhet i begrepsbruken er Morten Irgens, viserektor ved Høgskolen i Gjøvik og dekan ved Avdeling for informatikk og medieteknikk. Irgens understreker at *informasjonssikkerhet* har med sikring av informasjon å gjøre, uavhengig av om den er lagret digitalt eller ikke. *IT-sikkerhet* derimot handler om sikring av selve informasjons- og kommunikasjonsteknologien (IKT), altså maskinvare og programvare. *Cybersikkerhet* dreier seg derimot om sikring av alt som er sårbart via IKT. Irgens har laget en modell (figur 10) som illustrerer forskjellen på begrepene:

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

Feltet *analog informasjon* i figur 10 omfatter mange typer informasjon, herunder bøker og håndskrevne notater, men også informasjon som gis muntlig. *Annet enn informasjon* dekker mengden av faktorer som er sårbare via IKT. Et eksempel er det iranske atomanlegget som i 2010 ble angrepet av dataormen Stuxnet, som for alvor viste verden hvilken industriell og militær sprengkraft et cyberangrep kan ha. Viruset skal angivelig ha manipulert de såkalte spin-syklusene til sentrifugene som anriket uran, slik at de så å si ristet seg selv i stykker.

Irgens argumenterer for at også naturen, dyr og mennesker kommer inn under den samme sårbarhetskategorien *(annet enn informasjon).* Dersom noen for eksempel sender råseptik ut i drikkevannet i Oslo via kontrollsystemet på renseanlegget oppe ved Maridalsvannet, vil det få konsekvenser for natur, dyr og mennesker. Irgens' forståelse av begrepet stemmer tilsynelatende godt med Langø og Sandviks beskrivelse i artikkelen «Cyberspace og sikkerhet». For dem handler cybersikkerhet «i første rekke om trusler mot individer, organisasjoner eller samfunn gjennom og i dette cyberspace-miljøet» (Langø og Sandvik, 2013, s. 222).

Det eksisterer ingen nasjonal strategi for cybersikkerhet, men Regjeringen har gitt ut en nasjonal strategi for informasjonssikkerhet. Strategien er sektorovergripende og omhandler også Forsvarets ansvar innen informasjonssikkerhet. Forsvarsdepartementet offentliggjorde sine cyberretningslinjer for forsvarssektoren 1. mars 2014. Retningslinjene er innrettet mot håndtering av digital informasjon og informasjonssystemer (FD, 2014). Disse dokumentene til sammen kan forventes å gi en indikasjon på hvilke aktører som har ansvar og roller dersom sivil kritisk infrastruktur utsettes for et cyberangrep.

Nytt domene – nye gråsoner – nye dimensjoner

En cybertrussel kan oppstå helt uten forvarsel, sa forsvarsminister Ine Eriksen Søreide under sikkerhetskonferansen 2014. En hendelse kan eskalere fra lokalt nivå til nasjonalt og videre til internasjonalt på sekunder. Ministeren kalte dette en fundamental erkjennelse. Hun påpekte at overrumplingsmomentet utfordrer beredskapssystemet vårt, som er tuftet på at vi normalt har et minimum av tid til å sette inn mottiltak. Søreide fremhevet viktigheten av at alle samarbeider godt. Hun erkjente samtidig at samarbeidet på tvers av sektorene er ikke godt nok i dag (Søreide, 2014).

Det at et angrep kan ramme uten forvarsel er likevel ikke helt unikt for cyberdomenet. Det var ingen som hadde forutsett angrepene 22. juli, og det er ikke tvil om at bomben rammet regjeringskvartalet like brått som

brutalt. Imidlertid innebar angrepet likevel en fysisk forberedelse, og det andre angrepet innebar en fysisk forflytning som kanskje kunne ha vært oppdaget og stoppet.

Roger Johnsen påpeker i artikkelen «Cyberkrigføring og Forsvarets operative evne» at det ikke er enkelt å observere styrkeoppbygging i cyberdomenet. Eskalering av konflikten krever ikke fremføring av militære styrker, og angripers fysiske posisjon er lite relevant (Johnsen, 2013, s. 245).

Det er sivile myndigheter, med politiet i spissen, som skal sørge for den indre sikkerheten i Norge. Forsvaret skal i prinsippet bare ivareta rikets sikkerhet i forhold til eksterne trusler. Forskeren Kristin Bergtora Sandvik påpeker at cyberangrep kan befinne seg i en *gråsone* mellom Forsvar og politi. Dette skyldes at angriperen kan inneha flere roller. Vedkommende kan for eksempel være en såkalt *patriotisk hacker* og samtidig jobbe på direkte oppdrag fra en statsmakt. Hvorvidt cyberangrepet kan sies å være økonomisk eller militært motivert, vil avhenge av «hvor omfattende og sofistikert angrepet er, men også av geopolitiske betraktninger, av de strategiske ressursene til landet som blir angrepet, og av hvem aggressoren antas å være» (Sandvik, 2013, s. 252).

Høyrepolitiker Anders Werp mener det vil være så vanskelig å fastslå om et cyberangrep er en kriminell handling eller krigshandling at det kan bli full forvirring om hvem som har ansvaret dersom nasjonen vår rammes av et alvorlig cyberangrep. Han hevder at det er «komplett umulig å skille mellom det militære og sivile ansvaret» (Gabrielsen, 2013).

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

Ifølge Forsvarsdepartementet er digitale angrep særegne på den måten at de som hovedregel forårsaker relativt beskjedne eller ingen direkte fysiske skader, samtidig som den umiddelbare konsekvensen og de avledede/indirekte skadene kan være betydelige (FD, 2012a, s. 1, 2). Et cyberangrep vil i første rekke kunne ramme samfunnssikkerheten ved at kritiske funksjoner settes ut av spill, men avhengig av omfang og mål kan det også true statssikkerheten (Prop. 73 S (2011—2012), s. 24). Imidlertid vil det ofte være vanskelig å fastslå angrepets mål. For det første kan ett og samme system brukes til både militære og sivile formål. Systemer kan, som vist i kapittel 4, være knyttet sammen på en måte som gjør at et angrep på det ene feltet får konsekvenser for det andre. Et angrep vil også kunne føre til følgeskader som ikke var intendert. På den annen side vil de tette koblingene også kunne utnyttes. Erfaring fra moderne krigføring viser at cyberoperasjoner rettet mot sivil IKT-infrastruktur «må kunne forventes å være en del av et militært anslag fra en statspart» (Innst. 388 S (2011—2012), s. 80). En fiende vil derfor kunne tenkes å angripe Telenors datasystemer for å ramme offentlige myndigheter (NUPI, 2011).

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

Juridiske og folkerettslige utfordringer

Kristin Bergtora Sandvik understreker i artikkelen «Cyberkrig og internasjonal rett» at cyberkriminalitet, cyberterrorisme og cyberkrig stiller både nasjonale myndigheter og det internasjonale samfunnet overfor store lovtekniske utfordringer. Alvorlige cyberangrep kan representere forbudt maktbruk, men Sandvik påpeker at det er omdiskutert hvor denne grensen går. En tilnærming er å se på hvilket instrument som er brukt og vurdere hvorvidt konsekvensene tilsvarer kinetisk maktbruk, en annen tilnærming har vært å betrakte alle angrep på kritisk infrastruktur som væpnede angrep, mens

den tredje tilnærmingen er å se på de samlede konsekvensene for staten (Sandvik, 2013, s. 258). Sandvik understreker at vilkårene for å kunne tilskrive en stat ansvaret for angrep utført av en tredjepart fra statens territorium er omdiskuterte. Det er usikkert hvorvidt det eksisterende rammeverket er i stand til å skille mellom ulike aktiviteter som cyberspionasje, nettverksangrep og aktiviteter som krysser terskelen for å utgjøre *væpnede angrep*.

Det avgjørende kriteriet for at en stat kan holdes ansvarlig for et cyberangrep utført av ikke-statlige aktører er, ifølge Forsvarsdepartementet, at «staten har effektiv kontroll over eller direkte instruerer den gjeldende grenseoverskridende rettstridige cyberoperasjonen begått av den ikke-statlige aktøren» (FD, 2012a, s. 3). FN-paktens artikkel 2(4) gir et klart definert forbud mot statlig maktbruk mot andre stater. Departementet sier at det er naturlig å se på ikke bare hvilket virkemiddel som brukes, men hvilket skadepotensial virkemidlet har.

Cyberangrep vil bare unntaksvis være tilstrekkelig alvorlige til å utløse reglene om maktbruk og selvforsvar etter folkeretten. Oftest vil det dreie seg om forstyrrelser der det vil være aktuelt å iverksette mottiltak. Mottiltak defineres i denne sammenheng som «ellers ulovlige handlinger som gjøres lovlige på grunn av en forutgående ulovlig handling — i denne sammenheng et ulovlig dataangrep» (FD, 2012a, s. 3) Som eksempel på mottiltak nevner FD diplomatiske reaksjoner, import- og eksportforbud.

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

Det er internasjonal enighet om at krigens folkerett skal gjelde også for cyberoperasjoner. «Cyberangrep er underlagt de samme begrensninger og

reguleringer som andre typer angrep», heter det i *Manual i krigens folkerett*[26] (Forsvaret, 2013, s. 190). Samtidig erkjennes det at den konkrete anvendelsen kan by på utfordringer.

Oppsummering

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

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

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

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

Kapittel 5
Aktører, ansvar og oppgaver i det nasjonale cyberdomenet

PST har i lengre tid vært bekymret for at myndighetene ikke har god nok kontroll over det norske ekom-nettet. De har tatt opp sin bekymring knyttet til spionasje og manipulering av telenettet gjentatte ganger med Regjeringen, blant annet i et intervju med TV2 i februar 2014. Da TV2 konfronterte Justisministeren med dette, hevdet han at sikkerheten i ekom-nettet hører inn under samferdselsministerens ansvar. Samferdselsministeren på sin side påpekte at han ikke har ansvar for «spionasje og sånne ting» og pekte på justisminister og forsvarsminister. Det er «viktig at vi fordeler ansvaret der det er riktig at det ligger», sa samferdselsministeren (Østby, 2014).

Hvem har egentlig ansvaret?

For å kunne drøfte Cyberforsvarets rolle ved en alvorlig cyberhendelse i ekom-infrastrukturen må vi ha en viss kjennskap til de ulike aktørene, deres ansvar og oppgaver. De sivile aktørenes antatte kapasitet indikerer om de vil kunne få behov for bistand eller ei. Cyberforsvarets oppdrag og kapasiteter vil på sin side gi en god indikasjon på hva det vil kunne bistå med, og kanskje like viktig — hva det ikke vil bistå med.

Ved hjelp av en innholdsanalyse skal dette kapitlet kartlegge og diskutere hvilke aktører som er gitt ansvar, oppgaver og myndighet knyttet til ekom-infrastruktur og håndtering av en eventuell cyberhendelse. Videre vil vi belyse aktørenes antatte kapasitet.

Nasjonal strategi for informasjonssikkerhet

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

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

De fire andre prioriteringene handler mer om forebyggende arbeid, bevisstgjøring og kompetanseheving.

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

Nasjonal sikkerhetsmyndighet

NSM og Forsvarssjefens sikkerhetsavdeling (FSA) ble opprettet 1. januar 2003, samtidig som Forsvarets overkommando/Sikkerhetsstaben (FO/S) ble lagt ned. FSA ble opprettet til støtte for Forsvarssjefen, mens NSM ble opprettet som et direktorat under FD for å ivareta overordnede og tverrsektorielle sikkerhetsoppgaver i henhold til sikkerhetsloven (St.prp. nr 1 (2002—2003), s. 30). NSM ivaretar de utøvende funksjoner i sikkerhetsloven på vegne av departementet, fører tilsyn med sikkerhetstilstanden i virksomheter underlagt loven og kan ved behov gi pålegg om forbedringer (Sikkerhetsloven, 1998). Samtidig er fagmiljøet i NSM viktig for å understøtte JDs ansvar for IKT-sikkerhet[27]. NSM rapporterer direkte til JD hva angår oppgavene i sivil sektor. VDI ble opprettet høsten 2000 som en prøveordning og ble fra 2003 etablert fast under NSM.

NSM er det sentrale direktorat for informasjons- og objektsikkerhet. I NSMs årsrapport for 2013 innleder direktør Kjetil Nilsen med å si at nasjonen ikke er godt nok sikret når det gjeler internett og datasystemer. NSM har utvidet med 60 nye personer og har nå passert 200 ansatte som skal hjelpe norske virksomheter til å styrke sin egen sikkerhet i fremtiden. Å sikre samfunnets evne til å oppdage, varsle og håndtere alvorlige IKT-hendelser er et prioritert område i *Nasjonal strategi for informasjonssikkerhet*. Målsettingen er at «Norge skal ha en døgnkontinuerlig, proaktiv operativ beredskap for å kunne forebygge, oppdage og koordinere håndteringen av alvorlige IKT-hendelser» (Regjeringen, 2012a, s. 21).

Begrepet *alvorlige IKT-hendelser* er i strategien definert til å være målrettede angrep mot kritisk IKT-infrastruktur samt sensitiv, taushetsbelagt og gradert informasjon. Det påpekes at både myndigheter og infrastruktureiere skal inngå i samarbeidet. NorCERTs rolle som nasjonal CERT fremheves spesielt — NorCERT er operasjonssenteret i NSM.

NorCERT skal ved hjelp av VDI og nasjonalt samarbeid ha «evne til å forebygge, oppdage og analysere data knyttet til alvorlige hendelser på internett»

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

(Regjeringen, 2012a, s. 21). NorCERT er i tillegg gitt i ansvar å koordinere håndteringen av slike hendelser, men hva Regjeringen legger i å *koordinere håndteringen* står ikke beskrevet.

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

I årsrapporten fra NSM fremkommer det at NorCERT i 2013 behandlet 3901 saker manuelt ved varsling, dialog og analyse (NSM, 2014a, s. 4). Femti av disse ble kategorisert som alvorlige. NSM sier flere av angriperne kan ha vært inne i de aktuelle datasystemene over flere år, noe som gir grunn til å stille spørsmål ved vår evne til å oppdage innbrudd. NSM fremstiller sensornettverket, VDI, som den *digitale innbruddsalarmen for AS Norge*, men virkeligheten tyder på at AS Norge ikke har alarm på alle dører og vinduer (NSM, 2014b, s. 33).

NSMs arbeid med objektsikkerhet er blitt intensivert de siste årene. I 2013 ble utpekt flere hundre *skjermingsverdige objekter*: «eiendom som må beskyttes mot spionasje, sabotasje eller terrorhandlinger av hensyn til rikets eller alliertes sikkerhet eller andre vitale nasjonale sikkerhetsinteresser» (Sikkerhetsloven, 1998: § 3).

Forskrift om objektsikkerhet[28] gjelder for alle statlige og kommunale forvaltningsorganer samt de virksomheter som er omfattet av sikkerhetsloven (FD, 2009). Forskriften skal sikre at objekter blir identifisert og beskyttet i henhold til en felles standard. Objekteier har ansvar for defensive og forebyggende sikring, mens politiet på sin side skal ivareta de offensive tiltakene. Om nødvendig kan politiet bruke makt for å hindre eller begrense anslag mot objekter.[29]

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

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

Ved siden av de ovennevnte oppgavene leder NSM den nasjonale, tverrfaglige Cyberkoordineringsgruppen (CKG). Gruppens medlemmer kommer fra NSM, E-tjenesten og PST. Gruppens formål er å fremskaffe tidsriktig informasjon om trusler i cyberdomenet for å gi et beslutningsgrunnlag til den operative og strategiske ledelsen. Gruppen vedlikeholder og formidler et helhetlig cyberrisikobilde (FD, 2014).

Justis- og beredskapssektoren

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

I *Nasjonal strategi for informasjonssikkerhet* fastslås det at politiet «skal ha tilstrekkelig kompetanse og kapasitet til å avdekke, identifisere og håndtere datakriminalitet» (Regjeringen, 2012a, s. 23). Begrepet datakriminalitet defineres som «kriminalitet rettet mot datasystemer og datanettverk, og kriminalitet hvor sentrale elementer av handlingsforløpet begås ved hjelp av datautstyr eller datanettverk» (Regjeringen, 2012a, s. 22). Datakriminalitet er et bredere begrep og dekker et større omfang enn «alvorlige IKT-hendelser og alvorlige hendelser på internett», som NorCERT er gitt i ansvar å koordinere håndteringen av.

I henhold til *Nasjonal strategi for informasjonssikkerhet* har politiet fått i oppgave å håndtere cyberangrep mot kritisk ekom-infrastruktur. Dette samsvarer også godt med politiloven. I politilovens § 2 i står det at politiet skal beskytte samfunnet og verne om lovlig virksomhet, opprettholde orden og sikkerhet og verne mot alt som truer den alminnelige tryggheten i samfunnet.

En arbeidsgruppe nedsatt av POD (heretter omtalt som arbeidsgruppen), kartla i 2012 politiets arbeid med IKT-kriminalitet, elektroniske spor og politioppgaver på nett. Arbeidsgruppen refererte til paragraf § 2 i politiloven og fastslo at dette «må også gjelde for Internett» (Storruste og Magnussen, 2012, s. 23). Arbeidsgruppens rapport, *Politiet i det digitale samfunnet,* indikerer imidlertid at politiet ikke har tilstrekkelig kompetanse og kapasitet til å håndtere datakriminalitet i dag. Politidistriktene arbeider i liten grad med denne typen kriminalitet, det er ikke etablert egne enheter for å ivareta disse sakene og sakene fordeles derfor på ulike driftsenheter og etterforskningsmiljøer. Politiet foretar ikke noen «systematisk patruljering på Internett». I den grad de i det hele tatt utfører politiarbeid på internett, «skjer det sporadisk av tjenestemenn med forskjellig grad av opplæring og erfaring» (Storruste og Magnussen, 2012, s. 17).

Kripos er et særorgan underlagt POD. Kripos skal ha spisskompetanse på en rekke fagområder, deriblant kommunikasjonskontroll og sporing på internett (Politiet, 2011, s. 46). Rapporten *Politiet i det digitale samfunnet* påpeker at Kripos har et særskilt ansvar for å etterforske alvorlig IKT-kriminalitet. Det understrekes at Kripos har erfaring med etterforskning av grove skadeverk, men det omtales ikke i hvilken grad de innehar oppgaver eller erfaring knyttet til håndtering av pågående skadeverk. Rapporten indikerer imidlertid at Kripos har begrenset kapasitet, og dette skal være en av grunnene til at distriktene

ofte blir stående fast i de sakene som krever datateknisk kompetanse — fordi de ikke får tilgang på bistand fra Kripos. I rapporten heter det at dataangrep mot sentrale samfunnsinstitusjoner grenser mot PSTs arbeidsområde, men grensene mellom PST og andre enheter i politiet er ikke nærmere beskrevet i rapporten (Storruste og Magnussen, 2012).

PST er Norges sivile etterretnings- og sikkerhetstjeneste og har ansvar for nasjonens indre sikkerhet. PSTs primære oppgave er, som gitt i politiloven, å forebygge og etterforske straffbare handlinger mot nasjonens sikkerhet. PST utarbeider trusselvurderinger som ledd i arbeidet med å ivareta den norske stats sikkerhet og selvstendighet. Etaten har en rådgivende funksjon for regjeringen og andre norske myndigheter. PST skal ha fått økte bevilgninger til området cybersikkerhet de siste årene (Meld. St. 21 (2012—2013), men det fremkommer ikke i denne studiens forskningsmateriale hva den vil kunne bidra med ved et pågående cyberangrep.

Det er gjennomgående forebygging og etterforskning som står i fokus i PODs rapport. Håndtering av cyberhendelser ved bruk av den makt og myndighet som tilligger politiet er ikke omtalt i rapporten. Dette kan være en indikasjon på at politiet ikke innehar tilstrekkelig kapasitet. Politiets målsetting er å håndheve lov og orden i det digitale samfunnet på en effektiv og sikker måte (Storruste og Magnussen, 2012, s. 25), men innholdet i rapporten antyder at dette ikke var tilfellet i 2012. Imidlertid kan det ha skjedd endringer i ettertid.

Samferdselssektoren

Samferdselsdepartementet har ansvar for sikkerheten knyttet til ekomnett og ekom-tjenester. Departementet forvalter loven om elektronisk kommunikasjon (ekomloven) og etatsstyrer PT. Å styrke IKT-infrastrukturen oppgis som et prioritert område i *Nasjonal strategi for informasjonssikkerhet*. Samferdselsdepartementet er gitt i ansvar å sørge for en robust og pålitelig ekom-infrastruktur, begrense konsekvensene ved utfall og øke sikkerheten i mobilnettene (Regjeringen, 2012b, s. 15— 17). PT har på vegne av departementet

ansvar for å sette krav til telesikkerhet og teleberedskap, vurdere tiltak for å øke robustheten i telenettene, samt føre tilsyn med at pålagte tiltak blir iverksatt (PT, 2014). PTs vurdering er at operatørene har gjennomgående god evne til å håndtere løpende drift, men at de ikke har tilfredsstillende fokus på og evne til å opprettholde nødvendig sikkerhet i ekstraordinære situasjoner. Denne vurderingen gjorde PT blant annet på grunnlag av sårbarheter i utstyr og nettstrukturer, herunder:

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

(PT, 2012a, s. 9, 10).

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

Ekomloven stiller krav til at tilbyder må opprettholde nødvendig beredskap og tilby sine ekom-nett og tjenester med forsvarlig sikkerhet i hele spekteret fra fred til krig (Ekomloven, 2003). Dette er helt i tråd med ansvarsprinsippet, som ble presentert innledningsvis i kapittel 3: Den som har ansvar for en virksomhet under normale forhold, har også et ansvar i en krisesituasjon. I kravet om nødvendig beredskap ligger det at nett og tjenester skal sikres på en slik måte at brukerne, selv i situasjoner der nettet utsettes for ekstraordinære påkjenninger, så langt som mulig skal kunne benytte grunnleggende ekom-tjenester.

Nasjonal strategi for informasjonssikkerhet påpeker at infrastruktureierne i IKT-sektoren skal inngå i den proaktive operative beredskapen for å forebygge, oppdage og koordinere håndteringen av alvorlige IKT-hendelser.

Telenor er den dominerende leverandøren av ekom-nett og teletjenester i Norge og vies derfor ekstra oppmerksomhet i denne innholdsanalysen. I et innlegg i debatten om *digital robusthet* fremhever administrerende direktør i Telenor, Berit Svendsen, at robustheten til et tele- og datakommunikasjonsnett er avhengig av en betydelig drifts-, beredskaps- og sikkerhetsorganisasjon. Telenor har etablert et eget responsmiljø, Telenor Security Operations Centre, TSOC. Operasjonssentralen overvåker Telenors infrastruktur for å avdekke eventuelle fysiske brudd, programvarefeil og sikkerhetstrusler. Hvert eneste døgn blir det oppdaget små feil og iverksatt feilretting (Svendsen, 2014). Ved hjelp av egne sensorer i sin infrastruktur kan Telenor oppdage og varsle sine kunder om angrep. På bloggen sin sier TSOC at de «driver en 24/7-tjeneste for sikkerhetsovervåkning av kunders nettverk», og at deres analytikere «gjør kontinuerlig analyse av uønsket aktivitet på internett» (Telenor SOC, 2014).

Forsvarssektoren

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

Forsvarsdepartementets målsetting er at Forsvarssektoren skal ha tilstrekkelig informasjonssikkerhet i cyberdomenet, og til enhver tid forebygge, avdekke, vurdere og forsvare seg mot cyberangrep. Sektoren skal være forberedt på å håndtere alle former for hendelser som kan ramme egne IKT-systemer og

ha evne til å gjenopprette normal funksjonalitet. Cyberforsvaret har ansvar for å beskytte Forsvarets egen infrastruktur og ivareta håndtering i Forsvaret, mens NSM har et nasjonalt sektorovergripende ansvar for informasjonssikkerhet.

Forsvarsdepartementet fremhever at det er viktig å sikre nødvendig samordning med sivil sektor i cyberkriser, og påpeker at det er NSM som skal koordinere. Samtidig konstaterer departementet at de cyberangrep som krever koordinering på sentralt nivå, skal håndteres i henhold til gjeldende prinsipper for sentral krisehåndtering (FD, 2014, s. 11). Den sentrale krisehåndteringen består som tidligere nevnt av et lederdepartement (skal ivareta samordningen mellom departementene i mindre alvorlige kriser), Kriserådet (skal sørge for samordningen i komplekse kriser), og Krisestøtteenheten (skal være sekretariat for sivil krisehåndtering).

Den enkelte fagstatsråd har ansvar for krisehåndtering innenfor egen sektor og for å samordne denne med øvrige departementer og sektorer. Hvor NSMs koordineringsrolle kommer inn i det sentrale krisehåndteringsapparatet, er ikke spesifisert. FD sier at Forsvarets bistand ved cyberhendelser kan innebære eksempelvis faglig rådgivning, støtte fra enheter med særskilt kompetanse og bistand til gjenoppretting av kommunikasjonsnettverk (FD, 2014, s. 12).

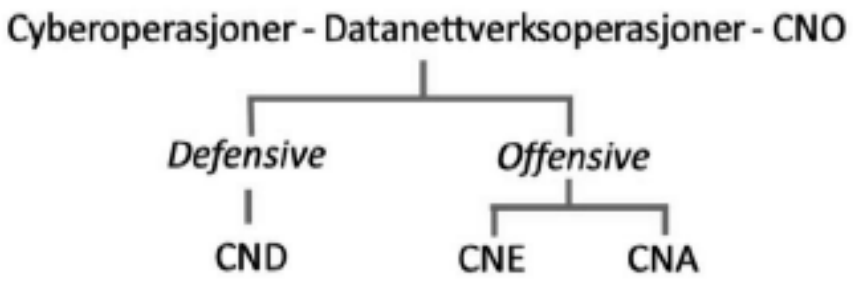
Cyberoperasjoner

Cyberoperasjoner er operasjoner som har til hensikt å nå definerte målsettinger i og gjennom cyberdomenet, herunder tiltak for å påvirke motstanders datanett og beskytte egne nett. Begrepene cyberoperasjoner og datanettverksoperasjoner omtales som synonymer i FDs cyberretningslinjer og tilsvarer det som i NATO kalles Computer Network Operations (CNO).

I NATO-doktrinen *Allied Joint Doctrine for Information Operations* (AJP 3.10) beskrives CNO som en av flere informasjonsaktiviteter. Poenget er å påvirke

motpartens vilje, forståelse og evne til støtte for alliansens oppdrag, samt å sikre at egen informasjon blir ivaretatt, slik at denne er trygg og tilgjengelig for egne beslutningstakere (NATO, 2009). CNO omfatter Computer Network Exploration (CNE), Computer Network Attack (CNA) og Computer Network Defence (CND). FD sier at CNE skal bidra til å «søke etter, fange opp, identifisere og lokalisere aktiviteter og informasjon i cyberdomenet i den hensikt å oppnå situasjonsforståelse og for å kunne gjenkjenne trusler». CNA skal «bidra til å redusere eller hindre en motstanders evne til å utnytte cyberdomenet til egne operasjoner», mens CND «er å anse som en defensiv aktivitet som skal sikre handlefrihet i egen informasjonsinfrastruktur, til tross for offensive aktiviteter fra en motstander» (FD, 2014, s. 6).

Cyberoperasjoner kategoriseres, som vist i figur 11, i offensive og defensive operasjoner. De offensive omfatter både CNE og CNA, mens CND er defensiv. Nasjonalt er det E-tjenesten som har fått ansvar for offensive cyberoperasjoner og Cyberforsvaret for defensive cyberoperasjoner.



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

E-tjenesten – offensive cyberoperasjoner

E-tjenesten er underlagt Forsvarssjefen, men den er ikke avgrenset til å arbeide med militære problemstillinger. Tjenesten arbeider innenfor de saksfeltene overordnede politiske og militære myndigheter til enhver tid prioriterer (Etterretningstjenesten, 2014). I sin FOKUS-vurdering for 2014

sier E-tjenesten at den primært har fokus på cybertrusler fra statlige aktører, eksempelvis Russland og Kina. Dernest er tjenesten opptatt av «selvstendige, ikke-statlige aktører som opererer på vegne av, støttes eller utnyttes av statlige myndigheter» og organiserte ekstremistgrupper (Etterretningstjenesten, 2014, s. 59).

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

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

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

Cyberforsvaret – defensive cyberoperasjoner

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

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

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

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

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

Det er angrep på logiske sårbarheter[30] i ekom-infrastrukturen som står i fokus i denne studien. *Avdeling for beskyttelse av kritisk infrastruktur* (BKI) i Cyberforsvaret antas å ha særskilt kompetanse på dette feltet. BKI-miljøet var tidligere en del av FOST (FSA), men ble etter opprettelsen av INI overført dit. BKI skal «bidra til å beskytte Forsvarets infrastruktur gjennom støtte til

[30] Jf s. 19: Logiske sårbarheter omfatter sårbarheter realisert i programvare, herunder protokoller og tjenester samt logisk redundans. Angrepsmidler mot logiske sårbarheter kan være «alt fra utnyttelse og bruk av allmenn tilgjengelig infrastruktur og kode som publiserte nettverksverktøy på Internett, til angrepskode og mer».

analyse av sårbarheter, ondsinnet kode og angrep mot Forsvarets systemer. Avdelingen har deployerbare elementer og mulighet til å bistå med rådgivning og liaisonering ved håndtering av trusler og angrep mot norsk infrastruktur ute og hjemme» (Prop. 73 S (2011—2012), s. 103). Avdelingen utgjør *Forsvarets sentrale responsmiljø* (CERT).

I en reportasje i *Forsvarets Forum* 2013 ble BKI og *Cyber-ambulansen* presentert. Utrykningskapasiteten ble beskrevet i form av tre biler med tilhengere, klargjort og tilpasset for *cyberkrig* og klare til å rykke ut på kort tid. Den militære styrken skulle bestå av «noen dusin mannlige og kvinnelige dataingeniører» (Ravnaas, 2013). «I prinsippet kan vi koble oss til og bistå hvem som helst, når som helst og hvor som helst», sa oberstløytnant Gunnar Salberg, daværende sjef for BKI. Samtidig presiserte han at det er NorCERT og NSM som sitter i førersetet når det gjelder bistand til næringsliv og det sivile samfunn, mens BKI er en ekstra ressurs som kan benyttes ved behov. Både banker, kraftselskaper og andre viktige aktører kan i gitte tilfeller få nyttig assistanse av styrken, enten til å analysere en hendelse eller til å løse den mer konkret og direkte (Ravnaas, 2013).

Salberg påpekte samtidig at BKIs hovedansvar er sikring av Forsvarets egne nettverk, eksempelvis ved øvelser og operasjoner: «I likhet med baser som har kringvern i form av soldater og vaktposter, sikrer BKI eksempelvis datanettverk på øvelser» (Ravnaas, 2013). I samme intervju avkreftet Salberg myten om at Cyberforsvaret kan gå til motangrep i cyberspace: Hovedvekten ligger på «defensive operasjoner der vi overvåker, avslører og setter i gang tiltak for å forhindre nye angrep».

Oppsummering

Ekom-leverandørene skal kunne forebygge, oppdage og koordinere håndteringen av alvorlige IKT-hendelser i egen infrastruktur. De skal opprettholde nødvendig beredskap til at grunnleggende ekom-tjenester også skal kunne benyttes i situasjoner hvor nettene utsettes for ekstraordinære

påkjenninger. PTs vurdering er at operatørene ikke har tilstrekkelig fokus på og evne til dette i dag.

Operasjonssenteret i NSM, NorCERT, skal ved hjelp av VDI og nasjonalt samarbeid ha evne til å oppdage og analysere data knyttet til alvorlige hendelser på internett, samt å varsle andre virksomheter om dette. Det er imidlertid frivillig å være med i VDI-samarbeidet, også for de virksomheter som eier kritisk infrastruktur. Hvordan NorCERT skal kunne oppdage og analysere data knyttet til angrep mot en virksomhet hvor de ikke har sensor, fremkommer ikke. Dersom en hendelse rammer flere virksomheter, har NorCERT fått i ansvar å *koordinere håndteringen*, uavhengig av om disse virksomhetene er med i VDI-samarbeidet eller ei. Det er imidlertid ikke beskrevet hva denne koordineringen innebærer, og NSMs myndighet er avgrenset til håndhevelse av sikkerhetsloven.

Ansvar for offensive tiltak og myndighet til å bruke makt for å hindre eller begrense anslag mot objekter ligger hos politiet, både i de fysiske og digitale domener. Innholdsanalysen i denne studien viser at politiet er gitt i ansvar å avdekke, identifisere og håndtere datakriminalitet, uavhengig av om denne rammer en eller flere virksomheter. De skal altså kunne håndtere et pågående cyberangrep mot ekom-infrastrukturen ved bruk av den makt og myndighet som tilligger politiet. Imidlertid tilsier analysen at politiet ikke har tilstrekkelig kompetanse og kapasitet til å håndtere dette i dag. Politidistriktene arbeider i liten grad med denne typen kriminalitet, de foretar ikke noen systematisk patruljering på internett, og i den grad de i det hele tatt utfører politiarbeid på internett, skjer det sporadisk av tjenestemenn med forskjellig grad av opplæring og erfaring. Politiet vil neppe ha tilstrekkelig kapasitet til å ivareta sitt ansvar dersom ekom-infrastrukturen rammes av en alvorlig cyberhendelse. I slike tilfeller vil det altså kunne bli behov for bistand.

Cyberforsvarets ansvar og myndighet er knyttet til Forsvarets kommunikasjonsinfrastruktur. Cyberforsvarets oppdrag er å etablere, drifte, videreutvikle, beskytte og bekjempe trusler mot denne infrastrukturen, samt understøtte Forsvarets operasjoner hjemme og ute.

Cyberforsvaret skal i tillegg kunne yte bistand til sivil sektor ved digitale angrep. Det siste er likevel ikke en dimensjonerende oppgave for Cyberforsvaret, og det skal kun skje dersom det ikke finnes relevante sivile ressurser. I

en cyberkrise skal Forsvaret kunne bistå med faglig rådgivning og støtte fra enheter med særskilt kompetanse. Den enheten som vurderes å være mest sentral ved angrep på logiske sårbarheter i ekom-infrastrukturen, er Cyberforsvarets *Avdeling for beskyttelse av kritisk infrastruktur* (BKI). Avdelingen har deployerbare elementer og mulighet til å bistå med rådgivning og liaisonering ved håndtering av trusler og angrep mot norsk infrastruktur.

Innholdsanalysen viser at det fortsatt er noe uklarhet rundt ansvar og oppgaver knyttet til håndteringen av cyberangrep, samt at sivile myndigheter vil kunne få behov for bistand dersom ekom-infrastrukturen rammes av en alvorlig cyberhendelse. Videre viser analysen at Cyberforsvaret besitter relevante kapasiteter som kompetanse, verktøy og erfaring fra sikring av egen infrastruktur. Det trengs likevel ytterligere empiri for å kunne si noe mer presist om Cyberforsvarets rolle.

Kapittel 6
Cyberforsvarets rolle ved et angrep på sivil infrastruktur

Det er liten tvil om at sivile myndigheter vil kunne få behov for bistand dersom nasjonen rammes av et alvorlig cyberangrep. For bedre å kunne drøfte når og hvordan Cyberforsvaret skal bistå i et slikt tilfelle skal vi se på håndteringen av to cyberhendelser: industrispionasjen mot Telenor og den etterfølgende Øvelse CyberDawn i 2013. Ved å sammenstille erfaringer fra disse to casene vil vi få et bedre grunnlag for å vurdere Cyberforsvarets potensielle rolle dersom ekom-infrastrukturen blir utsatt for et cyberangrep.

Kildene til denne casestudien består av rapporter[31], video[32], medieoppslag[33] og egne intervjuer[34].

[31] Rapport fra Norman Shark om Industrispionasjesaken (Fagerland et al., 2013). Intern rapport forfattet av Telenor, men med bidrag fra alle aktørene etter øvelse CyberDawn (Dyrlie og Landaasen, 2013a).
[32] Telenor gjorde opptak under hele øvelsen og har i ettertid satt dem sammen til en film. Kortversjonen ligger tilgjengelig på internett.
[33] Øvelse CyberDawn fikk medieoppslag både før, under og etter øvelsen. Sentrale aktører ble intervjuet.
[34] Forfatteren har intervjuet 8 ressurspersoner som har mye kunnskap om emnet og som alle sitter i virksomheter som vil være sentrale dersom infrastrukturen skulle rammes av en alvorlig cyberhendelse, herunder NSM, POD, FOH, FD, to fra Telenor og to fra Cyberforsvaret.

Dette kapitlet vil ha fokus på de oppgavene som er vektlagt i *Nasjonal strategi for informasjonssikkerhet,* herunder *oppdage, varsle, analysere, koordinere og håndtere.* Mens innholdsanalysen i kapittel 5 viste hvem som har fått ansvar for å ivareta oppgavene samt aktørenes antatte kapasitet, vil vi nå se på hvem som faktisk ivaretok oppgavene i disse to cyberhendelsene og hvordan. Det ene tilfellet dreide seg om industrispionasje, nærmere bestemt et målrettet internasjonalt angrep mot Telenors forretningsvirksomhet, mens det andre innebar et angrep på samfunnskritisk infrastruktur.

I denne sammenhengen vil vi særlig se på hvilke oppgaver det viste seg å være behov for støtte til. Som en generalisering er det fristende å spørre: Har Cyberforsvaret kunnskap og verktøy til å kunne støtte på de felter der støtten blir etterspurt? Kan Cyberforsvaret bistå gitt dagens prinsipper for krisehåndtering og regulering av det sivil-militære samarbeidet?

Industrispionasjesaken

Vinteren 2013 ble Telenor utsatt for et målrettet cyberangrep. PCene til flere av sjefene i selskapet ble regelrett tappet for data. Innledningsvis var det umulig å si om angrepet kom fra Norge eller utlandet, men mye tydet på at det måtte være godt organiserte og ressurssterke miljøer som sto bak.

Industrispionasjen ble oppdaget av Telenor Security Operations Centre (TSOC). Operasjonssentralen reagerte på at det var unormal trafikk til ukjente IP-adresser i utlandet. Angrepet hadde startet med at ledere i Telenor fikk tilsendt elektronisk post fra tilsynelatende kjente forbindelser. E-postene kom som en av flere i en pågående korrespondanse, skrevet på norsk og med innhold som forventet. E-postene inneholdt imidlertid lenker til infiserte nettsider og/eller infiserte zip-filer. Når disse ble åpnet, ble det installert en ondsinnet kode på harddisken, en trojaner, som så sørget for å sende ut data fra PCen. Logger i Telenors systemer viste at e-post, alle typer filer, passord og andre personlige data var blitt tappet. Fordi så mye forskjellig informasjon ble lastet ned, var det vanskelig å se hva angriperne egentlig var ute etter. Den ondsinnede koden var skreddersydd og ukjent for Telenors underleverandører.

Telenor varslet umiddelbart både NorCERT og Cyberforsvaret og holdt dem løpende orientert underveis. Hendelsen ble også anmeldt til Kripos (Johansen, 2013; NSMs sikkerhetskonferanse, 2013).

Sikkerhetseksperter i det norske firmaet Norman Shark, som hadde utviklet en unik programvare for malware-analyse, gransket skadevaren og avdekket en omfattende global infrastruktur av såkalte kommandoservere — servere som brukes til å sende data eller skadevare, ta imot stjålne data, samt kontrollere ofrenes datamaskiner. Normans analyse tydet på at angrepet stammet fra India, og at samme infrastruktur har vært benyttet til omfattende spionasje mot ofre i minst tolv land. Angrepene skal ha pågått i minst tre år og pågår visstnok fortsatt (Jørgenrud, 2013a). Ifølge Snorre Fagerland, analysesjef i Norman, har majoriteten av angrepene vært rettet mot militæret og myndighetene i Pakistan, men det er ikke funnet bevis for at angrepene er sponset av eller utført på ordre fra en nasjonalstat (Fagerland et al., 2013).

Øvelse CyberDawn 2013

Samme år tok Telenor initiativet til den storstilte øvelsen CyberDawn. Det var også Telenor som ledet øvelsen. I tillegg deltok Cyberforsvaret, DNB, Sparebank 1, NSM og IT-selskapet Evry. I tillegg var Post- og Teletilsynet, Politidirektoratet, Kripos og Asker og Bærum Politidistrikt involvert. Øvelsen ble kjørt 3. og 4. september 2013, samtidig som Forsvarets *Øvelse Hovedstad* foregikk i Oslo og Akershus (29. august til 5. september). Fiktive nyheter ble sendt ut til deltakerne de siste ukene før øvelsen. Disse nyhetene dannet et globalt bakteppe og trusselbilde: Ifølge scenarioet var all handel med aksjer og verdipapirer på den amerikanske Nasdaq-børsen blitt stanset, og NRK hadde informasjon som indikerte at norske hackere kunne gjøre det samme mot norske finansinstitusjoner (Dyrlie og Landaasen, 2013; Tønnesen og Landaasen, 2013a).

Øvelse CyberDawn startet med at datamaskinene til ansatte i Telenor ble kompromittert. I likhet med Industrispionasjesaken tok noen utenfra kontroll

over Telenors maskiner. Angriperen fikk mulighet til å samle informasjon og grave seg videre innover i Telenors systemer.

Til forskjell fra Industrispionasjesaken innebar CyberDawn også at datamaskinene til driftspersonell også ble kompromittert. Angriper fikk tilgang til Telenors database over alle samband i Norge, og vedkommende kunne bruke basen til å planlegge angrep mot transportnettet, samtidig som han manipulerte databasen og gjorde det vanskelig for Telenor å feilsøke. Det var uklart hvilken hensikt angriper hadde, men det var klart at den samfunnskritiske infrastrukturen sto i fare. Telenor varslet derfor både Samferdselsdepartementet og Post- og teletilsynet. Administrerende direktør i Telenor ga ordre om at nettet måtte isoleres for å unngå spredning, og all tilgjengelig ekspertise måtte hentes inn. En nasjonal krise i det digitale rom var et faktum, og Telenor henvendte seg til politiet for å få støtte til å stoppe angrepet. Politiet vendte seg til Forsvaret, og FOH ga Cyberforsvaret ordre om å bistå Telenor (Dyrlie og Landaasen, 2013; Tønnesen og Landaasen, 2013a).

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

Oppdage hendelsen og varsle

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

på internett. Avdelingsdirektør ved operativ avdeling i NSM, Hans Christian Pretorius, understreker at NorCERT kan se trafikken som går inn og ut av de nettverkene hvor de har en VDI-sensor. De kan se om virksomheten lekker data, fra hvilke klienter (IP-adresser) det lekker data og til hvilken server på yttersiden disse dataene sendes til. Alarmer trigges dersom det oppdages trafikk fra en kjent server eller dersom det oppdages kjent skadevare[35] (Pretorius, 2014).

NorCERT mottar varsler fra nasjonale og internasjonale samarbeidspartnere gjennom det sivile CERT-samarbeidet, herunder informasjon om skadevare og kommandoservere[36], og oppdaterer databasen sin fortløpende med denne informasjonen. Det er imidlertid den som har blitt angrepet — den som har signaturen — som bestemmer i hvilken grad NorCERT kan dele denne informasjonen med andre, det vil si varsle andre (Pretorius, 2014).

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

Cyberforsvaret har ansvar for å oppdage og varsle angrep mot Forsvarets sensorinfrastruktur. Forsvaret har en fast infrastruktur med sensorer som er i døgnkontinuerlig drift, i tillegg til mobile ressurser som kan tas ut ved behov. Dette kan for eksempel være å dekke midlertidige behov under operasjoner og øvelser, eller å øke eksisterende sensorkapasitet ved hendelser i de militære nettverkene (Malmedal, 2014; Heen, 2014).

Cyberforsvaret har inngått en samarbeidsavtale med Telenor. Intensjonen med avtalen er først og fremst kompetanseheving. Telenor og Cyberforsvaret sender hverandre sikkerhetsvarsler når de oppdager sårbarheter. Dette er informasjon som for så vidt kan deles med alle via NorCERT, men her deles den direkte, noe som er nyttig for begge parter. For eksempel gjorde den informasjonen Cyberforsvaret fikk fra Telenor i forbindelse med *Industrispionasjesaken* at Cyberforsvaret var i stand til å undersøke om Forsvaret var utsatt for tilsvarende

[35] Begrepene skadevare og malware brukes ofte om hverandre som en fellesbetegnelse på ondsinnet programvare, f.eks. datavirus, ormer og trojanere. Begrepet malware kommer av det engelske uttrykket Malicious Software.
[36] Servere som brukes til å sende data eller skadevare, ta imot stjålne data, samt kontrollere ofrenes datamaskiner.

angrep (Malmedal, 2014). Dersom Forsvarets nettverk hadde vært rammet, ville Cyberforsvaret ha varslet Telenor og NorCERT. Cyberforsvaret støtter i utgangspunktet ikke med noen kapasiteter ut over dette.

Analyse

I forrige kapittel 5 så vi at NorCERT ved hjelp av VDI og nasjonalt samarbeid, herunder samarbeid med den virksomhet som eier ekom-infrastrukturen, skal ha evne til å analysere alvorlige hendelser på internett.

Analyse er i denne sammenheng å etablere situasjonsforståelse, å finne ut hva man er utsatt for, hva skadevaren har gjort og gjør, hva uvedkommende holder på med og hvorfor, samt hvordan man kan minimere konsekvenser og normalisere situasjonen.

NorCERT har gjennom VDI-samarbeidet forpliktet seg til å bistå medlemmer og partnere med analyse. Deltagerne er med på å finansiere NorCERT gjennom medlemskap eller partnerskap.[37] Partnere får tilbud om tettere og bedre oppfølging enn medlemmer, for eksempel støtte på egen lokasjon. Både medlemmer og partnere får mer informasjon og støtte fra NorCERT enn dem som ikke er tilknyttet samarbeidet, uavhengig av om virksomheten forvalter kritisk infrastruktur eller ikke[38] (Pretorius, 2014). Samtidig er det ikke tilfeldig hvem som er en del av samarbeidet.

Pretorius finner det naturlig at de objekter som pekes ut som kritisk infrastruktur også får VDI-sensor etter hvert. Imidlertid er det, som innholdsanalysen viste, opp til eier av objektet å søke om tilknytning til VDI. NorCERTs intensjon og oppdrag er likevel å støtte med det de kan, selv om virksomheten ikke er en del av samarbeidet. Det forutsetter imidlertid at virksomheten sender en RFI (request for information) til NorCERT. I dette ligger det at den angrepne

[37] Partnere betaler 500 000 kr i medlemsavgift, medlemmer 200.000 kr (NSM).
[38] I en krisesituasjon vil imidlertid NorCERT prioritere tiltak og prosedyrer uavhengig av medlemskap/partnerskap og koordinerer hendelseshåndteringen ut fra en helhetlig nasjonal verdivurdering i en krisesituasjon (NSM).

virksomheten selv må si fra om at de *lekker* data til en spesifikk IP-adresse eller at deres sensorer har fanget opp en ukjent signatur, for så å spørre om NorCERT har kjennskap til denne fra før. Dersom NorCERT har kjennskap til serveren eller har signaturen i sin database og slik kjenner hvilke egenskaper denne programvaren har, kan de informere virksomheten om hvilke plattformer som kan ha blitt infisert, hva de skal lete etter og på den måten bistå (Pretorius, 2014).

Analyse omfatter både analyse av malware sample (skadevare) og av nettverk (trafikk og logger). Det er hensiktsmessig å skille mellom disse, da den ene typen analyse forutsetter tilgang til nettverket og den andre ikke. Analyse av skadevare kan i prinsippet gjøres fra hvor som helst, mens analyse eller overvåkning ved bruk av sensorer i nettverket krever tilknytning.

Analyse av malware (skadevare)

I situasjoner som *Industrispionasjesaken* vil den angrepne virksomheten kunne få behov for støtte til analyse av malware. Ettersom angrepene kan ramme uten forvarsel og eskalere raskt, er det viktig å få hurtig oversikt over situasjonen for å begrense skadene. Når flere miljøer og ressurser fra forskjellige virksomheter med sine kontaktnett samarbeider, øker muligheten for å *knekke koden* (Dyrlie, 2014).

Cyberforsvaret skal ha kompetanse og ressurser innen analyse av sårbarheter og ondsinnet kode. Telenor varslet Cyberforsvaret umiddelbart om angrepet i 2013 og holdt dem løpende orientert, men BKI støttet ikke. Det nye totalforsvarskonseptet innebærer (som nevnt i kapittel 3) at Forsvaret, inklusive Cyberforsvaret, besitter ressurser som i større grad skal kunne brukes til støtte for politiet og sivile myndigheter. På den annen side kommer ikke Telenor inn under kategorien *myndighet.* Med dagens regulering av det sivil-militære samarbeidet kan ikke Cyberforsvaret bistå private selskaper direkte.

Når vi snakker om *bistand*, gjelder det primært bistandsinstruksen, altså bistand til politiet. Sekundært siktes det også til det nasjonale CERT-apparatet,

hvor Cyberforsvaret kan inngå i en større dugnad koordinert av NorCERT (Malmedal, 2014). Imidlertid kom det ingen anmodning fra NorCERT om å bistå i denne situasjonen. BKI ville heller ikke ha hatt kapasitet til å bidra til analysen av koden på daværende tidspunkt uten å måtte omdisponere personell (Heen, 2014).

Hovedprinsippene *ansvar, likhet og nærhet*, som ble presentert innledningsvis i studien, innebærer at den virksomheten som har ansvar for fagområdet til daglig, også har ansvar for å håndtere ekstraordinære hendelser. Hendelsen skal håndteres med en organisasjon som er mest mulig lik den man opererer med i det daglige, og på så lavt nivå som mulig.

Industrispionasjesaken ble håndtert i tråd med disse prinsippene. Telenor etablerte kriseledelse for å sikre koordinering og beslutninger. De varslet Post og teletilsynet, men verken PT eller departementet hadde noen rolle i håndteringen. På den annen side er det ingen aktør i samfunnet, hverken privat eller offentlig, som greier å holde oversikt over alle trusler som kan rettes mot nettverk og elektroniske informasjonssystemer. Derfor er det viktig at aktørene samarbeider godt.

Prinsippene *ansvar* og *samvirke* skal (som påpekt i kapittel 3) være overordnet og styrende i sektorovergripende kriser, slik som scenarioet i CyberDawn. I CyberDawn ble Cyberforsvaret bedt om å bistå i analyse av ondsinnet kode. BKI mottok ondsinnet kode, en *malware sample,* fra en av øvelsesdeltagerne og bisto i tråd med samvirkeprinsippet: NorCERT hadde da allerede gjennomført en initial analyse og ønsket at BKI skulle støtte opp under de vurderinger som var gjort (Dyrlie og Landaasen, 2013, s. 7).

NorCERT håndterer flere tusen cyberhendelser årlig. Avdelingen besitter mye kunnskap og erfaring relatert til datanettverk, trusler og sårbarheter. Det kan være grunn til å stille spørsmål ved behovet for bistand fra Cyberforsvaret til denne oppgaven. På den annen side besitter Cyberforsvaret mye kunnskap og erfaring relatert til denne type infrastruktur og analyse av malware, samtidig som de har et annet kontaktnett enn NorCERT. Når ressurser fra forskjellige virksomheter med sine kontaktnett samarbeider, øker muligheten for å lykkes.

Forsvarets ressurser skal kunne tas i bruk til støtte for sivile myndigheter, slik som NSM, i henhold til det nye totalforsvarskonseptet.[39] Cyberforsvaret vil følgelig kunne få spørsmål om å bistå gjennom CERT-samarbeidet også ved andre hendelser. Samtidig har Cyberforsvaret begrenset kapasitet. Det vil være opp til FOH å avgjøre om det skal brukes militære ressurser så fremt det faller inn under alminnelig bistand. Ifølge oberstløytnant Roger Johnsen ved FOH vil en slik beslutning kunne fattes i løpet av noen minutter (Johnsen, 2014).

Analyse av nettverk (overvåkning)

Det andre scenarioet som involverte Cyberforsvaret i øvelse CyberDawn var sikkerhetsmessig overvåkning av driftsnettet til Telenor. Telenor hadde bedt politiet om støtte til å finne ut hva de var utsatt for, hva denne angriperen faktisk holdt på med og hvordan de kunne normalisere og minimalisere konsekvensene av hendelsen (Landaasen, 2014). Politiet vendte seg til Forsvaret, og Cyberforsvaret fikk ordre om å bistå (Tønnesen og Landaasen, 2013b).

Hvor realistisk er dette scenarioet? Hva kan Cyberforsvaret bistå med ut over det Telenor selv kan? På den ene side fremstår det i første omgang lite sannsynlig at en virksomhet som Telenor har behov for ressurser fra Cyberforsvaret. Telenor er den dominerende leverandøren av ekom-tjenester i Norge og har solid ekspertise på feltet. Telenor har også, som vist i kapittel 5, en egen operasjonssentral som kontinuerlig overvåker infrastrukturen og iverksetter tiltak. På den annen side innebar scenarioet i CyberDawn at det nettet Telenor bruker til drift og overvåkning ble angrepet. Noen hadde tuklet med dataene slik at driftspersonellet ikke kunne ikke stole på det de så på skjermene sine (Landaasen, 2014). Ettersom drifts- og støttesystemene overvåker og styrer ekom-nettene, er de en kritisk del av infrastrukturen. I en slik situasjon ville Telenor kunne få behov for støtte.

[39] Instruksen for bistand til sivile myndigheter foreligger ikke ennå.

Det er primært NorCERT, ikke Cyberforsvaret, som skal bistå eier av kritisk infrastruktur ved tilsiktede hendelser. På den annen side har ikke NorCERT sensorer i Telenors infrastruktur. NorCERT besitter heller ikke mobile kapasiteter, noe som vil begrense deres mulighet til å bistå i en slik situasjon.

Cyberforsvaret er, på lik linje med Telenor, leverandør av landsdekkende kommunikasjonsinfrastruktur. Telenor og Cyberforsvaret sitter på mye av det samme utstyret, teknologien og kompetansen. Samarbeidsavtalen mellom Cyberforsvaret og Telenor har bidratt til å skape en felles arena for faglig samarbeid, en arena hvor personell fra Cyberforsvaret og Telenor i fellesskap kan se på konkrete problemer, teste nytt utstyr og ha samtreningsøvelser (Malmedal, 2014). De har derfor kjennskap til hverandres organisasjon og infrastruktur. Dersom infrastrukturen blir infisert, vil partene kunne støtte hverandre, sjekke om den andre parten har tilsvarende enheter i sine nett og om disse er infiltrert. Siden miljøene bruker ulike verktøy, sitter på hver sin del av situasjonsbildet og har ulike kontaktnett, har de også muligheter for å utfylle hverandre.

Cyberforsvarets mobile ressurser skal i prinsippet kunne bistå hvem som helst, når som helst og hvor som helst. Oberstløytnant Bjarte Malmedal bekrefter at Cyberforsvaret har bygd opp teknologi og materiell som gjør det i stand til å koble seg til nærmest alle IP-baserte nettverk (Malmedal, 2014). Forutsatt at BKI får nødvendig støtte fra en som har god kjennskap til nettet, kan cybersoldatene koble til sitt mobile utstyr, kartlegge, analysere og bidra med sine vurderinger og råd.

Cyberforsvarets målsetting med å delta på øvelse CyberDawn var imidlertid ikke å påvise hva de faktisk kan bistå med. Det interessante for Cyberforsvaret var å øve på prosessen for tilkobling av utstyr, herunder skaffe til veie nødvendig informasjon og tilganger, mer enn å teste verktøyene sine. Prosessen for tilkobling er omfattende og tidkrevende, og dette ble løst ved hjelp av direkte kontakt mellom teknisk personell i Telenor og BKI. Det er imidlertid den samme prosessen som brukes når BKI kobler seg til militære ugraderte nettverk, eksempelvis under vinterøvelsen, ifølge Stig Rune Heen, analytiker i BKI (Heen, 2014).

Få, om noen, andre nasjonale ressurser enn Cyberforsvaret har nødvendig verktøy og kompetanse dersom Telenor skulle trenge støtte, mener

sikkerhetssjefene Dyrlie og Landaasen i Telenor (Dyrlie, 2014; Landaasen, 2014). Samtidig er Cyberforsvarets ressurser dimensjonert for å beskytte Forsvarets egne systemer, basert på Forsvarets ambisjonsnivå. Cyberforsvaret er i utgangspunktet ikke dimensjonert for å sikre sivile nettverk. Seniorrådgiver i Forsvarsdepartementet, Torbjørn Braastad Tynning, påpeker at det er stor sannsynlighet for at Forsvaret selv vil ha behov for sine cyberressurser dersom nasjonen rammes av en alvorlig cyberhendelse (Tynning, 2014).

Erfaring fra moderne krigs- og konfliktsituasjoner viser at cyberoperasjoner rettet mot sivil IKT-infrastruktur kan være en del av et militært anslag fra en fremmed stat. En alvorlig cyberhendelse vil kunne fordre at Forsvaret øker overvåkningen av egne nettverk og har ressurser tilgjengelig dersom krisen eskalerer. På den annen side viste terroranslagene 22. juli at Forsvaret strekker seg langt for å bistå sivilsamfunnet, selv i situasjoner hvor det er uklart hva Norge står overfor. Som vi tidligere har sett, kan ikke Cyberforsvaret bistå eier av kritisk infrastruktur direkte. Cyberforsvaret vil kunne bistå, men det må skje etter anmodning om bistand fra politiet, slik det ble gjort i øvelse CyberDawn.

Koordinering og håndtering

Håndtere innebærer i denne sammenheng å gjennomføre nødvendige tiltak for å stoppe inntrenger, minimere konsekvenser og normalisere situasjonen. Håndtering forstås som bruk av de menneskelige, finansielle eller tekniske ressurser den aktuelle virksomheten disponerer.

Ansvarsprinsippet innebærer at den virksomhet, myndighet eller etat som har ansvar for et fagområde til daglig, også har ansvar for å håndtere ekstraordinære hendelser på området. Kritisk infrastruktur er, som tidligere påpekt, ikke noe unntak fra ansvarsprinsippet. Innholdsanalysen i kapittel 5 viste at tilbyder er pålagt å opprettholde nødvendig beredskap, det vil si tilby sine ekom-nett og tjenester med forsvarlig sikkerhet i hele spekteret fra fred til krig.

Ved hendelser i Telenors infrastruktur er det Telenor som har ansvaret for å få tjenestene opp å gå igjen. Det er heller ingen andre enn Telenor som *kan* håndtere hendelser i Telenors nett, sier sikkerhetssjef Storm Jarl Landaasen (Landaasen, 2014). Han får støtte fra Hans Christian Pretorius, avdelingsdirektør i NSM. Pretorius forklarer dette med det han kaller *verdikjedekompetanse* — kjennskap til infrastrukturen og de tjenestene som kjøres. Ifølge Pretorius vil NorCERT kunne gi virksomheten råd, men den angrepne virksomheten må ha mulighet til *selvberging* — verktøy og kunnskap til å kunne iverksette tiltakene som blir anbefalt (Pretorius, 2014).

Denne oppfatningen deles av major og analytiker Stig Rune Heen i Cyberforsvaret. Forutsatt at BKI får nødvendig støtte, kan cybersoldatene koble til sitt mobile utstyr, analysere og gi sine vurderinger og råd, men de vil normalt ikke gjøre noe ut over dette. De ruter ikke om trafikk, filtrerer ikke trafikk eller stenger ned porter — det må eier av nettverket gjøre selv (Heen, 2014).

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

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

Scenarioet i CyberDawn innebar et angrep på samfunnskritisk infrastruktur. Situasjonen dreide seg om en pågående alvorlig kriminell handling som hadde potensial til å ramme liv og helse. Slike situasjoner er i utgangspunktet politiets ansvar. Håndtering vil kunne innebære å måtte ta ned en spesifikk tjeneste eller tjenester i et gitt område for å isolere problemet. Politiet skal

kunne håndtere slike situasjoner med den makt og myndighet som tilligger politiet.

I det utilsiktede utfallet i Sunnmøre som ble nevnt innledningsvis i studien, satte politiet stab, kalte inn liaison fra Telenor, beordret egne folk ut i gatene og instruerte befolkningen i forhold til bruk av ekom-tjenestene (Dagbladet, 2014; Korsnes et al., 2014; Rosbach og Utne, 2014). Men selv om politiet viste at de maktet å håndtere konsekvensene av utfall i ekom-infrastrukturen, indikerte innholdsanalysen at politiet ikke har tilstrekkelig kompetanse og verktøy til å håndtere selve cyberangrepet — altså utøve makt i cyberdomenet. Dette bekreftes av Torgeir Magnussen, politiinspektør i POD: Øvelsen avdekket at politiet ikke har tilstrekkelige ressurser og kompetanse til å utføre det politiarbeidet som vil være nødvendig i en nasjonal krise utløst i cyberdomenet (Magnussen, 2014).

Rapporten *Politiet i det digitale samfunnet* ble skrevet i 2012, men Magnussen sier det ikke har skjedd store endringer på dette feltet i ettertid. Noe av forklaringen kan være 22. juli-kommisjonens ensidige fokus på beredskap i det fysiske domenet. En annen årsak synes å være en overdreven tiltro til hva NSM har hjemmel og kompetanse til å gjøre i forbindelse med en slik krise (Magnussen, 2014).

POD har fått i oppdrag av JD å lage et utkast til nasjonal strategi for bekjempelse av IKT-kriminalitet. Dette utvalget vil se på disse hvilke kapasiteter politiet bør ha i fremtiden (Magnussen, 2014). Som beskrevet i kapittel 3 er forutsetningen for bistand ifølge den nye bistandsinstruksen at politiets ressurser normalt skal være uttømt eller funnet utilstrekkelige for å løse oppdraget. I mangel på ressurser kan politiet, i tråd med bistandsinstruksen, vende seg til Forsvaret. Forsvaret står i en særstilling hva gjelder ansvar for å bekjempe fiendtlige datanettverksoperasjoner. Forsvaret skal ha evne til å gjennomføre cyberoperasjoner, herunder CND, CNE og CNA. Det er *hva* politiet måtte trenge bistand til som avgjør om Cyberforsvaret er en relevant ressurs eller ei.

Bruk av bistandsinstruksen

Blant de bestemmelser som regulerer bruk av Forsvarets ressurser i fredstid står bistandsinstruksen (omtalt i kapittel 3) særlig sentralt. Det er imidlertid ikke gitt at instruksen er egnet for bruk ved hendelser i cyberdomenet. Instruksen har så langt ikke vært i bruk i forbindelse med noen reell cyberhendelse, men den ble brukt under øvelse CyberDawn. I sluttrapporten fremhevet politiet viktigheten av å håndtere hendelser i cyberdomenet etter de samme retningslinjer som hendelser i andre domener i (Dyrlie og Landaasen, 2013, s. 9).

Bistandsinstruksens virkeområde er gitt i instruksens generelle bestemmelser. Den omfatter enhver form for støtte av militært personell og materiell, til politiet, i fred, krise og krig. Støtte fra Cyberforsvarets personell og materiell til analyse og sikkerhetsmessig overvåkning skulle derfor komme inn under instruksens virkeområde. I ettertid er det imidlertid blitt stilt spørsmål ved om Cyberforsvarets støtte reelt sett var bistand til Telenor eller politiet. Å overvåke et driftsnett *til støtte for Telenor* fremstår i utgangspunktet ikke som politiarbeid. Bistand til politiet dreier seg om bistand til det som er politiets ansvar og politiets oppgaver (Tynning, 2014).

På den annen side er Regjeringens viktigste oppgave å forebygge hendelser og kriser. Dersom kriser likevel oppstår, er målet å håndtere dem raskt og effektivt ved bruk av samfunnets ressurser. Forsvaret skal primært bistå politiet i politiets oppgaver, men dersom krisen ekspanderer til strategisk nivå, vil forsvarsministeren kunne legge sitt bidrag på bordet til lederdepartement eller Kriserådet. Det kan da bli besluttet at Forsvaret skal bistå med det som er mulig. Forsvaret vil kunne hjelpe samfunnet med å håndtere en krise i tilfeller hvor det er omfattende skader og politiet har en form for skadestedsledelse (Johnsen, 2014).

I øvelse CyberDawn ble analyse og overvåkning håndtert som politioppgaver. Politiet sier at de ikke ønsker å se på cyberdomenet som noe spesielt; de forholder seg til de oppgavene politiet har, uavhengig av domene. Telenors ansatte påpeker på sin side at hendelser i cyberdomenet må håndteres noe forskjellig fra hendelser i fysiske domener: «objekteier vil ha en mer sentral rolle i denne type hendelser enn det man ser i den tradisjonelle krisehåndteringen» (Dyrlie og Landaasen, 2013, s. 9).

Alle respondentene i denne studien støtter tilsynelatende det synspunkt at infrastruktureier vil ha en annen rolle dersom hendelsen eller angrepet skjer digitalt enn om det er en fysisk trussel. Men hvilken rolle skal eier ha, og hvordan skal bistanden organiseres? På den ene side er det naturlig at den som eier og drifter infrastrukturen, også må lede og koordinere håndteringen av sin infrastruktur i en krise. Dette vil være i tråd med ansvars-, nærhets- og likhetsprinsippene (kapittel 3). Det er eier av kritisk infrastruktur som kjenner sine systemer best. Det er virksomheten selv som besitter påkrevd kunnskap, verktøy og rutiner for å kunne iverksette nødvendige tiltak i infrastrukturen for å kunne normalisere situasjonen, eventuelt med den støtten de trenger fra Cyberforsvaret.

Samtidig, påpeker Telenor, kunne Cyberforsvaret i en tenkt nasjonal cyberkrise der Telenor var rammet, ha hatt en egen innsatsleder, en representant i Telenors kriseledelse. En slik representant, som kjente til hva Cyberforsvaret kunne bistå med i detalj, ville ha en unik kompetanse i en situasjon der man må diskutere tiltak (Dyrlie, 2014).

En alvorlig cyberkrise vil imidlertid få mange ringvirkninger, og liv og helse må gå foran alt annet. Dette taler for at politiet må styre krisehåndteringen. Eierens fokus vil være på gjenoppretting av systemene, mens politiet har fokus på liv og helse. En krise trenger en enhetlig ledelse, sier politiinspektør Torgeir Magnussen. Som presisert i gjennomgangen av de sentrale prinsippene i kapittel 3 er det ideelle at beslutninger fattes så lavt som mulig, men likevel på tilstrekkelig høyt nivå til at overordnede målsettinger blir ivaretatt. Det er ingen grunn til at andre enn politiet skal ha ledelsen i en sivil krise bare fordi den har utgangspunkt i det digitale rom (Magnussen, 2014).

Oberstløytnant Roger Johnsen sier at FOH ville ha krevd stedlig politiledelse i en reell angrepssituasjon. Oppdraget til bistandsenheten må være like tydelig som om det var en fysisk trussel. Forsvaret har én rapporteringsvei, og det er til overordnet politimester. Infrastruktureier har mye kompetanse på sin infrastruktur, men dette dreier seg om maktanvendelse (Johnsen, 2014). På den annen side viser funn i denne studien at politiet ikke har tilstrekkelig kunnskap og erfaring med håndtering av alvorlige cyberhendelser og bruk av makt i dette domenet. Politiet vil være mer avhengig av kunnskapen og kompetansen til dem som eier infrastrukturen enn det de vil være i den fysiske verden. Like fullt er det altså den politimesteren som anmoder om

bistand som har den overordnede ledelsen av operasjonen. Vedkommende skal blant annet påse at de midler som tas i bruk ikke overskrider rettslige eller andre grenser som er satt for politiets virksomhet (Magnussen, 2014). Dette er i tråd med føringene i bistandsinstruksen som vist i kapittel 3. Hvordan politimesteren evner å følge opp og lede operasjonen uten en *våpeninstruks* for bruk av cybermakt, og med begrenset kunnskap og erfaring, gir ikke denne studien noe svar på.

Under CyberDawn kategoriserte politiet først overvåkning av Telenors driftsnett som alminnelig bistand. Forsvaret[40] var uenig og definerte det som *håndhevelsesbistand.* Dersom et stort privat selskap blir utsatt for en tilsiktet hendelse som forstyrrer IKT-systemene deres i betydelig grad, og politiet ber om bistand fra Forsvaret, så er det meget sannsynlig at det ville bli vurdert som håndhevelsesbistand, sier Johnsen (Johnsen, 2014). Det kan imidlertid være problematisk å ha en bistandsinstruks som *normalt* vil utløse håndhevelsesbistand. Det tar millisekunder fra et tastetrykk gjøres på andre siden av kloden til det kan få effekt og kanskje eskalere videre i Norge. Respondentene fra Telenor og POD fremhever i tråd med dette viktigheten av at bistandsanmodningen behandles raskt, slik at sivil sektor kan få effekt av Forsvarets bistand i den kritiske fasen. Selv prosedyren for alminnelig bistand vil kunne ta for lang tid ved alvorlige hendelser, mener Magnussen. Han antyder at vi trenger en annen prosedyre for godkjenning av bistand for at samfunnet skal få effekt av bistanden.

Under CyberDawn ble Asker og Bærum politidistrikt kontaktet av Telenor. Politidistriktet kontaktet så Kripos, og i fellesskap formulerte de en bistandsanmodning, basert på den beskrivelsen Telenor hadde sendt til dem. Anmodningen ble så håndtert i POD. I en reell situasjon skulle anmodningen, som beskrevet i kapittel 3, gått fra ansvarlig politimester via POD, JD, FD, FST og så til FOH, men departementene og FST var ikke med på øvelsen.[41] I CyberDawn-scenarioet fungerte både telefon og mail, men likevel tok det relativt lang tid å håndtere anmodningen. Det er i og for seg ingen ting som alene tar for lang tid, men beslutningssløyfen for håndhevelsesbistand blir totalt sett for lang (Landaasen, 2014; Magnussen, 2014).

[40] Forsvaret er i dette tilfellet personellet i Øvelse Hovedstad som spilte FOH.
[41] FOH ble spilt av personell i Øvelse Hovedstad.

Den nye bistandsinstruksen søker å bøte på dette ved å legge opp til at bistanden kan forberedes *før* den er godkjent, i hastesituasjoner. Samtidig viste erfaringene fra 22. juli at prosessen kunne gå fort når det gjaldt. Under øvelse CyberDawn sto Cyberforsvarets biler på Fornebu allerede da øvelsen startet. I en reell situasjon ville de måtte ha blitt klargjort og kjørt ut, og dette ville uansett ta noe tid. Samtidig viser denne studien at prosessen for tilkobling av sensorer også tar tid. Deler av dette arbeidet vil imidlertid kunne utføres parallelt med at anmodningen går sin gang.

Oppsummering

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

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

Cyberforsvaret har kompetanse på analyse av sårbarheter og ondsinnet kode; det besitter mobile kapasiteter og har erfaring med bruk av dem. Disse ressursene skal i henhold til det nye totalforsvarskonseptet kunne stilles til disposisjon for sivile myndigheter. Videre er det funn som tilsier at Forsvaret kanskje ikke vil kunne avgi cyberressurser dersom nasjonen rammes av en alvorlig cyberhendelse. Beslutningen om å avgi ressurser til politiet for håndtering av et cyberangrep mot kritisk ekom-infrastruktur vil sannsynligvis fattes på

strategisk nivå. Det er viktig at beslutningen tas raskt for å oppnå ønsket effekt av bistanden. Samtidig er det viktig å sikre seg tilstrekkelig informasjon for å fatte den beste beslutningen. Cyberforsvaret er dimensjonert for å sikre Forsvarets egne systemer, systemer som er avgjørende for Forsvarets operative evne og effektivitet. Samtidig vil håndhevelsesbistand kunne ha politiske implikasjoner, som nevnt i kapittel 3. Beslutningsprosessen omfatter mange ledd, og den vil kunne ta tid dersom det er uklart hva slags trussel nasjonen står overfor.

Kapittel 7
Konklusjoner

Denne studiens tema er sivil-militært samarbeid i en cyberkrise. Teksten har fokusert på Cyberforsvarets rolle dersom sivil elektronisk kommunikasjonsinfrastruktur rammes av et cyberangrep. Dette kapitlet vil oppsummere de viktigste funnene i lys av problemstillingen: *Hva er Cyberforsvarets rolle dersom sivil elektronisk kommunikasjonsinfrastruktur rammes av et cyberangrep? Når kan Cyberforsvaret bistå, og hva kan det bistå med?*

Oppsummeringer og funn

I Norge har forholdet mellom sivile og militære myndigheter tradisjonelt vært regulert slik at Forsvaret skal ivareta rikets sikkerhet i forhold til eksterne trusler, mens politiet skal sørge for landets indre sikkerhet.

Det nye totalforsvarskonseptet innebærer imidlertid gjensidig støtte og samarbeid mellom Forsvaret og sivilsamfunnet. Forsvaret skal bistå sivilsamfunnet når viktige samfunnsinteresser og liv og helse står på spill — bistå med tilgjengelige kapasiteter, kompetanse og ressurser. Dette gjelder bistand både til politiet og til sivilsamfunnet for øvrig.

Forsvarets bistand til politiet er regulert gjennom bistandsinstruksen. Det er også under utarbeidelse en egen instruks for Forsvarets bistand til andre

sivile myndigheter. Bistandsinstruksen gjelder all form for støtte, herunder både personell og materiell, i fred, krise og krig. Forutsetningen for bistand er at politiets ressurser skal være uttømt eller funnet utilstrekkelige for å løse oppdraget. Utgangspunktet er fortsatt at sivile kriser håndteres med sivile ressurser, men terskelen for å be om bistand fra Forsvaret er blitt lavere.

Det nasjonale systemet for krisehåndtering og bruken av militære ressurser i fredstid er i utgangspunktet uavhengig av hvilket domene krisen oppstår i. Håndteringen av en alvorlig cyberhendelse må forholde seg til systemet for nasjonal krisehåndtering og sivil-militært samarbeid. Hovedregelen er at Forsvaret skal kunne bistå sivile myndigheter ved hendelser i cyberdomenet etter de samme prinsipper og regler som for annen militær bistand til samfunnssikkerhet. Dette systemet definerer i stor grad både *når* og med *hva* Cyberforsvaret vil kunne bistå. Cyberforsvaret kan bistå sivile myndigheter ved et cyberangrep mot ekom-infrastrukturen dersom hendelsen setter viktige samfunnsinteresser, liv og helse på spill, og under forutsetning av at politiets personell og materielle ressurser ikke strekker til. Cyberforsvaret vil i så fall kunne bistå med all tilgjengelig kompetanse og ressurser. Hva skal til for at et cyberangrep får konsekvenser for samfunnssikkerheten? Hvilke cyberressurser har det sivile samfunnet? Hvilke ressurser besitter Cyberforsvaret? Når er det åpenbart at politiets personell og materiell ikke strekker til?

Første del av selve undersøkelsen i denne studien omhandler ekom-infrastrukturen og cyberdomenet (kapittel 4). Samfunnet er blitt helt avhengig av fungerende ekom-nett, og studien viser at det er få, om noen, alternativer som kan erstatte Telenors landsdekkende infrastruktur. Samtidig er det så tette koblinger mellom denne infrastrukturen og andre systemer at svikt hos Telenor kan få drastisk negative følger for funksjonaliteten i andre systemer, med andre ord gi sektorovergripende konsekvenser. Deler av Telenors ekom-infrastruktur, herunder stamnett og drifts- og overvåkningssystemene, defineres derfor som kritiske for det norske samfunnet. Studien utelukker ikke på noen måte at også andre ekom-virksomheter besitter samfunnskritisk infrastruktur, men ettersom Telenor er den dominerende leverandøren av ekom-nett og ekom-tjenester i Norge, har selskapet fått en sentral plass i studien.

Cyberangrep er i denne studien definert som målrettede angrep med ulike formål, herunder både spionasje og sabotasje. Angrepene kan være vanskelige

å definere fordi angripernes identitet og motiver kan være uklare. Angrepene kan ligge i en gråsone mellom kriminell virksomhet og krigshandlinger, mellom politiets og Forsvarets ansvarsområder. Hovedregelen er likevel at cyberangrep mot sivil infrastruktur håndteres av sivile myndigheter inntil Regjeringen beslutter noe annet.

Andre del av undersøkelsen kartla og diskuterte aktører, ansvar, oppgaver og myndighet i det nasjonale cyberdomenet (kapittel 5). Dette ble gjort ved en innholdsanalyse med utgangspunkt i *Nasjonal strategi for informasjonssikkerhet*. Analysen viser at ekom-leverandøren er gitt i ansvar å oppdage, analysere og håndtere hendelser i egen infrastruktur, mens operasjonssenteret i NSM, NorCERT, ved hjelp av Varslingssystem for digital infrastruktur (VDI) og nasjonalt samarbeid, skal ha evne til å oppdage og analysere data knyttet til alvorlige hendelser på internett. Det er imidlertid frivillig å være med i VDI-samarbeidet, også for de virksomheter som eier samfunnskritisk infrastruktur. Dersom en hendelse rammer flere virksomheter, har NorCERT fått i ansvar å koordinere håndteringen av dem. NSMs myndighet er begrenset til håndhevelse av sikkerhetsloven.

Politiet har ansvar for å forebygge, avdekke, identifisere og håndtere datakriminalitet. Politiet skal kunne håndtere et pågående cyberangrep mot ekom-infrastrukturen ved bruk av den makt og myndighet som tilligger politiet. Innholdsanalysen indikerte at politiet ikke har tilstrekkelig kunnskap eller verktøy til å utøve makt i dette domenet i dag.

Tredje del av undersøkelsen drøftet to caser som innebar cyberangrep mot sivil infrastruktur. Intensjonen var å se på hvordan disse ble håndtert og hvilken bistand det var behov for i disse to casene. De oppgavene eller innsatsfeltene som viste seg å ha behov for støtte ble så drøftet fortløpende basert på teorigrunnlag og funn fra tidligere i studien. Studien viser at politiet ved et cyberangrep vil kunne få behov for bistand til analyse, herunder etablere en situasjonsforståelse, finne ut hva skadevaren har gjort og fører til, hva inntrenger holder på med og hvorfor, samt gi råd om hvordan man kan minimere konsekvenser og normalisere situasjonen. Studien utelukker ikke at sivile myndigheter også vil få behov for annen type bistand, men oppgaven gir ikke tilstrekkelig empiri til å si noe om dette.

Hva kan Cyberforsvaret bistå med, og når?

Studien viser at Cyberforsvarets ansvar og oppgaver primært er knyttet til Forsvarets nettverk. Cyberforsvarets ressurser er dimensjonert for å sikre Forsvarets egne systemer, systemer som er avgjørende for Forsvarets operative evne og effektivitet. Cyberforsvarets rolle er først og fremst å støtte opp under den nasjonale sikkerheten. Dette gjøres gjennom å sikre Forsvarets kommunikasjonsinfrastruktur og understøtte Forsvarets operasjoner hjemme og ute. Samtidig vil Cyberforsvaret, som Forsvaret for øvrig, kunne få en bistandsrolle dersom et cyberangrep setter samfunnssikkerheten i fare, eller viktige samfunnsinteresser, liv og helse står på spill, men dette er ikke en dimensjonerende oppgave for Cyberforsvaret. Slik støtte må eventuelt skje innenfor rammene av Bistandsinstruksen.

Et cyberangrep mot Telenors samfunnskritiske ekom-infrastruktur, herunder stamnett og drifts- og støttesystemer, vil ha potensial til å true viktige samfunnsinteresser. Samtidig viser studien at politiet har begrenset kompetanse og utilstrekkelige ressurser til å kunne håndtere pågående cyberhendelser helt alene.

Cyberforsvaret har teknologi, kunnskap og erfaring fra drift og overvåkning av egen landsdekkende ekom-infrastruktur. Det har kompetanse på analyse av sårbarheter og ondsinnet kode, besitter mobile kapasiteter og har erfaring med bruk av dem i nettverk de har lite kjennskap til fra før. Dersom sivil ekom-infrastruktur rammes av et cyberangrep som truer samfunnssikkerheten, vil Cyberforsvaret kunne bistå sivile myndigheter med faglig rådgivning og støtte fra enheter med særskilt kompetanse. Den enheten som vurderes å være mest sentral i forhold angrep på logiske sårbarheter i ekom-infrastrukturen, er Cyberforsvarets *Avdeling for beskyttelse av kritisk infrastruktur* (BKI). Avdelingen har deployerbare elementer og mulighet til å bistå med rådgivning og liaisonering.

Prinsipielt skal Cyberforsvaret kunne bistå med all tilgjengelig kompetanse og ressurser dersom sivil ekom-infrastruktur rammes av et cyberangrep som truer samfunnssikkerheten, og politiets personell og materielle ressurser ikke strekker til. Hvorvidt Forsvaret kan avgi cyberressursene dersom samfunnskritisk infrastruktur rammes av et cyberangrep, vil avhenge av det totale situasjonsbildet.

Stadig et sårbart samfunn

En bistandsanmodning om å støtte politiet ved håndtering av et cyberangrep mot kritisk ekom-infrastruktur vil måtte behandles på strategisk nivå. Det er viktig å sikre seg tilstrekkelig informasjon for å fatte den beste beslutningen. Samtidig er det vesentlig at bistandsressursene blir stilt til disposisjon raskt, slik at samfunnet skal få ønsket effekt av bistanden.

Beslutningsprosessen for håndhevelsesbistand omfatter mange ledd og vil kunne ta tid dersom det er uklart hva nasjonen står overfor. Sårbarhetsutvalget beskrev utfordringene samfunnet sto overfor i 2000 som en voksende og vanskelig definerbar risiko — dette som følge av bevisste handlinger i en gråsone mellom fred og krig. Utvalget argumenterte for at samarbeidet mellom politi og forsvar måtte bli bedre, fordi politiet hadde begrenset kapasitet til å møte de nye utfordringene samfunnet sto overfor. Studien viser at dagens utfordringer i cyberdomenet, tankevekkende nok, fortsatt passer inn i beskrivelsen fra 2000. Politiet har svært begrenset med ressurser og kompetanse til å utføre det politiarbeidet som vil være nødvendig i en nasjonal cyberkrise, til tross for at trusler mot cyberdomenet stadig øker.

Sårbarhetsutvalget etterlyste en avklaring på hvordan samvirket mellom politi og militære styrker skulle kunne etableres i det som ble vurdert som særlig kritiske situasjoner *uten* at det krevde medvirkning fra vedkommende departementer. Utvalget mente det var nødvendig med en raskere beslutningsprosess for å begrense tap, men kunne ikke vise til klare eksempler på hvorfor det skulle være behov for å justere instruksverket på området.

Scenarioet i CyberDawn innebar en kritisk situasjon for nasjonen. Scenarioet hevdes å være høyst realistisk og vil kunne være det i flere år fremover. Det er gått 14 år siden Willoch-utvalget leverte rapporten sin, og bistandsinstruksen er endret to ganger siden da. Terskelen for å be om bistand fra Forsvaret er blitt lavere med den nye instruksen, men beslutningssløyfen er fortsatt lang. Det er derfor grunn til å spørre om regelverket rundt beslutningsprosessen ivaretar cybertrusler i tilstrekkelig grad. Samtidig vil det i dag, som i 2000, være vanskelig å argumentere definitivt for at den ikke gjør det så lenge det ikke finnes reelle hendelser å vise til.

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

Forkortelser

BKI	Avdeling for Beskyttelse av kritisk infrastruktur
CERT	Computer Emergency Response Team
CNA	Computer Network Attack
CIS TG	Communication Information System Task Group
CKG	Cyberkoordineringsgruppen
CND	Computer Network Defence
CNE	Computer Network Exploration
CNO	Computer Network Operations
CYFOR	Cyberforsvaret
CTO	Avdeling for Cybertjenester og operasjoner
DSB	Direktoratet for samfunnssikkerhet og beredskap
EKOM	Elektronisk kommunikasjon
E-tjenesten	Forsvarets etterretningstjeneste
FAD	Fornyings-, administrasjons- og kirkedepartementet
FD	Forsvarsdepartementet
FFI	Forsvarets forskningsinstitutt
FFOD	Forsvarets fellesoperative doktrine
FKI	Forsvarets kommunikasjonsinfrastruktur
FLO	Forsvarets logistikkorganisasjon
FOH	Forsvarets operative hovedkvarter
FO/S	Forsvarets overkommando/Sikkerhetsstaben
FOST	Forsvarets sikkerhetstjeneste [fra 2009]
FSA	Forsvarets sikkerhetsavdeling [til 2009]
FST	Forsvarsstaben
IKT	Informasjons- og kommunikasjonsteknologi
INI	Forsvarets Informasjonsinfrastruktur [fra 2012 Cyberforsvaret]
INI OPS	INI-operasjoner
ISP	Internet Service Provider
J6	Joint 6 — Samband
JD	Justis- og beredskapsdepartementet
KSE	Krisestøtteenheten
NorCERT	Norwegian Computer Emergency Response Team (NSM)
NOU	Norges offentlige utredninger
NSM	Nasjonal sikkerhetsmyndighet

NUPI	Norsk utenrikspolitisk institutt
PBS1	Politiets beredskapssystem, del 1
POD	Politidirektoratet
PST	Politiets sikkerhetstjeneste
PT	Post- og teletilsynet
SD	Samferdselsdepartementet
TSOC	Telenor Security Operations Centre
VDI	Varslingssystem for digital infrastruktur

Liste over figurer

Litteratur- og kildeliste

Andersen, Rune (2013). «Politiets ansvar og rolle ved krisehåndtering». Paper presentert på Foredrag for Stabsstudiet 7. juni 2013, Forsvarets stabsskole.

Beredskapsloven (1950). LOV-1950—12—15—7: *Lov om særlige rådgjerder under krig, krigsfare og liknende forhold.* Oslo: Justis- og beredskapsdepartementet.

Bistandsinstruksen (2012). FOR-2012—06—22—581: *Instruks om Forsvarets bistand til politiet.* Oslo: Forsvarsdepartementet.

Bjerga, Kjell Inge (2012). «Tettere sivilmilitært samarbeid etter 22. juli». *Trygge samfunn. Tidsskrift for Kvinners frivillige beredskap* nr. 4, s. 9. Oslo: KFB.

Bjerga, Kjell Inge og Magnus Håkenstad (2013). «Hvem eier krisen? Politi, forsvar og 22. juli», i Heier og Kjølberg (red.), s. 54—74.

Bjørgo, Tore et al. (2013). *Program for samfunnssikkerhet (SAMRISK II). Rapport til Forskningsrådet fra programplanutvalget nedsatt av Divisjonsstyret for samfunn og helse*. Oslo: Forskningsrådet.

Bogen, L. og K. Mørkestøl (2005). *Håndtering av IKT-kriser — aktører og roller*. FFI-rapport 2005/03 536. Kjeller: Forsvarets forskningsinstitutt.

Brattekås, K., J. M. Hagen og T. Sandrup (2011). *Evaluering av øvingseffektar — EKOM 2011*. FFI-rapport 2011/01 905. Kjeller: Forsvarets forskningsinstitutt.

Breivik, Terje og Kjetil Kjenseth (2014). Representantforslag fra stortingsrepresentantene Terje Breivik og Kjetil Kjenseth om etablering av en nasjonal bredbåndsplan. Dokument 8: S (2013—2014), 23. januar.

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

[DSB]

Direktoratet for samfunnssikkerhet og beredskap (2012). *Samfunnets sårbarhet overfor bortfall av elektronisk kommunikasjon.* Tønsberg: DSB.

Direktoratet for samfunnssikkerhet og beredskap (2013a). *Nasjonalt risikobilde: Katastrofer som kan ramme det norske samfunnet*. Tønsberg: DSB.

Direktoratet for samfunnssikkerhet og beredskap (2013b). *Teknologiskiftet i Telenors infrastruktur.* Tønsberg: DSB.

Dyndal, Gjert Lage (red.) (2010). *Strategisk ledelse i krise og krig.* Bergen: Fagbokforlaget.

Dyndal, Gjert Lage (2010). «Tydelige rammer, men allikevel mange gråsoner», i Dyndal (red.), s. 13—24.

Dyndal, Gjert Lage og Sigmund Simonsen (2013). «Krisehåndtering: Sentralisert over-departemental ledelse eller desentalisert sektoransvar?» *Minervanett,* 10. oktober. Hentet fra <http://www.minervanett.no/krisehandtering/>

Dyrlie, Rune og Storm J. Landaasen (2013a). *Øvelse CyberDawn 2013. Sluttrapport.* Fornebu: Telenor.

Dyrlie, Rune (2013b). Innlegg på NSMs sikkerhetskonferanse [videoklipp].

[Dyrlie, Rune — respondent]

Ekomloven (2003). LOV-2003—07—04—83: *Lov om elektronisk kommunikasjon.* Oslo: Samferdelsdepartementet.

E-tjenesten, NSM og PST (2013). *Trusler og sårbarheter 2013. Samordnet vurdering fra E-tjenesten, NSM og PST.*

Etterretningstjenesten (2014). *Etterretningstjenestens vurdering FOKUS 2014,* 20. januar.

Fagerland, Snorre, Morten Kråkvik, Jonathan Camp og Ned Moran (2013). *The Hangover report: Unveiling an Indian cyberattack infrastructure,* 20. mai. San Diego: Norman Shark.

Forskningsrådet (2013). *Samfunnssikkerhet (SAMRISK II). Om Programmet*.

Forskrift om objektsikkerhet (2010). FOR-2010—10—22—1362. Oslo: Forsvarsdepartementet.

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

[FD]:

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

Forsvarsdepartementet (2012b). *«Et forsvar for vår tid»*: *Iverksettingsbrev til forsvarssektoren for langtidsperioden 2013—2016.* Oslo, 28. juni.

Forsvarsdepartementet (2013). *Høringsnotat. Om lov om Forsvarets ansvar for å avverge luftbårne terroranslag og Forsvarets bistand til politiet.* Oslo, 11. juli.

Forsvarsdepartementet (2014a). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner «FDs cyberretningslinjer»*. Oslo, 1.mars.

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

Fridheim, Håvard og Janne Hagen (2007). *Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer – sluttrapport.* FFI-rapport 2007/01 204. Kjeller: Forsvarets forskningsinstitutt.

Gabrielsen, Christofer Kjos (2013). «Høyre frykter 'digitalt 22. juli'». *TV 2,* 21. februar. Hentet fra <http://www.tv2.no/a/3 993 710> (lest mai 2014).

Grunnloven (1814). LOV-1814—05—17: *Kongeriget Norges Grundlov, given i Rigsforsamlingen paa Eidsvold den 17de Mai 1814.* Oslo: Justis- og beredskapsdepartementet.

Hagen, Janne M., Håvard Fridheim og Tonje Grunnan (2010). *(U) Sikkerheitspolitisk krise, nasjonal kriseleiing og sivilmilitært samarbeid.* Sladdet versjon. FFI-rapport 2010/01 009. Kjeller: Forsvarets forskningsinstitutt.

Hamnes, Leif (2012). «Norsk tillitskultur passer dårlig i cyberspace». *Teknisk ukeblad,* 3. juli. Intervju med forsvarsminister Espen Barth Eide.

[Heen, Stig Rune — respondent]

Heier, Tormod og Anders Kjølberg (red.) (2013). *Mellom fred og krig: Norsk militær krisehåndtering*. Oslo: Universitetsforlaget.

Heieraas, Bjørn Olav (2010). «Bajonetter til innvortes bruk: sivil-militære relasjoner i historisk perspektiv», i Dyndal (red.), s. 91—107.

Hillestad, Linn Kongsli og Espen Sandli (2013).Det er ikke et spørsmål *om* vi blir utsatt for et sånt angrep, det er et spørsmål om *når*». Intervju med generalmajor Roar Sundseth, sjef for Cyberforsvaret. *Dagbladet,* 18. oktober. I serien *Null CRTL*. Hentet fra <http://www.dagbladet.no/nullctrl/> (lest juni 2014)

Høyre-Frp-regjeringen (2013). *Politisk plattform for en regjering utgått av Høyre og Fremskrittspartiet.* Sundvollen, 7. oktober.

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

Irgens, Morten (2013). «Cybersikkerhet er ikke informasjonssikkerhet er ikke IKT-sikkerhet». Blogginnlegg, 27. juli. Hentet fra <http://mortenirgens.com/?p=769> (lest mai 2014).

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

Johansen, Per Anders (2013). «Spionerte på Telenor-sjefer, tømte all e-post og datafiler». *Aftenposten,* 17. mars.

[Johnsen, Roger — respondent]

Johnsen, Roger (2013). «Cyberkrigføring og Forsvarets operative evne». *Internasjonal politikk* nr. 2, s. 241—251. (Temanummer *Fokus: Politikk i cyberspace.*) Oslo: NUPI.

Johnsen, Siw Tynes og Torbjørn Kveberg (2014). *Cyberdomenet, cybermakt og norske interesser*. FFI- rapport 2013/02 712. Kjeller: Forsvarets forskningsinstitutt.

Karlsen, Stina G. (2013). «Dagbladet stakk av med gjev datapris». *Dagbladet,* 27. november.

Kirknes, Leif Martin (2013). Cyberforsvaret vil ha cyberstrategi. Intervju med sjef for Cyberforsvaret, Roar Sundseth. *Computerworld*, 2. oktober. Hentet fra

Knudsen, Eigil (2013). «Britiske 'NSA' hacket belgisk telegigant. Ny, stor skandale avslørt av Snowden-dokumenter». xxxxxx, 23. september. Hentet fra <http://www.tek.no/artikler/britiske-nsa-hacket-belgisk-telegigant/137 709>

Korsnes, Malin K., Sara L. Roaldseth og Frode Berg (2014). «Politiet har sendt etterforskere til stedet hvor strømbruddet skjedde». *NRK,* 6. mars. Hentet fra <http://www.nrk.no/mr/pressekonferanse-om-telekollaps-1.11 587 154>

[Landaasen, Storm Jarl — respondent]

Langø, Hans-Inge og Kristin Bergtora Sandvik (2013). «Cyberspace og sikkerhet». *Internasjonal politikk* nr. 2, s. 221—228.

[Magnussen, Torgeir — respondent]

[Malmedal, Bjarte — respondent]

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

Meld. St. 21 (2012—2013). *Terrorberedskap. Oppfølging av NOU 2012: 14, Rapport fra 22. juli-kommisjonen.* Oslo: Justis- og beredskapsdepartementet.

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

NOU 2000: 24. *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Innstilling avgitt til Justis- og politidepartementet 4. juli.

NOU 2006: 6. *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Innstilling avgitt til Justis- og politidepartementet 5. april.

NOU 2012: 14. *Rapport fra 22. juli-kommisjonen*. Avgitt til statsministeren 13. august.

NSM (2014a). *Sikkerhetstilstanden 2014. Rapport.* Oslo: Nasjonal sikkerhetsmyndighet. Hentet fra <https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2014.pdf>

NSM (2014b). *Årsrapport 2013.* Oslo: Nasjonal sikkerhetsmyndighet.

NTB/Dagbladet (2014). «Nødnettet gikk ned, politiet måtte ut i gatene», 6. mars.

NUPI (2011). *Nye sikkerhetstrusler: cyberangrep. Del 6: Hvordan forsvarer vi oss?* Oslo: NUPI.

Nystuen, Kjell Olav og Håvard Fridheim (2007). *Sikkerhet og sårbarhet i elektroniske samfunnsinfrastrukturer – refleksjoner rundt regulering og tiltak*. FFI-rapport 2007/00 941. Kjeller: Forsvarets forskningsinstitutt.

Næringslivets sikkerhetsråd (2012). *Mørketallsundersøkelsen — Informasjonssikkerhet og datakriminalitet.*

Politiet (2011). *Politiets beredskapssystem del 1 (PBS 1). Retningslinjer for politiets beredskap.* Oslo: Politidirektoratet.

[PT]

Post- og teletilsynet (2012a). *Sårbarhetsanalyse av mobilnettene i Norge*. PT-rapport nr. 1/2012.

Post- og teletilsynet (2012b). *Foreløpige erfaringer og forslag til tiltak etter ekstremværet Dagmar*. PT-rapport nr. 2/2012.

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

Post- og teletilsynet (2014). «Om Post- og teletilsynet» (PT). Hentet fra <www.npt.no/om-pt> (lest mai 2014).

[Pretorius, Hans Christian — respondent]

Prop. 1 S (2007—2008). (2007). *Proposisjon til Stortinget (forslag til stortingsvedtak)*.

Prop. 1 S (2013—2014). *Proposisjon til Stortinget (forslag til stortingsvedtak)*. Oslo: Forsvarsdepartementet.

Prop. 73 S (2011—2012). *Et forsvar for vår tid*. Oslo: Forsvarsdepartementet.

Ravnaas, Paal (2013). «Cyber-ambulansen. Sorte biler rykker ut for å beskytte Forsvaret mot ondsinnede koder eller virus». *Forsvarets forum,* 2. september.

Regjeringen (2012a). *Nasjonal strategi for informasjonssikkerhet*. Oslo: Fornyings-, administrasjons- og kirkedepartementet.

Regjeringen (2012b). *Nasjonal strategi for informasjonssikkerhet — Handlingsplan*. Oslo: FAD.

Regjeringen (2013a). *Forsvarets bistand til politiet og Forsvarets ansvar for å avverge luftbårne terroranslag.*

Regjeringen (2013b). Klargjering om bistandsinstruksen og Grunnloven § 99.

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

Rosbach, Marius og Tormod Utne (2014). «Omfattende feil med telefon og internett». *Sunnmørsposten,* 6. mars.

Rui, Jon Petter (2011). «Politiets behov for støtte fra Forsvaret: Lovgivning er nødvendig». *Lov og rett nr. 8,* s. 445—446.

Sandvik, Kristin Bergtora (2013). «Cyberkrig og internasjonal rett». *Internasjonal politikk* nr. 2, s. 252—263.

Senel, Emrah og Erik Hattrem (2014). «Slik skal Lærdal få mobildekning igjen». *NRK,* 19. januar.

Sikkerhetsloven (1998). LOV-1998—03—20—10: *Lov om forebyggende sikkerhetstjeneste.* Oslo: Forsvarsdepartementet.

Spiegel Online International (2013). «Belgacom attack: Britain's GCHQ hacked Belgian telecoms firm».

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

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

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

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

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

St.prp. nr. 1 (2002—2003). *For budsjetterminen 2003*.

St.prp. nr. 1 (2007—2008). *For budsjettåret 2008*. Oslo: Forsvarsdepartementet.

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

Storruste, Bente og Torgeir Magnussen et al. (2012). *Politiet i det digitale samfunnet. En arbeidsgrupperapport om: elektroniske spor, IKT-kriminalitet og politiarbeid på internett*. Oslo: Politidirektoratet.

Sundseth, Roar (2013). «Cyberoperasjoner — utfordringer i Cyber». Foredrag i Oslo Militære Samfund, 18. februar.

Sveinbjørnsson, Sigvald (2012). «Hver tredje ISP bryr seg ikke. Nå reagerer Norges førstelinjeforsvar mot kyberkriminalitet». *Digi.no,* 4. mai. [Teknisk Ukeblads nettavis for IKT-bransjen].

Svendsen, Berit (2014). «Digital robusthet — mer enn fiberkabler». *E 24*, februar.

Søreide, Ine Eriksen (2014). «Åpning av sikkerhetskonferansen — Part 1» [videoklipp].

Telenor SOC (2014). «TSOC-nyhetsbrev — daglige oppdateringer fra TSOC». Hentet fra <http://telenorsoc.blogspot.no/> (lest mai 2014).

[Tynning, Torbjørn Braastad — respondent]

Tønnessen, Kristin V. og Storm J. Landaasen (2013a). «Cyberkriser må koordineres på tvers». Fornebu: Telenor Norge.

Tønnessen, Kristin V. og Storm J. Landaasen (2013b). Cyberkriser må koordineres på tvers [videoklipp]. Hentet fra <https://www.youtube.com/watch?v=OW3pMscYPJ4> (lest juni 2014)

Utheim, Eric B. (2013). «Eksplosjon i antall norske data-angrep». *E 24,* 29. mai.

Windvik, Ronny, Aasmund Thuv, Kjell Olav Nystuen og Tormod Sivertsen (2007). *Sårbarheter i Internett*. FFI- rapport 2007/00 903. Kjeller: Forsvarets forskningsinstitutt.

Østby, Lene (2014). «Huawei-saken: PST frykter kinesisk 4G-spionasje». Intervju med sekssjonssjef i PST, Erik Haugland. *TV2,* 9. februar.

Respondenter

Rune Dyrlie, sikkerhetsdirektør (Chief Security Technology Officer) i Telenor. Håndterte industrispionasjesaken i 2013. Intervjuet 24. februar 2014, Telenor, Fornebu.

Stig Rune Heen, major CTO BKI CND, Cyberforsvaret. Deltok som analytiker på CyberDawn. Intervjuet 25. februar 2014, telefonmøte.

Roger Johnsen, oberstløytnant OPS J6 Plan-Sys, Forsvarets operative hovedkvarter. Tidligere sjef for Forsvarets senter for beskyttelse av kritisk infrastruktur (BKI) og skolesjef ved Forsvarets ingeniørhøgskole. Intervjuet 5. mars 2014, Oslo.

Storm Jarl Landaasen, sikkerhetssjef (Chief Security Intelligence Officer & Crisis Manager) i Telenor. Var øvingsleder for CyberDawn 2013. Intervjuet 24. februar 2014, Telenor, Fornebu.

Torgeir Magnussen, politiinspektør. Spilte Politidirektoratet under CyberDawn 2013. Intervjuet 11. mars 2014, Politidirektoratet, Oslo.

Bjarte Malmedal, oberstløytnant CST Plan og utvikling, Cyberforsvaret. Intervjuet 21. februar 2014 ved Cyberforsvaret, Jørstadmoen.

Hans Christian Pretorius, avdelingsdirektør operativ avdeling i NSM. Intervjuet 20. mars 2014, NSM, Bryn.

Torbjørn Braastad Tynning, seniorrådgiver FD 2—4, Forsvarsdepartementet. Intervjuet 28. februar 2014, Akershus festning.

Vedlegg Informasjonsskriv til respondent

Forespørsel om deltakelse i forskningsprosjektet «Sivilmilitært samarbeid i en cyberkrise»

Bakgrunn og formål

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

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

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

Hva innebærer deltakelse i studien?

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

Hva skjer med informasjonen om deg?

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

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

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

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

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

FORSVARETS STABSSKOLE
FORSVARETS HØGSKOLE

Akershus Festning, bygning 10
Postboks 1550 Sentrum
0015 Oslo, Norge